DSS ACCESS

VOLUME 2, ISSUE 3

OFFICIAL MAGAZINE OF THE DEFENSE SECURITY SERVICE

BEST OF THE BEST

DSS RECOGNIZES 2013 COGSWELL RECIPIENTS

FALL 2013

VOLUME 2, ISSUE 3

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

Since I arrived at DSS just over two years ago, I have made partnering with industry a priority for the DSS workforce. I believe that a relationship built on mutual respect and understanding is the best way to ensure the protection of classified information and ultimately our nation's security. Nothing demonstrates that partnership more than the Cogswell Outstanding Industrial Security Achievement Awards.

As many of you may know, the award is named for Air Force Col. James S. Cogswell, the first chief of industrial security within the Department of Defense. Cogswell was responsible for developing the basic principles of the Industrial Security Program, which include an emphasis on the partnership between industry and government to protect classified information. Cogswell believed that partnership ultimately ensures the greatest protection for the U.S. warfighter and our nation's classified information.

In June, DSS presented the Cogswell award to just 24 cleared facilities out of a population of more than 13,500 facilities. These numbers show just how rigorous the criteria and how difficult it is to achieve the award. Cogswell recipients are truly the best of the best and I believe they have much to share with the rest of the industrial security community. So, we invited each 2013 Cogswell winner to share their success with our readers and write about their best practices, lessons learned, tips and techniques. I'm very pleased that six of our winners took us up on the offer and their input is captured in this issue.

As you can tell from their stories, the culture of security is very important and clearly present at each of these facilities. But ultimately companies don't create excellent programs, people do — people in the Government Contracting Activities, in cleared industry and at DSS — working in partnership.

DSS RECOGNIZES 2013 COGSWELL RECIPIENTS

THE CEREMONY

On June 26, 2013, the Defense Security Service presented the annual James S. Cogswell Outstanding Industrial Security Achievement Award to 24 cleared contractor facilities. The winning facilities represent the "best of the best," and their security programs stand as models for others to emulate. These 24 facilities represent less than 1 percent of the over 13,500 cleared contractors in the National Industrial Security Program (NISP).

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

Among this year's winners was one category "AA" facility, which is among the largest in the NISP. Sims, in his remarks during the award ceremony, said the recognition of an AA facility demonstrates that even the most complex security programs have the ability to attain this honor. "AAs are the largest companies in the NISP," he said. "They are also the most complex with more moving pieces that must be effectively managed. As a result, there's more opportunity for error but also more opportunities to excel and go above and beyond the basic requirements."

Sims also noted that the winners were working on a myriad of technologies. "Some are research and development centers. Some are doing intelligence services. Some are steeped in hardware, like electronics manufacturing, aviation design, naval systems or missile and space systems. Still others are involved in logistics and engineering support," he said. "This shows the breadth of the NISP and I'm glad the Cogswell represents that diversity of effort."

In presenting the awards, Sims said, "I can say that each of these recipients show clear management and corporate commitment to security. The culture of security is very important and clearly present at all of these facilities."

THE PROCESS

In order to win a Cogswell Award, facilities must demonstrate excellence in all areas of their industrial security programs. Winners must also receive two consecutive "Superior" ratings exceeding the baseline requirements of the National Industrial Security Program Operating Manual (NISPOM). Furthermore, a Cogswell winner provides leadership to other cleared facilities and actively participates in security awareness groups, such as local Industrial Security Awareness Councils and NCMS chapters, whose objectives are to foster communication and enhance security practices across the security community.

The Cogswell selection process is rigorous and spans an eight-month review. The process starts with the industrial security representative who nominates a facility. To even be considered, a facility must have two consecutive superior ratings. Superior ratings indicate a facility has exceeded the baseline requirements of the NISPOM. The fact that a facility has two consecutive superior ratings does not guarantee their Cogswell nomination. In fact, approximately three percent of the cleared facilities receive a superior rating each year. Two consecutive superior ratings does, however, clearly demonstrate a facility's commitment to security over time.

Once a pool of nominees is established in DSS, the list is vetted with 30 external agencies. The nominations are next reviewed by a national review team consisting of regional directors and representatives from across DSS. The review team recommends award recipients to DSS senior leadership for final decision based on the following criteria:

- Overall security program
- Senior management support
- Security vulnerability assessments
- Security education and awareness
- Level of experience of facility security officer and security staff
- Classified material controls

This year, all winning facilities were rated under the ratings matrix. The ratings matrix has not only provided more uniformity and consistency to the rating process but also brought more uniformity to the Cogswell selection process.

THE AWARD

In May 1966, the Defense Supply Agency established an Industrial Security Award Program for participating contractors of the Defense Industrial Security Program.

This Department of Defense (DoD)-wide program evolved from a similar program developed in November 1963 by the Bureau of Naval Weapons to recognize its prime (cleared) contractors for outstanding industrial security achievement.

In 1980, the Defense Investigative Service began administering this award program, known as the Department of Defense James S. Cogswell Outstanding Industrial Security Achievement Award.

The award, named in honor of Colonel James S. Cogswell, United States Air Force, the first chief of the unified office of industrial security, symbolizes a joint government-industry commitment to industrial security excellence. It also serves as an incentive to motivate contractors to improve their security programs.

The number of awardees has varied each year from a low of just nine to as many as 30. The most recent years have seen the number of awardees in the twenties.

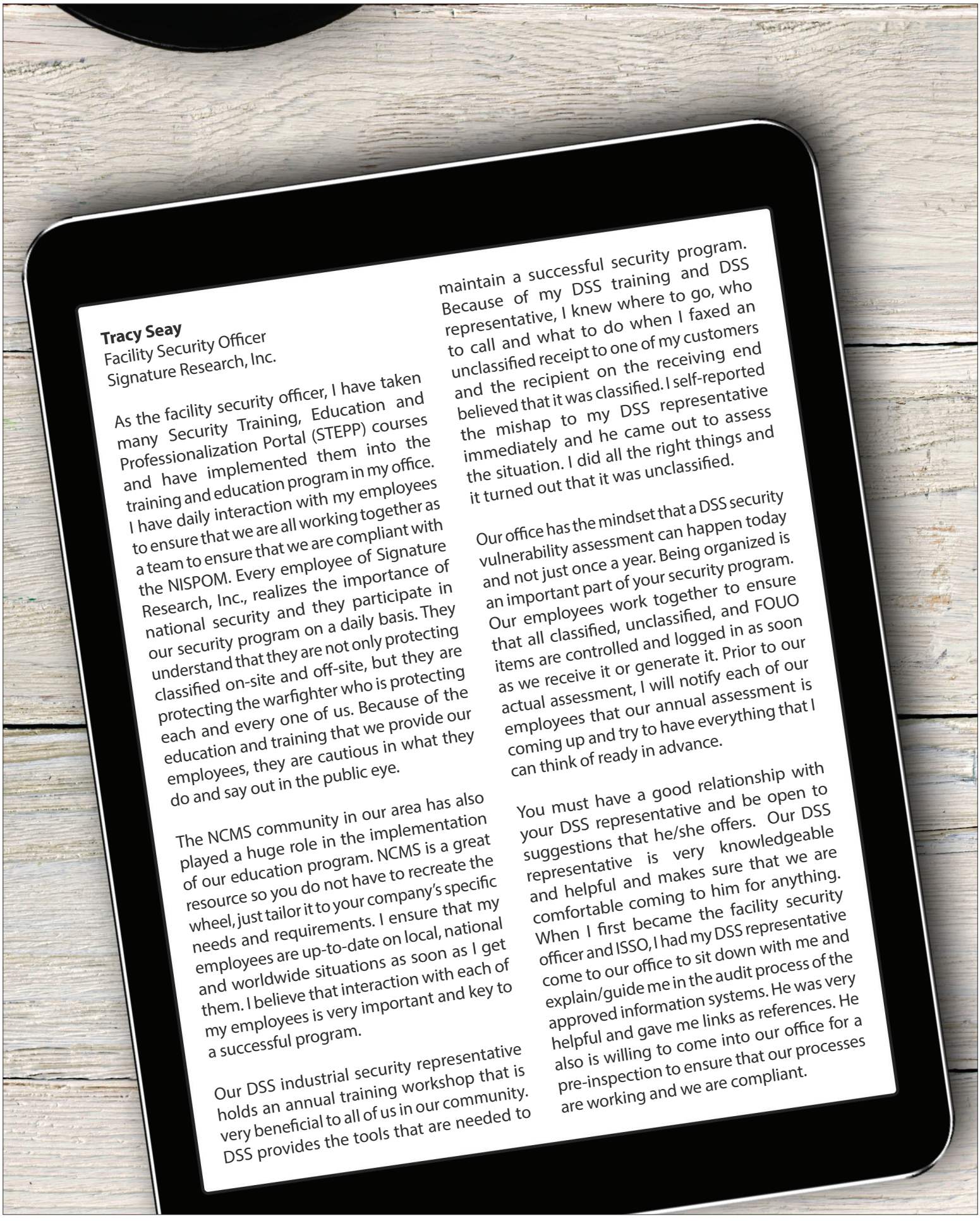
THE WINNERS

DSS is proud to recognize the following recipients of the 2013 Cogswell award:

- Aerojet-General Corporation — *Rancho Cordova, Calif.*
- BAE Systems Information Solutions, Inc. — *McLean, Va.*
- BAE Systems Land & Armaments, LP — *Minneapolis, Minn.*
- Battelle Eastern Science and Technology Center — *Aberdeen, Md.*
- Boeing Aerospace Operations, Inc. — *Oklahoma City, Okla.*
- The Boeing Company — *Oklahoma City, Okla.*
- The Boeing Company: Space and Intelligence Systems — *Seal Beach, Calif.*
- CDI Corporation — *Portsmouth, Va.*
- Celestica Aerospace Technologies Corporation — *Austin, Texas*
- The Columbia Group, Inc. — *Washington, D.C.*
- DRS RSTA, Inc. — *Dallas, Texas*
- DRS RSTA, Inc. — *Melbourne, Fla.*
- DRS Technologies, Inc. — *Arlington, Va.*
- General Dynamics Advanced Information Systems — *Bloomington, Minn.*
- L-3 Randtron Antenna Systems — *Menlo Park, Calif.*
- Logos Technologies, LLC — *Fairfax, Va.*
- The MITRE Corporation — *McLean, Va.*
- Northrop Grumman Guidance & Electronics Company, Inc. — *Woodland Hills, Calif.*
- Oceaneering — *Hanover, Md.*
- Rockwell Collins Simulation and Training Solutions — *Binghamton, N.Y.*
- Serco Inc. — *Reston, Va.*
- Signature Research, Inc. — *Navarre, Fla.*
- Southwest Research Institute — *San Antonio, Texas*
- URS Federal Technical Services — *Dahlgren, Va.*

HOW THEY DID IT

The winners of the 2013 Cogswell Award were invited to share their formulas for success. The next pages feature tips and lessons learned from facilities with proven track records on how to establish and maintain a high quality security posture.



Tracy Seay
Facility Security Officer
Signature Research, Inc.

As the facility security officer, I have taken many Security Training, Education and Professionalization Portal (STEPP) courses and have implemented them into the training and education program in my office. I have daily interaction with my employees to ensure that we are all working together as a team to ensure that we are compliant with the NISPOM. Every employee of Signature Research, Inc., realizes the importance of national security and they participate in our security program on a daily basis. They understand that they are not only protecting classified on-site and off-site, but they are protecting the warfighter who is protecting each and every one of us. Because of the education and training that we provide our employees, they are cautious in what they do and say out in the public eye.

The NCMS community in our area has also played a huge role in the implementation of our education program. NCMS is a great resource so you do not have to recreate the wheel, just tailor it to your company's specific needs and requirements. I ensure that my employees are up-to-date on local, national and worldwide situations as soon as I get them. I believe that interaction with each of my employees is very important and key to a successful program.

Our DSS industrial security representative holds an annual training workshop that is very beneficial to all of us in our community. DSS provides the tools that are needed to maintain a successful security program. Because of my DSS training and DSS representative, I knew where to go, who to call and what to do when I faxed an unclassified receipt to one of my customers and the recipient on the receiving end believed that it was classified. I self-reported the mishap to my DSS representative immediately and he came out to assess the situation. I did all the right things and it turned out that it was unclassified.

Our office has the mindset that a DSS security vulnerability assessment can happen today and not just once a year. Being organized is an important part of your security program. Our employees work together to ensure that all classified, unclassified, and FOUO items are controlled and logged in as soon as we receive it or generate it. Prior to our actual assessment, I will notify each of our employees that our annual assessment is coming up and try to have everything that I can think of ready in advance.

You must have a good relationship with your DSS representative and be open to suggestions that he/she offers. Our DSS representative is very knowledgeable and helpful and makes sure that we are comfortable coming to him for anything. When I first became the facility security officer and ISSO, I had my DSS representative come to our office to sit down with me and explain/guide me in the audit process of the approved information systems. He was very helpful and gave me links as references. He also is willing to come into our office for a pre-inspection to ensure that our processes are working and we are compliant.

Rick Ramsey, Director of Security
Cheryl Cotsimopoulos, Facility Security Officer
Corporate Security
Serco, Inc.

Serco's security team is a decentralized collaborative organization that supports over 8,000 employees throughout the world using a single process. This approach has provided our internal and external customers with the highest level of support, regardless of their location. The security program at Serco begins with a strong "Security Team" that develops a clear security mission statement and is backed by strong management support and an excellent DSS partnership.

These three foundations combined create an environment in which all members of Serco understand two of our most important business licenses, our facility clearance and our Special Security Agreement (SSA). At Serco, enhancements to the overall program include internal brochures, community involvement, assisting small businesses, an information security program, security education including monthly brown bag discussions, and most important, collaborative efforts demonstrated by all departments and employees.

Preparations for our DSS security vulnerability assessment include a collaborative effort between the entire security staff and all functional departments within Serco. The key to our success has always been, "Do it right all the time and be prepared at any time." No organization wants to fail an inspection or assessment but doing it right all the time and being prepared are critical. This approach served us well when our scheduled assessment was pushed up three months, and in fact, conducted within two weeks of announcement by DSS. Despite the change in schedule and expediting of preparation efforts, we received a Superior Rating. In the end, this really means focusing on the most important goal, the protection of national security, which relates back to readiness.

Serco actively prepares for our vulnerability assessment and features a collaborative effort between the entire security staff and all functional departments within Serco.

Annually, Serco security professionals conduct two self-inspections, a peer review and a Government Security Committee (GSC) review for each cleared location. Upon completion of these assessments, a formal write-up is provided to security leadership that is used when completing a status to the Chief Executive Officer (CEO). The results are rolled up into a status report that is provided to the CEO and briefed at our quarterly GSC meetings. The status report includes all applicable items from the National Industrial Security Program Operating Manual (NISPOM) specific to a location's classified operation.

The status report is then used to develop an action item list. Action items are derived from NISPOM chapters and self-inspection program categories, formal write-ups, and our Electronic Communications Plan. Action items are then assigned to all security members with a completion date for review. This allows another staff member to review what the site facility security officer has conducted in his/her self-inspection.

The key to a successful internal review is: Plan, evaluate, correct and evaluate again. Self-inspections cannot be done in a day. It takes time to do them correctly, particularly when properly reviewing the processes and items contained in a self-inspection.

Our final process is to compile various documents requested by DSS into books. These books contain not only requested information but enhancements we feel contribute to national security and the security program.

Serco views DSS security vulnerability assessments as an opportunity to have an outside partner review our program in order to identify vulnerabilities or weaknesses, and develop a course of action to close the gaps. Since security is always a moving target because of changing threats and technologies, staying ahead of the curve, developing enhancements and then sharing them with our communities enhances the efforts of security. This approach has yielded a security posture at Serco where each member of the company takes security seriously and it is further understood by all the impacts security has in protecting our nation's secrets.

Britt Morrison
Facility Security Officer
The Boeing Company and Boeing Aerospace Operations, Inc.

I have been the facility security officer at the Boeing Company in Oklahoma City, Okla., for nearly two years and was fortunate to inherit a stellar security program. We have a team of security professionals passionate about security, at work and within the community. Our team leads the Industrial Security Awareness Council of Oklahoma and is the liaison between the intelligence community and other cleared defense contractors in Oklahoma City.

Our senior leadership is committed to security excellence and provides the security team a seat at the table to ensure it has input dealing with all pertinent site issues and daily operations of our programs. Our site is actively involved with Boeing's Enterprise Security senior leadership where our local operations and issues can be addressed at that level.

The most important factor in our success is rounded out with our partnership with DSS. Our senior industrial security representative communicates changes and enhancements to the industrial security program and is very responsive to our needs. Our security program leverages the expertise of the industrial security representative, information system security professional, and the counterintelligence representative as a normal operating rhythm.

Yolanda Estrada
Facility Security Officer
The Boeing Company

There are many aspects to creating a successful National Industrial Security Program, none more important than the other. But there's one component that is absolutely necessary and missing it will bring a halt to your program and all the hard work you've put into it. It has everything to do with communication. Communication with your colleagues, program business partners and your DSS industrial security representative is critical to the success of your program.

As defense contractors, we are required to comply with the requirements of the National Industrial Security Program Operating Manual (NISPOM). We build the processes and procedures to ensure a sound program and continue to look for ways to improve on it. Boeing has a number of process actions teams designed to collaborate and come up with best practices that are deployed throughout the enterprise. An in-depth self-inspection program resulted from such collaboration and was recognized by DSS as a major contributor to the facility's rating.

I also found that working with our program business partners on how best to meet the requirements while helping the programs meet scheduled milestones and deliverables works best when you are having the dialogue right from the start.

Talking to your DSS industrial security representative to ensure you are on the right track is a way to ensure program success. This is a great way to validate what you are doing right and perhaps identifying areas where your program could use some help. Touch base, ask questions and have an ongoing dialogue. This is the best method for building a collaborative relationship between industry and DSS. Understanding NISPOM requirements and how to implement them can ensure a successful industrial security program. Having the collaborative environment is what helped take our program above and beyond, and ultimately earned us the Cogswell.

William B. Wheat
Facility Security Officer
Northrop Grumman Corporation

I have always viewed the DSS security vulnerability assessment (SVA) process as being tantamount to my days in college preparing for a final examination. Like most young students, I found myself "cramming" before some final exams. I soon discovered that my final exam scores bore a remarkable relationship to the time invested in preparing for the exam. So, while "cramming" was better than no preparation at all, I came to realize the results were not optimum and, in the long run, did not lend itself well for retention of information. So, it goes without saying that the key to achieving a successful SVA starts well before the SVA team arrives at one's doorstep. Just like in college, "cramming" for an SVA probably will not result in a good rating.

It is safe to say that the majority of facility security officers want to achieve a Superior or Commendable rating. Before all other considerations, there must be a level of trust established between the company and DSS. Trust establishes the baseline. The next steps include planning, preparation and organization of information, followed by a professional delivery of the information.

As soon as a DSS SVA has concluded, planning for the next DSS SVA should already have commenced. For our 2013 assessment, it was our first experience with the security rating matrix. In anticipation of the new assessment methodology, I created an "enhancement" folder on my desktop that was organized into the 13 enhancement categories. Each enhancement category contained its own spreadsheet. Having a repository for such data made it simple to add data that could reasonably be interpreted as being an "enhancement." The data repository also ensured I did not forget to include an achievement worth noting. Each entry into the spreadsheet was backed up by an artifact, including emails, flyers, newsletters, briefings, training materials, reports, etc. Just prior to the actual DSS SVA, the contents of the desktop folder were transferred into hard copy format and placed into a binder that was also organized into the same 13 enhancement categories. The binder provided the SVA team with a clear and concise overview of potential enhancement considerations. This delivery method also clearly demonstrated to the DSS SVA team leader the importance our facility placed in collecting enhancement points.

Executing an honest self-assessment by your security team is critical to understanding the effectiveness of one's security program and identifying where gap(s) may exist. If a company has the capability, a secondary self-assessment by a third party (e.g., corporate/enterprise level team) provides an ideal opportunity for another set of "eyes" to see what the local company team might have missed. The self-assessment results are then documented in a well-organized manner and delivered to DSS in a way that clearly demonstrates the facility's self-assessment process is both methodical and thorough.

Curt Armbruster
Vice President and Chief Security Officer
Logos Technologies

Logos Technologies is a relatively small company, however, the objectives we set for achieving outstanding security are no less rigorous than those set at larger businesses. In fact, because of the agility our size provides us, we have been able to implement sustainable practices across our entire workforce, in every facility.

To successfully bring our security program to its current level of excellence we focused on three areas: management support, security education and awareness, and systems security.

We started at the top by making it a priority to obtain senior management support for our security initiatives. As a result, we sent a clear message to all employees and customers that we take the issue very seriously. Our strategy to reinforce this commitment throughout our operations and company structure included:

- Making the Logos Technologies Security Director a direct report to the Chief Executive Officer (CEO) and a member of the company's corporate leadership team;
- Adding a CEO update to our annual online refresher training in which he re-emphasizes the importance of security;
- Including our CEO in all DSS review in-briefs and exit briefings.

We also created a security conscious staff. An educated staff is essential to executing a successful security program. After interviewing several randomly selected Logos Technologies employees, DSS was impressed by our employees' knowledge of security requirements and protocols. In fact, by responding to many of the questions with, "I would report that to Security," employees demonstrated that they were comfortable with and knowledgeable of our security structure and protocols. We were able to achieve this level of cooperation by ensuring that our facility security officers (FSO) and their staff are an integrated part of the general employee population.

Our employee educating initiatives included:

- Ensuring 100 percent participation in our annual refresher training;
- Hosting a counterintelligence briefing every six months;
- Encouraging reporting of suspicious contacts or solicitations.

Information systems are a challenge for a lot of FSOs. We instituted a number of steps that went beyond NISP requirements, making our systems less vulnerable and more manageable. We succeeded in strengthening our systems by:

- Proactively mitigating risks and planning for worst-case scenarios, including providing encryption and further system hardening, while maintaining a positive user experience.
- Ensuring our systems' health was maintained by generating granular reports of security, the system and computer audit logs.
- Keeping our security staff, including our information security systems manager, up to date with the latest training and certifications.

A continued focus on these core areas coupled with a strong partnership with our DSS industrial representative provided Logos Technologies with increased security and elevated our security program to higher levels.

IN THE WORDS OF AN INDUSTRIAL SECURITY REPRESENTATIVE:

Annie Backhus, industrial security representative in Alexandria Field Office #1, recommended DRS Technologies, Inc., for the Cogswell and shepherded the facility through the process. Here are her thoughts on what makes an effective, superior security program.

How do you define a successful security program?
My definition of a successful program is one where all members of the security team and senior management are heavily dedicated and involved. In order to be successful, the facility security officer (FSO) and security team must dedicate themselves first to establishing a strong foundation for their program. This includes taking the proper training and ensuring that all basic NISPOM requirements are met. In order to accomplish this, there needs to be very specific procedures in place for all aspects of the program, including personnel clearance processing, storage, transmission, reproduction, counterintelligence, etc. These processes need to be clear, concise, and disseminated to all involved. Once the foundation is strong, time and resources can be dedicated to looking forward by asking the questions: What threats may affect our facility? How can we strengthen our procedures? These are specific to each and every facility, and must include goals that are lofty, but achievable. In order to do this, senior management must be present and supportive throughout the year, not just during the DSS security vulnerability assessments, and the facility must work closely with DSS.

What did you learn through the Cogswell nomination process — i.e. how I can better help a facility improve, how much of a challenge it is for a facility to meet the requirements, etc.
Through the nomination process, I learned how difficult it can be to implement a robust security program and achieve multiple superior ratings. However, I also noted that it is achievable, as long as all facility and DSS personnel understand the importance of and are dedicated to doing the right thing. It takes constant coordination and communication between the facility and DSS to recognize areas that need improvement and implement lasting corrective actions.

How did the facility you nominated distinguish themselves from other facilities?
DRS Technologies consistently maintains an efficient and proactive security program. The FSO has created a security team consisting of four additional personnel, each concentrating on specific elements of this facility's security program. The FSO and his security team also act as mentors to other cleared facilities within the National Industrial Security Program. This support includes sharing security education materials, counterintelligence threat information, JPAS and personnel security assistance, and foreign ownership, control, or influence mitigation implementation guidance.

Additionally, DRS transitioned from a Special Security Agreement to a Proxy Agreement. This transition required considerable time, effort and coordination between DRS, the foreign parent, and DSS, but did not have a negative impact on the security posture. The DRS security team communicated consistently with DSS and proactively completed all required items. The team was not hesitant in requesting clarification from DSS, and was therefore able to respond to requests in a timely manner. Additionally, the facility's senior management was involved before, during, and after the transition.

Finally, during this transition DRS dedicated effort towards the future of its program. The team created and started implementing a cyber-security program to anticipate and possibly prevent cyber intrusions. This program includes trend analysis by country and method of intrusion, and is shared with other DRS facilities and companies participating in the Defense Industrial Base-network.

VIRGINIA BEACH FIELD OFFICE
RECEIVES INDUSTRIAL SECURITY AWARD

The Virginia Beach Field Office was recognized at the NCMS conference and was awarded the Industrial Security Award. This award is presented to the individual or organization that improved or advanced information security procedures, practices or policies of national interest.

NCMS acknowledged the field office's voluntary efforts to promote continuing security education and training. Additionally, the field office has established an exceptional reputation for attending NCMS charter meetings. The participation of counterintelligence specialists, information system security professionals (ISSPs), industrial security representatives, and the field office chief, who have created engaging discussions focused on industrial security, has led to the increase of attendance at the meetings.

The nomination package for the award stated, "The success of many chapters within the Virginia Beach Field Office region is the result of the support of the DSS Field office. Even with their busy schedule, the staff has attended every local meeting and has volunteered time to speak as well. They attend the meetings to address all issues regarding industrial security in both an open floor and panel format. This factor has driven attendance at each meeting of over 100-plus attendees since attendees know they will be able to speak to the representatives face-to-face."

Virginia Beach ISSPs also undertook an initiative to establish an information security conference dedicated to educating information security professionals. Feedback has been very positive as it allows industrial professionals to network and receive education that would not have been possible without the DSS request to create this conference. The program is now in its fourth year.

Congratulations to Beth Whatley, field office chief, and the entire Virginia Beach Field Office!

RECOGNITION FOR A JOB WELL DONE: At the award ceremony are (from left) Dustin Sievers, ISSP, Virginia Beach Field Office; Beth Whatley, Field Office Chief, Virginia Beach Field Office; Rhonda Peyton, former NCMS President; and Bruce Rainey, FCIS, Virginia Beach Field Office.

KEVIN JONES IS FIRST DSS RECIPIENT OF PRESIDENTIAL RANK AWARD

By Nicole Graham
Office of Public and Legislative Affairs

On June 18, Deputy Secretary of Defense Ashton Carter presented Kevin Jones, Director of the Center for Development of Security Excellence (CDSE), with the Presidential Rank Award of Meritorious Executive for 2012. The Award of Meritorious Executive is the second-highest form of recognition that a DoD executive can receive. Jones received the award as the result of his sustained accomplishments leading the transformation and delivery of security education and training for the DoD security community. He is the first DSS senior executive to receive this award.

Since the creation of the Senior Executive Service (SES) in 1978, the President honors a select group of senior executives who provide exemplary service to the federal government throughout their civil service career. In order to be considered for the award, senior executives must be "strong leaders, professionals, and scientists who achieve results and consistently demonstrate strength, integrity, industry and a relentless commitment to excellence in public service."

The award recognizes measurable program results arising from the candidate's contributions. For Jones, it was his "thorough understanding of the security training environment which enabled him to facilitate the restructuring of the agency's training and education programs." In order to meet expanding mission requirements and ensure program effectiveness, he realigned DSS Security Education, Training and Awareness to the current CDSE organizational structure.

Under Jones' leadership, CDSE launched the Security Education Professional Development certification program. The program was the first of its kind to achieve national recognition. Less than a year after the deployment of this unprecedented program, more than 1,200 security professionals have received this highly-valued credential.

Jones' forethought helped CDSE adapt to a changing profession, and Jones transformed how information is delivered in order to expertly execute the mission. By ensuring that required training is always available, CDSE has created an environment that allows the industrial security workforce to be in a constant state of preparedness. Jones attributes his success to the outcome of meaningful work, supportive leadership, willing colleagues and great teamwork. "I am very appreciative of the support from my colleagues," he said. "Any success achieved by CDSE is the result of a team effort."

A senior executive may be nominated to receive one of two Presidential Rank Awards. The Distinguished Executive rank is awarded to those who have achieved sustained extraordinary accomplishment during their career. By statute, only one percent of the senior executives can receive the Distinguished Executive award in a year. The Meritorious Executive rank is awarded to those who have achieved sustained accomplishment during their career. No more than five percent of senior executives can receive the Meritorious Executive award over the course of a year.

In order to be nominated, candidates must hold a career SES appointment, be an employee of the nominating agency on the nomination deadline and have at least three years of civilian service at the SES level. The process to be considered includes being nominated by agency heads, evaluated by boards comprised of private citizens, and approved by the President. The candidates are evaluated based on their leadership and the results of their performance.

A Q&A WITH **BILL STEPHENS**, CHIEF,

William D. Stephens has been the Director of Counterintelligence (CI), Defense Security Service, since August 2009.

Prior to joining DSS, Stephens had a distinguished military career, serving in a variety of progressively responsible leadership positions as a special agent and senior field commander with the Air Force Office of Special Investigations. He has extensive practical and managerial experience in CI, both in the field as a special agent and military commander, as well as at programmatic levels, having served in a number of CI-related senior positions on the Air Staff and in the Office of the Secretary of Defense.

DSS CI identifies the threat posed by foreign intelligence services, their surrogates and other hostile entities to Department of Defense classified technologies and information resident in the cleared national industrial base. DSS CI also provides that information to U.S. Government intelligence and federal law enforcement agencies to exploit. These efforts result in the best possible picture of the threat posed to cleared industry providing situational awareness for government and industry decision makers.

How do you explain the mission of the CI directorate and how CI works within the agency's larger industrial security mission?

I use the following formula to explain our mission: Risk is a function of threat, vulnerability and value/consequence.

Though every DSS directorate participates in each element of the risk equation, the CI directorate focuses primarily on working against the threat. Field operations focuses on working vulnerabilities at facilities and the steps required to mitigate them to ensure that classified information and technology in the hands of industry is secure. Is this wall high enough? Are there holes in the wall protecting the information? CI reconciles those vulnerabilities with the identity and skill of those presenting a threat in order to provide a better picture of the challenge.

The third element is to determine the consequences and the value of the information. The consequence can be described as the consequence to the American combat capability if the United States loses the technology and/or information. The value refers to the value to our adversary if they are successful at the theft. Value and consequence are not the same. A potential adversary may place a great deal of value on possessing a particular technology, but the fact that they have that technology may be of little consequence to the United States. In other cases, there could be very grave consequences for our adversaries to possess certain technology or types of information. We, as an organization and a Department, have to know what has been stolen and what we might have to face in any conflict.

The counterintelligence career field has seen many technological advances. What are some challenges the CI directorate faces as the result of these changes?

We, CI and DSS, are facing the same challenges everyone else is facing — the information age and how rapidly information moves. Since cleared facilities are under a persistent threat from our adversaries, our challenge is the ability to quickly detect and then respond to these attacks. We want to be ahead of our adversaries and ahead of the threat. This means anticipating what they want and knowing how they will try to obtain it so we can mitigate their collection efforts. Once our adversaries are inside the fence so to speak, we are on the defensive and trying to catch them. Recognizing these challenges requires a team effort. DSS does not have the authority to conduct CI investigations, so we want to be able to put actionable information into the hands of the agencies who can act on it. In short, our biggest challenge is the information age in general, and how to recognize and deal with that challenge.

Does the "information age" help CI do its job better? Can you leverage the technology?

Technology does speed up our reporting to the investigative agencies who can act on the information. However, we have to wrap industry into our overall reporting and have them report to us quickly. To move with speed at all levels, we must retool to be able to

communicate securely. We also have to encourage industry to become risk managers. We want to ensure our industry partners have the necessary training to understand the threats to the technology and information in their possession, how vulnerable that information is to attack, how they can defend against the attacks, and the value of the information should it be lost.

During your tenure, CI developed a web-based training program to increase the awareness of potential threats against U.S. technology. How important is education or training to an effective CI program?

The key to an effective CI program within the National Industrial Security Program is better educated facility security officers and senior leaders in industry. A lot of manpower is needed to train and reach a wide audience; however, that would prevent CI from focusing on and identifying immediate threats. We established a web-based CI course, "Thwarting the Enemy," which is designed to increase awareness and understanding in industry. It's a basic course that provides valuable, fundamental training to everyone. By raising the level of awareness across the board, we can target our CI resources to where they are the most effective — those facilities that have the greatest risk, vulnerability or value.

After receiving suspicious contact reports from industry, how does the CI directorate apply any lessons learned to increase CI efforts with our industry partners?

Not only does DSS have to be a master of its own information, so does industry. We introduced company assessments where we consolidate and analyze all the reporting received from a company. CI uses this data to show industry how they are being targeted, what technology is being targeted and by whom. In some cases, the company didn't know what another branch or facility was reporting to us or that technology they held was being targeted. We have been able to very clearly articulate the threat to them. Some companies have taken this information and changed their procedures.

What was your vision for the office when you arrived and have your realized those goals?

I believe we must be the masters of our own information. By that I mean we must understand where we are, and what we face; and only then can we move against the problem. I think DSS CI is better able to understand and articulate the threat to cleared industry than when I arrived. We still don't have a complete picture, but we have the best picture. The challenge is great though and we can only give an educated guess as to the true size of the threat. We use actual industry reporting to do our analysis and then extrapolate the assessment across the entire population, but it is still a projection.

How are DSS CI's efforts collectively helping the larger intelligence community to better protect national security?

DSS provides the intelligence community with insights on our opponents they may not otherwise have. Our efforts have enabled the community to identify potential gaps in the protection of cleared industry, resulting in better defenses against potential intrusions. The reception from the community has been very positive.

The CI directorate just marked 20 years. What do you consider the office's greatest success?

I think our biggest success is acting on the instinct to become masters of our own information. We have made tremendous progress in understanding the challenges and applying the risk management equation to what we do. It depicts a clear role for understanding threat.

What's next for DSS CI?

DSS CI will continue to focus on improving our processes and technology. Motivating industry reporting, providing a better picture of threats and improving our secure communication capabilities will ensure that we are delivering uncompromised products to the warfighter.

DSS TACKLES THE CCRI CHALLENGE

By Selena Hutchinson
Office of the Designated Approving Authority

Every day, cleared industry and government agencies process vast amounts of information vital to our national security on computers connected to the Secret Internet Protocol Router Network (SIPRNet) and other government owned networks.

Loss or compromise of classified information or unauthorized access to information systems and networks can have serious national security consequences. Industry and government alike are responsible for protecting not only the information, but the information systems it resides on in a manner that makes the information available as needed in support of critical programs.

A variety of regulations, directives, and standards have been promulgated to provide guidance to ensure this national security information is properly protected. An essential ingredient in the recipe for ensuring SIPRNet systems are secure is the command cyber readiness inspection (CCRI). CCRIs are conducted at each network enclave to evaluate both the technical and physical security measures employed to protect the system and information.

DSS and the Defense Information Systems Agency (DISA) have embarked on a path to enhance security oversight of industry SIPRNet systems by leveraging DSS' existing relationship with industry. The two agencies are well on the way to completely transitioning the CCRI mission from DISA to DSS for oversight of industry sites.

DSS employees team with DISA and receive CCRI training leading to certification by the U.S. Cyber Command to fill both technical and traditional (physical) security team roles. This cooperative partnership has resulted in an efficient training program and will lead to an enhanced security posture across industry SIPRNet sites.

The CCRI is a comprehensive review of a DoD network enclave's cyber-security posture including a thorough assessment of all aspects of the site's information assurance and physical security programs. CCRI criteria are based on multiple key standards and directives including the DISA Security Technical Implementation Guides (STIG) and Chairman of the Joint Chiefs of Staff Instructions 6211.02D and 6510.01F. Sites are typically given advance notice prior to a CCRI to ensure adequate time to prepare for the inspection. Currently, teams composed of both DSS and DISA inspectors evaluate sites over a one-week period.

CCRI CHALLENGES

The DISA STIGs provide an extensive set of recommendations and checklists to ensure that all DoD cyber assets meet a minimum acceptable level of security. However, implementing the STIG checklist presents challenges for industry contractors because some of the information assurance terminology is unfamiliar. The process is also time consuming and resource intensive.

Failure to adhere to the STIG standards can have serious consequences, including disconnection from the SIPRNet and a negative impact on the associated program being supported.

DSS serves as the facilitator to interpret policy and guidance as necessary. DSS personnel also bring technical knowledge honed through the certification and accreditation process. DSS involvement has improved the security posture across industry partner sites and helped overcome challenges in the CCRI process. Specific initiatives launched at DSS include:

- **A pre-CCRI assistance program including a site visit to preview the system.** Well before the scheduled CCRI, DSS information system security professionals (ISSPs) visit the contractor site to preview the SIPRNet system to assess the security posture. The ISSP provides additional support and consultation as needed to assist in securing the system.

  In cases when significant problems are identified, the regional designated approving authority will become personally involved and will meet with both company management and the government sponsor to ensure the right level of attention is focused on the requirements for SIPRNet security controls and the upcoming CCRI.

  Based on the initial visit, DSS schedules follow-up visits to ensure actions are carried through to completion. Corrections made to the local SIPRNet node improve the local security posture and strengthen security across the larger DoD network. The goal of the DSS CCRI program is to ensure SIPRNet nodes are properly secured from the date of initial accreditation until the information system is disestablished.

- **An outreach program** was initiated to make contact with government sponsors of industry SIPRNet sites. The government sponsor of a contractor SIPRNet node plays a significant role in ongoing support and preparation for CCRIs. DSS implemented a process including personal contact with the government sponsor as soon as the

inspection appeared on the schedule. DSS explains the sponsor's critical role in support of the node and positive impact their involvement has on the outcome of a CCRI.

During the conversation, DSS answers questions, offers to meet with them, and provides individual training and guidance on the role of a government sponsor at a contractor site. Significantly improved CCRI results and positive feedback from sponsors demonstrate the value added by this step in the CCRI preparation process.

- **An aggressive, focused approach to technical training** was established with DISA, ensuring that DSS personnel are able to leverage every CCRI as a training opportunity, and ultimately obtain certification toward establishing viable CCRI teams. The relationship with DISA field security operations (FSO) has enabled DSS to efficiently schedule personnel for training. The training program is working as DISA FSO has referred other DoD offices to DSS to gain insight on how to get new team members through the training and certification process.

"THE MISSION IS HERE NOW AND WILL GROW INTO THE FUTURE."

– **Randy Riley,** *Office of the Designated Approving Authority*

To address these looming challenges and the substantial workload, DSS has made a major investment in training ISSPs and industrial security representatives to handle the new CCRI mission. "The mission is here now and will grow into the future. We've spent the past two years training and preparing our workforce to ensure success," said Randy Riley, Office of the Designated Approving Authority. "It's important to remember the CCRI is simply a checkpoint along the way and should not be viewed as a one-time only event requiring the team to secure the system. Our goal is to ensure the nodes are always CCRI-ready."

As the program evolves, DSS personnel become trained and certified, and new processes are implemented, contractor nodes received passing scores on 23 consecutive CCRIs. The scores were not only "pass," they were in the range of "excellent" to "outstanding." These scores prove that DSS is poised to overcome the challenges of this new mission with the participation and cooperation of its industry partners.

A successful outcome of a CCRI represents a strong security posture for the industry node and contributes significantly to security of the defense industrial base as a whole. A more secure network reduces vulnerabilities and reduces the potential of cyber intrusions and compromise of classified DoD data across the Global Information Grid. Partnership and cooperation are the watch words for DSS in overcoming challenges in this resource constrained environment.

FACILITY CLEARANCE SPONSORSHIP FOR A CLASSIFIED/SENSITIVE RELATIONSHIP?

Q **How does a government activity or cleared contractor sponsor the facility clearance (FCL) when the government/contractor relationship is sensitive or classified?**

An FCL is an administrative determination that, from a national security standpoint, a facility is eligible for access to classified information at the same or lower classification category as the clearance being granted.

A contractor or prospective contractor cannot apply for its own FCL. A procuring activity of the government, or cleared contractor in case of a subcontract, may sponsor the FCL when a definite, classified procurement need has been established.

When the company will be performing on a DoD classified contract in which the classification level is at a handling caveat that DSS field personnel do not have access, the government activity or cleared contractor in the case of a subcontract, should contact the DSS Special Access Program (SAP) Division and request an FCL sponsorship via secure channels. The DSS Special Access Program Division will validate the need for the FCL with the government activity and sponsor the FCL.

INSIDER THREAT PROGRAM LEVERAGES AGENCY EXPERTISE

DSS recently established the Insider Threat Working Group and Insider Threat Executive Advisory Group to deter, detect and mitigate insider threat, and leverage counterintelligence, information assurance, security, and other relevant functions and resources to identify and counter the insider threat. The following questions and answers are provided to help introduce the program to DSS employees and explain how it will be implemented at DSS.

What is an Insider Threat?

Executive Order 13587, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, dated Nov. 21, 2012, defines the following:

Insider: Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks, or systems.

Insider Threat: The threat that an insider will use his/her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

Why is the insider threat important?

Historically, in most espionage cases, co-workers admitted after the fact that they noticed questionable activities but failed to report incidents to authorities because they did not want to get involved or cause problems for their co-workers. Ignoring the questionable behaviors can only increase the potential damage an insider can have on national security and industry, resulting in:

- **Loss or compromise of classified, export-controlled, or proprietary information**
- **Weapons systems cloned, destroyed or countered**
- **Loss of technological superiority**
- **Economic loss**
- **Loss of life**

How do you detect an insider threat?

Detecting potentially malicious behavior among employees with access to classified information involves gathering information from many sources and analyzing that information for clues or behaviors of concern. A single indicator may say little; however, if taken together with other indicators, a pattern of behavior may be evident. Depression, use of alcohol or drugs, stresses in personal life, financial trouble and being disgruntled with an employer are all indicators that have appeared in actual espionage cases.

These factors, combined with an employee working unusual hours, accessing information he/she didn't need to do a job, a sudden increase in wealth or improper use of an office computer system can point to someone who could pose a threat. It is important to combine multiple sources of information to determine if a situation deserves closer scrutiny or should be formally brought to the attention of the Insider Threat Working Group. It could also be referred to an external investigative or administrative entity, such as the FBI or DoD Inspector General.

Is there a way to stop an insider threat?

The DSS insider threat program's goal is to deter or identify only those individuals who pose a threat to national security information. However, there is no fool-proof way to completely mitigate the insider threat. One way to increase the odds of detecting an insider threat is to examine information regarding suspicious or anomalous behavior of those employees with access to classified information. For example, an agency may have monitoring capabilities that identify inappropriate employee activity on a classified network, which trigger a

"red flag," or an alert. That may lead to further analysis of the employee's behavior and the discovery of additional flags. Analyzing those flags and/or anomalies may reveal a behavior pattern of serious concern.

DSS' insider threat program also seeks to better educate the work force about what types of behavior might be consistent with a malicious insider and to know, should they see it in another employee, how to report such behavior.

What harm can someone do to our government based on the release of unauthorized classified information?

The reason information is classified is to restrict the information to only those who require it to support our national security objectives. Classified information, by definition, is information that, if publicly available, can cause a level of damage to the nation's security and put the lives of American warfighters in danger. For example, the unauthorized release of classified information could: provide details about weapons systems we rely on to defend our country; expose our overseas intelligence operations and personnel; and identify critical vulnerabilities in the U.S. national infrastructure which, if exploited, could damage internal U.S. defense, transportation, health and/or communications capabilities.

Reportable Behaviors

Each employee has a responsibility to ensure the protection of classified information. The behaviors listed below may indicate an insider threat and should be reported to the Insider Threat Working Group.

- **Keeping classified materials in an unauthorized location**
- **Attempting to access sensitive information without authorization**
- **Obtaining access to sensitive information inconsistent with present duty requirements and need to know**
- **Using an unclassified medium to transmit classified materials**
- **Discussing classified materials on a non-secure telephone**
- **Removing classification markings from documents**
- **Repeated or un-required work outside of normal duty hours**
- **Sudden reversal of financial situation or a sudden repayment of large debts or loans**
- **Attempting to conceal foreign travel**
- **Questionable downloads of files on removal media (thumb drives, CDs, etc)**

The Insider Threat Working Group is working to deter, detect and mitigate the insider threat, with the goal of minimizing any potential damage an insider can have on national security.

INCREASING JOINT DUTY ASSIGNMENT AWARENESS

In June, DSS hosted a Joint Duty Assignment (JDA) Information Exchange at the Russell-Knox Building in Quantico, Va. The goal of the event, spearheaded by the DSS Human Capital Management Office, was to increase awareness of the Joint Duty Program and highlight the opportunities for career and professional development that joint duty offers.

Russell Knox houses elements of DSS, the Defense Intelligence Agency, Naval Criminal Investigative Service (NCIS), Army Criminal Investigative Command (CID), and the Air Force Office of Special Investigations. Also nearby are the National Geospatial-Intelligence Agency, Marine Corps Intelligence Activity and Defense Threat Reduction Agency.

All expressed interest in creating and supporting JDA opportunities through "job swaps" that will enable intelligence professionals to understand the importance of collaboration and apply those best practices to their home agencies upon their return. Most sent representatives with just over 100 interested employees attending.

The keynote speaker was Marilyn Hudson, lead and resident expert of the intelligence community joint duty program in the Office of the Under Secretary of Defense for Intelligence. Hudson previously led this program at the Office of the Director of National Intelligence. Hudson provided details on the background, value, and application process for the program. She also shared the career and professional development benefits of participating in a JDA and then opened the floor to questions.

Additional speakers included Rebecca Allen, DSS Chief of Staff; Michael Rich, NCIS Career Program Manager; and Dan Quinn, Army CID Chief of Staff. Each speaker provided an overview of their agency's mission and the career fields they are considering for this JDA initiative.

In addition to the speakers, each participating agency staffed an information booth, similar to a career fair, and provided informational material about their organization and available JDA opportunities. This setting allowed participants to speak with agency representatives and gather additional information before leaving the event.

With standing room only attendance, the event was considered a resounding success and has paved the way for new JDA opportunities that will greatly enhance DSS employees and the DSS mission.

OVERDUE PERIODIC REINVESTIGATION?

FACILITY CLEARANCE BRANCH WORKS TO MITIGATE RISKS

Note: *At the time of publication, due to a funding shortfall in the FY13 Personnel Security Investigations for Industry Program budget, DSS suspended submission of most Top Secret PRs for cleared industry to the Office of Personnel Management effective June 14, 2013 through Sept. 30, 2013.*

By Jeremy Hargis
Facility Clearance Branch, Industrial Security Field Operations

The key management personnel (KMP) of a company are at the forefront of the decision and management process, and can impact the course of a company. DSS identifies KMPs who are required to be cleared in connection with the facility clearance (FCL) due to their level of control and influence within the company.

Recently, the Facility Clearance branch (FCB) renewed its focus and dedicated significant manpower to mitigating vulnerabilities associated with KMPs who were overdue for a periodic reinvestigation (PR). The consequences of KMP not submitting the required PR could lead to a loss of personnel security clearance eligibility and have an adverse effect on the facility's clearance. Contractor employees accessing classified information without an in-scope investigation are a risk to classified information and national security as a whole. The priority for FCB is to identify and mitigate these critical vulnerabilities in a timely manner.

In early 2012, FCB and the Quality Assurance office (QAO) began compiling data on contractors identified in the Industrial Security Facilities Database as required to be cleared in conjunction with the FCL. With the assistance of the then-Defense Industrial Security Clearance Office, the data was merged with contractors identified in the Joint Personnel Adjudication System (JPAS) as KMPs.

The resulting analysis identified 1,000 KMPs who were overdue for their required PR. FCB identified the KMP, notified the responsible field office and coordinated the submission of the overdue PR. Today, FCB, regional staff, and industrial security representatives have successfully mitigated over 2,000 vulnerabilities and potential risks to classified information.

The team comprised of FCB, QAO and the Personnel Security Management Office for Industry (PSMO-I) continue to identify and mitigate KMPs overdue for a PR every 60-90 days. The mitigation of this critical vulnerability led to numerous other actions and identification of security related issues in the past year, to include:

- **6 FCL invalidations;**
- **75 FCL terminations;**
- **125 KMP change conditions;**
- **Identification of JPAS records with no servicing or owning Security Management Office (SMO);**
- **Visibility of facilities with no JPAS access; and,**
- **KMPs not accurately identified in JPAS with the correct category classification.**

A contractor accessing classified information is required to submit a PR per National Industrial Security Program Operating Manual (NISPOM), paragraph 2-201d, which states that contractors may be subject to a PR program as specified by the Cognizant Security Authority. Currently, contractors with access at the Top Secret level are required to complete a PR every five years from the closing date of the previous investigation *(Please see note regarding current policy regarding submission of TS PRs).*

Contractors with access at the Secret level are required to complete a PR every 10 years. Given that these dates are reflected in JPAS, and NISPOM paragraph 2-200b requires that contractors maintain the accuracy of their employees' access records, facility security officers are responsible for submitting SF-86 forms through the Electronic Questionnaires for Investigations Processing system for a contractor's PR no later than the applicable due date.

Currently, PSMO-I monitors compliance with PR submission requirements, runs monthly reports of overdue PRs and requests e-QIPs for the PRs. If the contractor's SF-86 for a PR is not submitted within 30 days from issuance of the overdue notification, PSMO-I may administratively withdraw the eligibility from JPAS and issue a No Determination Made.

For individuals with no owning SMO identified in JPAS, PSMO-I may enter a Loss of Jurisdiction. Loss of a KMP's eligibility has an adverse effect on the FCL, and DSS is responsible for ensuring each cleared facility has a valid FCL in order to perform on a classified contract.

In conclusion, vulnerability identification and mitigation is the top priority in the protection of classified information. The value of mitigating this vulnerability is the strengthening of the Defense Industrial Base. Conversely, inaction may lead to the potential compromise of classified information.

Deciphering the acronyms associated with the National Industrial Security Program (NISP) can be a challenge. To help understand the acronyms, as well as the agencies that are part of the NISP in this edition, we introduce the acronym "CSA".

What is a CSA?

A CSA is a Cognizant Security Agency and are the Executive Branch departments and agencies authorized in Executive Order 12829, "National Industrial Security Program," to establish industrial security programs. The agencies identified as CSAs are the Department of Defense, the Department of Energy, the Nuclear Regulatory Commission, and the Office of the Director of National Intelligence.

What are their responsibilities?

CSAs conduct oversight of contractor security programs and provide support to ensure contractor compliance with the requirements of the National Industrial Security Program Operating Manual (NISPOM), in order to protect classified information. The CSAs inspect and monitor contractors, licensees, and grantees who require or will require access to, or who store or will store classified information, and determine eligibility for access to classified information. Each contractor has only one CSA. The type of classified material related to the contract and its preponderance determines which CSA provides oversight of the contractors under the NISP.

The Secretary of Defense has the authority to issue, after consultation with affected agencies, standard forms or other standardization that will promote the implementation of the NISP. This includes maintaining the NISPOM.

Executive Branch agencies who are not CSAs have signed agreements with DoD to provide industrial security services. These agencies include:

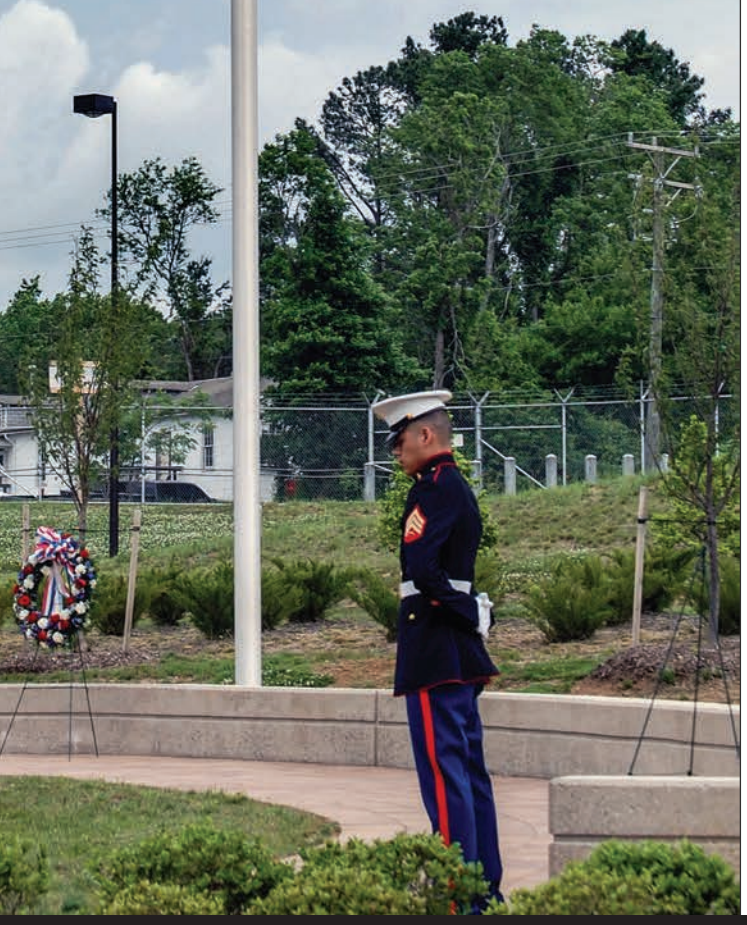
- **National Aeronautics and Space Administration**
- **General Services Administration**
- **Small Business Administration**
- **Department of the Treasury**
- **Department of the Interior**
- **Department of Labor**
- **Department of Justice**
- **Government Accountability Office**
- **United States International Trade Commission**
- **Nuclear Regulatory Commission**
- **Department of Health and Human Services**
- **Federal Communications Commission**
- **National Archives and Records Administration**
- **Department of Commerce**
- **Department of State**
- **National Science Foundation**
- **Department of Transportation**
- **Department of Agriculture**
- **Environmental Protection Agency**
- **Federal Reserve System**
- **United States Trade Representative**
- **United States Agency for International Development**
- **Department of Education**
- **Department of Homeland Security**
- **Office of Personnel Management**
- **Overseas Private Investment Corporation**

The Director of National Intelligence retains authority over access to intelligence sources and methods, including sensitive compartmented information. The Secretary of Energy and the Nuclear Regulatory Commission retain authority over access to information under their respective programs classified under the Atomic Energy Act of 1954.

While each of the CSAs have a unique role over the type of classified material and classified programs under their cognizance, they collectively support the overall goal of the NISP to serve as a single, integrated, cohesive industrial security program to protect classified information and to preserve our nation's economic and technological interests.

DSS REMEMBERS

Spring brought a season of remembrance to the Defense Security Service with a number of events remembering DSS employees as well as servicemen and women who lost their lives in defense of the United States.



MEMORIAL DAY

Stan Sims, DSS Director, led the Russell-Knox observance of Memorial Day with a wreath-laying ceremony on May 23. The ceremony continued a tradition started last year, with invitations extended to the entire Russell-Knox workforce.

Participating and offering remarks were Mark Ridley, Acting Director, Naval Criminal Investigative Service (NCIS); Coleen Kalina, Chief, Office of Counterintelligence, Defense Intelligence Agency; Jeffrey Specht, Executive Director, Air Force Office of Special Investigations; and, Army Col. Timothy Chmura, Deputy Commander, Army Criminal Investigation Command. Also participating was Gracie Thomas of NCIS who delivered a stunning rendition of "America the Beautiful." In his remarks Sims said, "This simple ceremony is acknowledgement that we have not forgotten the meaning and traditions of Memorial Day. We here at the Russell-Knox Building, we remember.

"The wreath that we will lay at the base of the American flag today is part of a national tradition of remembrance. The wreath symbolizes the eternal spirit of our nation's heroes; it is a visible and public acknowledgement of their service and legacy," Sims added.

Adding solemnity to the ceremony were Marine Corps Sgt. Miguel Sandoval and Lance Cpl. Michael Noyes, who served as the honor guard and assisted Sims in placing the wreath, and Marine Corps Cpl. Kyle Gould who rendered "Taps."

TOP: DSS Director Stan Sims, with Sgt. Miguel Sandoval, lays a wreath honoring those who served the country. **LEFT:** Sergeant Sandoval observes a moment of silence.

The Field of Empty Chairs, in the Oklahoma City National Memorial, are adorned with flowers and other items of remembrance.

OKLAHOMA CITY

Rebecca Allen, Chief of Staff, represented DSS at the 18th Anniversary Remembrance Ceremony of the bombing of the Alfred P. Murrah Federal Building in Oklahoma City. Allen attended the ceremony and met with family members of the five employees of the Defense Investigative Service (DIS) killed in the blast.

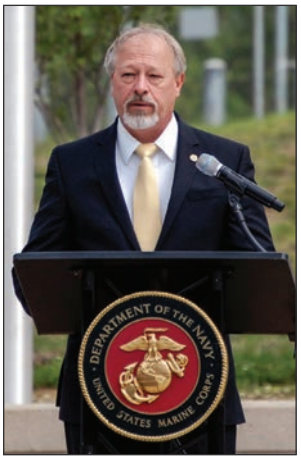
An unseasonably cold morning on April 19 drove the ceremony indoors to the First United Methodist Church, located across the street from the site of the building and memorial. The church provided an intimate setting for attendees whose focus was on not only the Oklahoma City victims and their families but also those killed and injured just a few days earlier at the Boston Marathon.

Gary Pierson, chairman of the Oklahoma City National Memorial Foundation, said, "... It is crucial that we continue what we started here over 18 years ago — overcoming evil with goodness, replacing fear with courage and helping others to move from despair to hope."

Mary Fallin, Governor of Oklahoma, reminded the audience that "light always chases away the darkness. Our thoughts and prayers are with the victims of the Boston Marathon." Rep. James Lankford reiterated that theme and stated that the day was about people and families, not places or events.

In keeping with the annual tradition, the names of the 168 who died in the blast were read with mentions of "my mother," "my sister," "my aunt," "my brother," "my son" and "my dad" included. Vickie Lykins, daughter of DIS Executive Secretary Norma "Jean" Johnson, read the names of the five DIS employees killed — Harley Richard Cottingham, Peter L. DeMaster, Johnson, Larry L. Turner and Robert G. Westberry.

Following the ceremony the approximately 1,000 attendees visited the Field of Empty Chairs adorned with flowers and other items of remembrance.



Michael Shydlinski honors five fallen DSS employees.

POLICE WEEK

The Air Force Office of Special Investigations (AFOSI) led the Russell-Knox community in a building-wide recognition of Police Week on May 13. President John F. Kennedy signed a proclamation in 1962 designating May 15 as Peace Officers Memorial Day and the week in which that date falls as Police Week. The nationwide observance recognizes the federal, state and municipal officers who have been killed or disabled in the line of duty.

Air Force Brig. Gen. Kevin Jacobsen, Commander, AFOSI, hosted the event, which included Army Maj. Gen. David Quantock, Commanding General, Army Criminal Investigation Command; Sam Worth, Principal Executive Assistant Director, Naval Criminal Investigative Service; and Rebecca Allen of DSS laying wreaths at their respective flags in honor of their fallen employees.

In his remarks, Jacobsen noted his desire to make the ceremony an annual event. A representative from each organization recited the names of their fallen as part of an end of watch roll call. The dates and stories of the fallen spanned decades and included Army CID Special Agent Walter Edward Snyder, who was killed in Germany in 1948 by a 17-year-old boy during an attempted prison escape. More recently, AFOSI Special Agents Thomas Crowell, David Wieger, and Nathan Schuldheiss, were killed in 2007 when their vehicle was struck by an explosive device while on assignment near Balad Air Base in Iraq.

Michael Shydlinski of DSS Counterintelligence and a former police officer, recited the names of the five DSS employees killed in Oklahoma City, all with an end of watch of April 19, 1995.

CHANGE IS INEVITABLE

Chapter 1, Section 3, of the National Industrial Security Program Operating Manual (NISPOM) outlines specific reporting criteria for cleared contractor facilities in the National Industrial Security Program.

Contractors are required to report certain events that have an impact on the status of the facility clearance (FCL), that impact the status of an employee's personnel security clearance (PCL), that affect proper safeguarding of classified information, or that indicate classified information has been lost or compromised.

WHAT TO REPORT

- **Reports pertaining to individuals**
- **Adverse information**
- **Suspicious contacts**
- **Change in cleared employee status**
- **Citizenship by naturalization**
- **Employees desiring not to perform on classified work**
- **Employees who refuse to sign the SF-312 pertaining to the facility clearance**
- **Any change in ownership, including stock transfers that affect control of the company**
- **Any change of operating name or address of the company or any of its cleared locations**
- **Any change to the information previously submitted for key management personnel (KMP)**
- **Action to terminate business or operations for any reason, imminent adjudication or reorganization in bankruptcy, or any change that might affect the validity of the FCL**
- **Any material change concerning the information previously reported by the contractor concerning foreign ownership, control, or influence (FOCI)**

The NISPOM requires that a firm's senior management official, facility security officer (FSO), and other officials determined by the cognizant security agency possess a PCL at the same level as the firm's facility clearance.

Since January 2012, DSS has discovered 18 cases where the KMP of a cleared contractor facility, who were required to be cleared in conjunction with an FCL, were uncleared or improperly cleared. The majority of these unreported changes were discovered by the DSS industrial security specialist during a security vulnerability assessment.

In one case, a company with an interim FCL had its interim clearance withdrawn when the company's senior management official's PCL was withdrawn. In a second case, a cleared contractor facility failed to submit requested documentation to DSS to mitigate a recent change in KMP as a result of a change in ownership that the company did not report.

Failure to report KMP changes can have significant consequences for a cleared contractor facility. In many of the 18 cases, companies were assigned marginal or unsatisfactory security ratings and had their FCLs invalidated or ultimately terminated.

When unreported KMP changes are discovered, government contracting activities (GCAs) are notified of the contractor's noncompliance. Compliance security vulnerability assessments may be scheduled to validate corrective actions, and administrative inquiries may be conducted to determine if unauthorized access to classified information occurred. Additionally, companies may have to appoint an alternate KMP or execute a temporary exclusion resolution to become compliant.

INVALIDATION

An invalidation of an FCL is an interim measure DSS takes to allow a cleared contractor to correct circumstances that negate the integrity of the contractor's security program or that have the potential for compromise of classified information. Invalidation renders the company ineligible to receive new classified material

or to bid on new classified contracts unless the GCA determines and certifies compelling reasons exist to issue a new classified contract or allow additional access to classified information.

DID YOU KNOW?

A benefit to having an alternate JPAS account user is to ensure a cleared contractor maintains uninterrupted JPAS access after the departure of a KMP. In addition to reporting KMP changes to your DSS industrial security specialist, cleared contractor facilities have the ability to remove and assign KMP designations in JPAS. This is done using the "Category" function on the "Display/Maintain Person" screen in JPAS.

HOW TO REPORT

Once aware of a company or organizational change required to be reported to DSS, the FSO should contact the company's industrial security specialist. The change will be noted, and the FSO will be instructed to submit all necessary documentation in an Electronic Facility Clearance System (e-FCL) package. If a company does not have an e-FCL account, the industrial security specialist will register the company for an account.

REMEMBER THESE STEPS

Contact DSS

Submit an e-FCL package

Remove and assign KMP designations in JPAS

TRAINING AVAILABLE

The Center for Development of Security Excellence provides an 85-minute course on NISP Reporting Requirements (IS150.16). This course introduces the reporting requirements that are outlined in NISPOM 1-300.

Additionally, the course discusses the reporting requirements for changed conditions affecting the FCL, PCL, and safeguarding; as well as reports for security violations and espionage, sabotage, terrorism and subversive activities. The course examines the typical reporting procedures and the potential impact on the contractor's overall security program. The significance of reporting KMP changes is discussed at length in this course. A course overview and registration information can be found at: www.cdse.edu/catalog/elearning/IS150.html.

BRAIN DRAIN & THE HUGUENOT EXODUS

By Charles Zakaib, *Counterintelligence Directorate*

A well-educated, experienced work force is important to any country's industrial base. A loss of core competencies within that work force, commonly referred to as "brain drain," can significantly degrade a country's competitive advantage.

Such was the case for 17th century France, which suffered a significant brain drain in commerce, culture, and industry in the wake of King Louis XIV's persecution of the Huguenots.

The Huguenots were French Protestants, a product of the broader Protestant Reformation that swept Europe and roiled Catholic governments beginning in the early 1500s. The Huguenots came from a broad cross-section of society that included a great number of middle-class professionals, such as tradesmen, craftsmen, intellectuals, and artisans. Also among them were noblemen and citizens of wealth and stature. Those societal connections allowed for some governmental leniency at first. Nevertheless, France remained a predominantly Catholic country and it steadily increased the restrictions on Huguenot practices and rights.

In 1598, after a series of religious wars, the Huguenots gained some liberties through the Edict of Nantes, issued by the erstwhile Huguenot Henry IV. Despite this victory, Huguenot freedoms again eroded. By 1661, Henry's grandson, Louis XIV, had begun to increase pressure on the Huguenots to convert to Catholicism. Many noble and upper-class Huguenots did convert, thereby further reducing the restraint of the government.

Eventually, in 1685, Louis convinced himself that the Huguenots were no longer a significant portion of the population, and thus he could persecute the remainder without much effect. So he issued the Edict of Fontainebleau, which revoked the Huguenot freedoms enshrined in the Edict of Nantes. To Louis' surprise, his act spurred one of the greatest migrations in European history.

In the years following Louis XIV's act of revocation, at least 200,000 Huguenots of all classes fled France rather than convert to Catholicism or submit to persecution. On the whole, the Huguenot émigrés were better educated and engaged in more skilled trades and professions than the average Frenchman. This rapid and large emigration of skilled citizens reduced France's competitive advantage vis-à-vis other European powers. As 20th century author Esther Forbes put it: "France had opened her own veins and spilt her best blood when she drained herself of her Huguenots, and everywhere, in every country that would receive them, this amazing strain acted as a yeast."

Indeed, many governments were eager to accept Huguenots in order to take advantage of their technological knowledge and skills. One oft-studied example is that of Brandenburg-Prussia. Soon after Louis XIV's edict, Frederick William, leader of Brandenburg-Prussia, issued the Edict of Potsdam, which granted support and privileges to Huguenot immigrants. As they settled in Berlin, Potsdam, and elsewhere, the French Protestants established factories and spread their unique knowledge of ceramics, gold and silver crafts, and especially textiles such as silk, velvet, and cotton.

At the time, German territories were rebuilding from the ravages of the Thirty Years' War and the latest outbreak of the plague. The influx of skilled Huguenots sped their revival and decreased the economic and cultural imbalance with France. In fact, 18th century scholar Johann Bekmann listed 46 professions established by Huguenots in Brandenburg that previously had not existed there. All told, between 16,000 and 20,000 Huguenots immigrated to Brandenburg-Prussia, with Berlin alone receiving nearly 5,000, almost 20 percent of its population.

Huguenot émigrés also had an impact on the military affairs of Europe. William of Orange, leader of the Protestant Dutch, eagerly recruited expert Huguenot shipwrights, soldiers, and sailors — representing critically important military skills — into his forces for his cross-channel invasion of England. Once there, they handily overran a Catholic ally of Louis XIV, James II, during the so-called Glorious Revolution of 1688. Later, William would again benefit from Huguenot manpower and know-how as French Protestants in Ireland joined him in his suppression of James' remaining strongholds there.

As for France, the Huguenot exodus, while not debilitating, did injure its position in Europe. Even

Louis XIV's military adviser and engineer, Sébastien Le Prestre de Vauban, was dismayed at his country's unforced error. The Revocation, he remarked, led to "the exportation of 60,000,000 livres ($12,000,000), the ruin of commerce; enemies' fleets were reinforced by 9,000 sailors, the best in the kingdom, and foreign armies by 600 officers and 1,200 men, more inured to war than their own."

The story of the Huguenots reminds us that proprietary knowledge and the competitive advantage it imparts are fragile yet critical assets. Fortunately, the United States has usually been the beneficiary of other countries' errors. Samuel Slater emigrated from Britain and founded America's industrial revolution. Albert Einstein, Wernher von Braun, and Igor Sikorsky all contributed mightily to U.S. defense technology.

So, while we protect what we have, we should always remember that, as Frederick William demonstrated, one country's loss can be another's gain. And, while machines and technologies themselves are important assets, so are brains and the knowledge and know-how they contain.

PARTNERSHIP WITH INDUSTRY: A FIRST-PERSON ACCOUNT

By Stefanie Valero
Industrial Policy and Programs

As a recent participant in the Partnership with Industry (PWI) program, my level of awareness of the issues faced by industry has greatly increased. Since witnessing industry's efforts in meeting National Industrial Security Program requirements, I am now better able to apply this knowledge to my current position within the DSS Foreign Ownership, Control, or Influence Operations Division.

The PWI provides an opportunity for industry and DSS industrial security professionals to "walk a mile" in each other's shoes. The goal of the program is for participants to gain a mutual understanding of their respective roles in industrial security, and to develop a better understanding and appreciation for the challenges and obstacles faced on both sides. The DSS participant spends four days onsite at a large cleared facility and one optional day onsite at a small or medium cleared facility.

Going into the PWI program, I expected to learn about the daily operations of the company; however, I didn't realize it would be so hands on. During my time, I assisted in two closed area self-inspections, and was able to provide recommendations and guidance to several individuals of the company's security team.

I participated in several tours throughout the company complex, and was involved in numerous 'meet and greet' sessions with a variety of employees. Of note was the collaboration center where an innovative network of different companies come together to enhance products to meet the warfighters' desired specifications. The corporate director of security provided a company overview briefing, which was very enlightening.

In talking with a program manager, I learned of the challenges associated with implementing a program in another country where the local people are protesting the placement of equipment due to perceived long-term health risks. At an insider threat/cybersecurity briefing, the company outlined real-life instances where suspicious employees were uncovered and then turned over to the Federal Bureau of Investigation for further investigation.

Also, several suspicious packages came into the shipping/receiving center, to include several magazines containing Microsoft hot spots. The security team was concerned that employees would plug the hot spots into the company computers, allowing for unauthorized network access by an outsider. However, the security team validated there was no suspicious intent.

I met with the International Traffic in Arms Regulations director and learned about the evolving challenges that industry faces complying with the Department of State/ Directorate of Defense Trade Controls regulations. Many more topics were covered during the week, to include learning how communications security (COMSEC) keys are processed which gave me a more informed viewpoint when processing COMSEC National Interest Determinations, as a part of my duties at DSS.

Participating in the PWI program gave me personal satisfaction to experience firsthand the partnership that DSS and industry have formed to protect classified information and technologies while providing the warfighter a competitive edge.

ST. LOUIS FIELD OFFICE: A DYNAMIC TEAM PERFORMING A DYNAMIC MISSION

It was all about teamwork, fiscal responsibility, motivation and productivity during the St. Louis Field Office all-hands meeting in Downers Grove, Ill., in March 2013. Though the agenda was compressed, the combined training and team-building event featured open and honest discussions centered on process improvement, revalidating priorities and fostering improved internal field office partnerships.

With all assigned industrial security representatives (ISR) and information system security specialists (ISSP) personnel coming from Wisconsin, Minnesota and St. Louis, the team gathered the first day with brief introductions of new team members, Larry Pyles and Charity Fuehne. Jennifer Andrews was recognized as the St. Louis' nominee to the region for employee of the quarter, and Salvatore Urbano and Paul Stalvig were recognized for completing the Northern Region's leadership development program.

Pat Kimball, Northern Region resource manager, provided training on equipment and supply ordering, proper use of government resources, and an overview of the do's and don'ts of the Defense Travel System. Heather Sims, St. Louis field office chief, followed with a review of topics from the supervisors' conference and Industrial Security Field Operation's FY13 priorities.

The team then discussed the current state, future state and perfect state snapshots of field office/individual goals and accomplishments. During a working lunch, the team further discussed DSS issues and challenges by answering questions, such as, "Why are you here at DSS?", "What can I contribute to the agency?", and "Why does the agency exist?"

After lunch, briefings included an overview of the security violation process by Kerry Waldrip, and an update on Arms, Ammunitions and Explosives from Brant Miederhoff. Urbano covered the Field Office foreign ownership, control or influence

Attendees of the St. Louis Field Office all-hands meeting participate in a team building exercise.

(FOCI) procedures for all FOCI signatory companies. He shared best practices with the office and showed the effectiveness of having one ISR with an alternate as the focal point for continuity and successful follow-through. Sims concluded the day's events with an open discussion of general reminders, quality assurance trends, supervisor ride-along schedules, certification and accreditation, Command Cyber Readiness Inspections, and individual project assignments.

The following day, Thomas Jessen from the International Branch gave a presentation on the role of the designated government representative and the responsibilities of the empowered official. Jennifer Andrews then provided a hands-on demonstration on the use and benefits of the security vulnerability assessment tool.

Visiting ISRs assisted the Downers Grove resident office personnel with overdue assessments, by conducting security vulnerability assessments or assisting with report writing. Gary Sims provided his new ISSPs with just-in-time training.

The value of an all-hands meeting can sometimes be difficult to measure, but in this case, every attendee gleaned new focus, team confidence, and great collaboration.

CHANTILLY FIELD OFFICE HOLDS OPEN HOUSE FOR INDUSTRY

The Chantilly Field Office recently held an open house for cleared contractors supported by the two field offices. More than 350 attendees came out on a rainy day to meet DSS representatives. The attendees were representative of a cross section of the cleared industrial base from companies such as MITRE, General Dynamics, ManTech, Lockheed Martin, Northrop Grumman, CACI, Rolls Royce, Kaseman, CGI Federal, ICF, Logistics Management Institute, Delex, DRS, Juniper, Knowcean and several others. Representatives from the Defense Intelligence Agency also attended. Overall the event was considered a great success with positive comments concerning partnership and assistance from DSS, and a request to hold the event annually.

ATLANTA FIELD OFFICE SUPPORTS CAREER DAY

Susan Parker, industrial security specialist from the Atlanta Field Office, recently participated in the annual Career Day at Compton Elementary School, Powder Springs, Ga. She created a visual display and "told the DSS story" in sessions with 3rd through 5th graders, providing a brief glimpse into the world of industrial security. The presentation was interactive, sparking several questions, and was so successful the principal invited Parker to participate in future Career Days.

RESIDENT OFFICES IN HAWAII, ALASKA OVERCOME GEOGRAPHIC CHALLENGES

When accomplishing the DSS mission, it's not unusual for the personnel assigned to field offices located throughout the United States to travel to facilities to conduct assessments.

However, the DSS personnel assigned to Alaska and Hawaii have to deal with weather, remote locations, and crossing the international date line in day-to-day duties.

With responsibility for covering more than 150 facilities, Matthew Gail, an industrial security representative in the Alaska resident office, finds it challenging once he leaves the Anchorage city limits. "While it is civilized in the Anchorage area, once you are in 'the bush', i.e., Fairbanks or Delta Junction for example, it gets a little more complicated," he said. "Some of my facilities in Fairbanks are in remote areas, and I have to be ready to deal with whatever happens, from moose in the road to extreme weather.

"The main challenge is distance," Gail continued. "Alaska is so big that Texas can fit inside it no problem. My facilities range from Delta Junction, where the facility's address is just a mile marker on the Alaskan Highway, down to Juneau and Sitka. As a matter of fact, I have a few facilities that when I visit them, I have to travel via float plane as there are no roads — only a small port and an airfield!"

Lisa Dearmin, an industrial security representative in the Hawaii resident office, can understand the challenge of distance. "The Hawaii resident office is required to travel to outer lying Hawaiian Islands and Guam throughout the year and sometimes for immediate needs, so we don't have the luxury of jumping in our GSA vehicles to travel to all 150 defense contractors we serve," Dearmin said, noting that "Guam is almost an eight hour flight from Honolulu and it involves crossing the international date line."

It's those geographical challenges that make working in these two offices unique and require industrial security representatives to be a jack of all trades.

"Because we are a geographically isolated resident office, we are almost entirely self-sufficient," Dearmin explained. "The Hawaii resident office provides a great deal of liaison and relationship building and maintenance with other federal agencies and government contracting agencies."

In addition to her duties as an industrial security representative, Dearmin notes there is no on-site information system security professional (ISSP) or field counterintelligence (CI) specialist, "so we are required to provide basic level CI and ISSP support."

"Up here in Alaska, the DSS rep literally has to be the jack of all trades and master of all since we have to answer a wide range of questions and issues, some of which pertain to the Alaska Native Corporation Act," Gail added. "Alaska is a major challenge to work in and every day is different. The winter months can be especially hard to accomplish our mission as I am basically covering all of my Anchorage facilities, which number over 100, but even then travel can be difficult."

Despite the geographic distance of these offices from the continental United States, neither resident office feels isolated from DSS. Technology keeps them connected, and both are quick to acknowledge the support they receive from the Tacoma field office and the field office chief, Darrin Slovanick.

TAKE OUR DAUGHTERS & SONS TO WORK DAY

DSS WELCOMES ALMOST 50 CHILDREN TO THE ANNUAL EVENT

By Nicole Graham
Office of Public and Legislative Affairs

On April 25, tenants of the Russell-Knox Building (RKB), Quantico, Va., hosted about 350 children for "Take Our Daughters and Sons to Work Day." A total of 49 daughters, sons, grandchildren, nieces and nephews of DSS employees attended the day-long event.

The program, originally called "Take Our Daughters to Work" was founded in 1993 by Gloria Steinem and the Ms. Foundation for Women to promote interest in career exploration. In 2003, the day was officially expanded to include boys.

For DSS children, the day began with a welcome by DSS Chief of Staff Rebecca Allen, who provided on overview of the agency and the collaborative components of RKB. She said she was excited to have everyone there for the day, and encouraged the children to have fun and ask a lot of questions. Her enthusiasm inspired the children to do just that which led to an impromptu question and answer period.

A joint opening ceremony was next on the agenda and included employees and children from DSS, the Defense Intelligence Agency (DIA) and Army Criminal Investigation Command (CID). DSS children — Abraham Richard, Amariya Davis-Landfair and Catherine Liu — volunteered to lead the group in singing the National Anthem and reciting the Pledge of Allegiance.

In the morning, DSS, DIA and CID coordinated on a wide range of activities that focused on teamwork, togetherness and collaboration. David Bauer, the assistant director of the DSS Counterintelligence operations division, led a program for the children on investigations. Other activities included demonstrations and sessions on polygraphs, criminal forensics, Human Intelligence (HUMINT), imagery devices, digital forensics, and operations and internet safety.

The activities were designed to provide the children with insight into the day-to-day operations of the investigative agencies. Brendan Layser especially enjoyed the HUMINT presentation of the day and said he may like to join the field after he finishes his education.

All of the children enjoyed the DSS activity entitled "Who We Are." Volunteers from across the agency — Selena Hutchinson, Timothy Harrison, Jason Benitez, Eric Coates, Shannon Sylvester, Dwayne Pierce and David Scott — put together an interesting and engaging program that focused on the DSS mission.

During the program, the children helped find spies around the classroom, conducted security interviews, and had their fingerprints taken. Hannah Kim said the activities and presentations taught her that DSS is working to keep the country safe.

After lunch, the children and their parents spent a beautiful afternoon outside watching a martial arts performance by the Marine Corps, military K-9 exercises and parachute demonstrations. The activities let the children participate in hands on experiences including trying self-defense moves on each other, trying on protective gear used to train the military dogs and getting an up close view of parachute equipment and gear.

To conclude the day, DSS hosted an ice cream social for participants. The children were able to relax and discuss the events of the day with their parents and new friends. Carine Livingston said she had a great time learning new things and meeting new friends, and she can't wait to visit again!

A total of 49 daughters, sons, grandchildren, nieces and nephews of DSS employees attended Take Our Daughters And Sons To Work Day at DSS Headquarters.

DSS UNVEILS SOCIAL MEDIA SITES

LIKE US ON FACEBOOK, FOLLOW US ON TWITTER

By Nicole Graham
Office of Public and Legislative Affairs

On April 16, 2013, DSS launched a social media strategy to include the establishment of a Facebook page and a Twitter feed.

Social media has been widely used as a way to connect with other people through people you already know. However, government agencies are increasingly using social media to efficiently share information and respond to a changing media environment.

A social media plan gives DSS another avenue to reach our industry partners. DSS uses Facebook and Twitter to rapidly share dynamic information that will be useful to stakeholders. The DSS Facebook page and Twitter feed are maintained by the Office of Public and Legislative Affairs, which reviews and clears the information to ensure the release of timely, useful data that adheres to DoD's policy for public release.

DSS employees are also encouraged to follow DSS but are reminded of the following policies when establishing private social media accounts:

- **Do not post sensitive information**
- **Do not represent yourself as acting or speaking for the Department of Defense or DSS**
- **Do not use your government email address to register**
- **Department users may access social networking sites for personal use on a limited basis as long as it does not affect productivity, distract from work-related tasks or cause undue burden on department resources.**
- **Use caution when downloading, opening or responding to content on a social networking site**
- **If using a government computer, you must ensure no executable software is downloaded.**
- **Think before you post!**

Have information you would like to post on the DSS Facebook page or Twitter feed? Contact dsspa@dss.mil for more information.

DEFENSE SECURITY SERVICE