Volume 4, Issue 3 Official Magazine of the Defense Security Service

DSS

ACCESS

COGSWELL AWARD WINNERS

FALL 2015

Volume 4, Issue 3

SPOTLIGHT

INSIDE

AROUND THE REGIONS

DSS ACCESS

Published by the Defense Security Service
Public Affairs Office

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

DSS Leadership

Director
Stanley L. Sims

Deputy Director
James J. Kren

Acting Chief of Staff
La Shawn B. Kelley

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

Anyone who reads these pages knows I have made partnership with industry the cornerstone of my mission philosophy as the Director of DSS. At this point, I'm sure I'm beginning to sound like a broken record, and you are tired of hearing it. But in June, I was honored to present awards to 41 cleared facilities in recognition of their outstanding security programs. The James S. Cogswell Outstanding Industrial Security Achievement Award demonstrates that the partnership envisioned by Colonel Cogswell is indeed alive and well.

I was struck by the variety of facilities that DSS recognized this year. For the first time that we could verify, we recognized a law firm. We also recognized a facility that had received eight consecutive superior ratings, which is a stunning achievement. We recognized two major U.S. universities that face unique challenges in incorporating security into an open academic environment.

We also recognized an AA facility that just a few years ago received an unsatisfactory rating from DSS. It was only through the combined, dedicated commitment of DSS and the company's management and security staff that this facility stood on the stage to accept their award. This was a true partnership, and it was gratifying to see the results first hand.

I could go on, but I think it's more valuable for the facilities we recognized to tell their own stories. So in this issue, we asked a representative sample of this year's Cogswell winners to tell us how they were successful and how they view their partnership with DSS.

You'll notice that without fail, they cite the partnership they have with their local security professionals and DSS field office as crucial to their success. They also cite the value of security education — staying current on the latest tools designed to inform and assist them in managing their security programs — another example of our partnership in action.

My commitment to partnership is not limited to industry. We continue to reap the benefits of the partnerships we have forged with other government agencies such as the FBI and Department of Homeland Security. You can also read about those successes in this issue.

Thanks for all you do for DSS and to advance the security of our nation.

DSS Presents:

The 2015 Cogswell Awards

On June 24, 2015, the Defense Security Service presented the annual James S. Cogswell Outstanding Industrial Security Achievement Award to 41 cleared contractor facilities. The winning facilities represent the "best of the best," and their security programs stand as models for others to emulate. These 41 facilities represent less than one-tenth of one percent of the over 13,000 cleared contractors in the National Industrial Security Program (NISP).

Each year, DSS partners with NCMS to host the Cogswell Award presentations during its annual training conference. In presenting the awards, DSS Director Stan Sims said the Cogswell is presented to those companies who understand the complexity of the security environment. They go above and beyond the minimum requirements expected of them to serve as leaders in the community.

Sims noted the steady growth in the number of Cogswell recipients over the past years:

2010, *9 facilities* | **2011,** *17 facilities* | **2012,** *26 facilities* | **2013,** *24 facilities* | **2014,** *40 facilities*

He said the increased numbers show how hard it is to achieve the award and how significant the accomplishment. But the numbers also shows it's possible and that DSS is committed to the award and recognizing the deserving.

The Cogswell Award was established in 1966 in honor of the late Air Force Col. James S. Cogswell — the first chief of the unified office of Industrial Security. Cogswell articulated the underlying principle of the Industrial Security Program — the need for a true partnership between industry and government to ensure the protection of classified information, materials, and programs.

Sims said, "Partnership with industry is a principle I strongly believe in. It's a principle I have been articulating since I arrived at DSS. Now, it's part of how we do business."

Sims described the Cogswell selection process as rigorous but fair. The process begins with a DSS Industrial security representative who nominates a facility. That facility must have achieved two consecutive superior ratings just to be considered for the award. Of the 13,000-plus cleared facilities, approximately three percent receive superior ratings each year. Two consecutive superior ratings demonstrates a facility's commitment to security over time.

Once nominated, the facility enters an eight-month DSS internal review process that includes a National Review Team of DSS regional directors and representatives from across DSS who consider each nomination. The National Review Team vets all nominations with 30 external agencies and makes recommendations to DSS senior leaders for a final decision based upon the following criteria:

- Overall security program
- Senior management support
- Security vulnerability assessments
- Security education and awareness
- Facility security officer (FSO) and security staff level of experience
- Classified material controls

The 2015 award recipients include a balance of both large and small companies, including two AA facilities. AA facilities are the largest and most complex in the NISP. Sims said that due to their size, AA facilities have more opportunity for error, but also more opportunities to excel and go above and beyond the basic requirements of the program.

The 2015 winners also represent a myriad of technologies, said Sims. "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 legal support, training, logistics and engineering support."

In closing, 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. But we know and you know, companies don't create excellent programs, people do — the FSOs, the security staffs, the company leadership. Without your commitment and your dedication your company would not be here today. And it's your willingness to be a partner with DSS that we honor you as well as your achievement."

Congratulations to the winners of **The 2015 Cogswell Award**

Alliant Techsystems Operations, LLC
Plymouth, Minn.

BAE Systems Land & Armaments, LP
Santa Clara, Calif.

BAE Systems Technology Solutions & Services, Inc.
Middletown, R.I.

Batelle Colonial Place Operations
Arlington, Va.

Batelle Memorial Institute – Charlottesville Operations
Charlottesville, Va.

Charles Stark Draper Laboratory
Cambridge, Mass.

Crowell & Moring, LLP
Washington, D.C.

DCS Corporation
Shalimar, Fla.

DRS ICAS, LLC
Beavercreek, Ohio

DRS Power Technology
Fitchburg, Mass.

DRS Sensors & Targeting Systems, Inc.
Cypress, Calif.

Force 3
Crofton, Md.

General Dynamics Advanced Information Systems, Inc.
Oakton, Va.

General Dynamics C4 Systems, Inc.
Scottsdale, Ariz.

General Dynamics Information Technology
Philadelphia, Pa.

General Dynamics Information Technology
Chesapeake, Va.

Honeywell International
Golden Valley, Minn.

iGov Technologies
Tampa, Fla.

Jacobs Technology
Beavercreek, Ohio

Jacobs Technology
Tullahoma, Tenn.

L-3 Communications Integrated Systems, LP
Greenville, Texas

L-3 Systems Company
Camden, N.J.

L-3 Unidyne
Middletown, R.I.

LexisNexis Special Services, Inc.
Washington, D.C.

Lockheed Martin Corporation Information Systems & Global Solutions
Littleton, Colo.

Lockheed Martin Corporation – Mission Systems & Training
Orlando, Fla.

Lockheed Martin Corporation Missiles & Fire Control
Orlando, Fla.

Lockheed Martin Sippican
Marion, Mass.

Logistics Management Institute
Tysons, Va.

The Protective Group, Inc.
Miami Lakes, Fla.

Raytheon Company
Tucson, Ariz.

Raytheon Company
Rancho Cucamonga, Calif.

Raytheon Company
Shalimar, Fla.

Raytheon Company
Arlington, Va.

Raytheon/Lockheed Martin Javelin Joint Venture
Tucson, Ariz.

Saab Defense and Security
East Syracuse, N.Y.

Scientific Research Corp.
Atlanta, Ga.

Stanley Associates
Orange Park, Fla.

Texas A&M University
College Station, Texas

The University of Rhode Island
Kingston, R.I.

Vencore Services & Solutions, Inc.
Brook Park, Ohio

IN THEIR OWN WORDS

We invited a representative sampling of the 2015 Cogswell winners to share their formula for success with ACCESS readers. The following are tips and lessons learned from facilities with proven track records on how to establish and maintain a high-quality security posture.

by Karen Kitts
Facility Security Officer
Jacobs Technology, Beavercreek, Ohio

Jacobs Technology, Inc. is the advanced technology arm of Jacobs Engineering, one of the nation's largest engineering and technical services-only companies. With 70-plus years of experience supporting government and commercial clients, we have earned a reputation for excellence and outstanding technical and managerial achievements in quality, performance, and safety.

I am delighted to add security to that list. I have been the Facility Security Officer for the Advanced Systems Group, part of the Systems Acquisition, Logistics, Test & Training line of business, for the last 12 years managing 700-plus personnel security clearances with offices and personnel throughout the United States and outside the contiguous United States (OCONUS). When I started in the security field I made two areas a priority — education and networking.

Education Awareness and Training. People are a company's greatest asset. This is one of the Jacobs core values. People are only as good as they are trained. Well-trained employees are informed and compliant with regulations.

I provide our employees frequent training using every means of distribution possible (in-person, email, intranet, conference calls, etc.). Having employees located throughout the United States and OCONUS is a challenge and requires much of the training to be electronic.

This training is created to be interactive and engaging. Most recently, I distributed a Security Madness bracket to coincide with March Madness. Games for each bracket were replaced with general security questions. Employees tracked their progress and advanced to additional rounds as the tournament continued.

The games (questions) became increasingly difficult with each new round. Adding fun to security is an excellent way of keeping employees engaged while teaching them valuable information at the same time.

I provide in-person training monthly to our local office and travel to offices out-of-state every one to three years. These briefings may be new information or reminders of existing policies or topics that are timely and relevant. Initial and refresher training is automated so once an employee is entered into our database, the system tracks when training is due.

Last year I developed a quarterly newsletter. It is a quick, easy-to-read, one-page product that includes a variety of security–related articles and an interactive task such as a crossword puzzle, matching game, seek and find, etc.

Continuing my own security training and professionalization is an ongoing commitment and supports credibility. I achieved the Industrial Security Professional certification in 2006 and am presently preparing for the Security Fundamentals Professional Certification. I attend brown bag seminars, webinars, and courses from the Center for Development of Security Excellence to stay current with security changes and new policies.

Networking. This has proven to be the most valuable part of my career. Upon the urging of my local Industrial security representatives in my first year as an FSO, I volunteered to be the chair of our local Industrial Security Awareness Council. This is a group of FSOs and government security professionals who meet quarterly to exchange ideas, provide presentations, etc. By volunteering at an early stage in my career, I established many relationships that continue today.

Additionally, I have volunteered for several positions within our NCMS Wright Flyer Chapter and at the national NCMS seminars. This summer I will undertake the role of Mentor Chair for our local chapter. This responsibility fits well with my passion for security. I enjoy sharing ideas, best practices, lessons learned, etc., with new FSOs.

With each new mentoring relationship I am involved in, I always learn something in return. Additionally, I have had the pleasure of working with several different Industrial security representatives building strong partnerships. Having an open-door policy and being approachable and trusted by our employees has enabled them to freely discuss security concerns with me such as reporting adverse information, seeking policy clarifications, etc. All of these relationships allow an exchange of information and ideas that supports our security program.

Our office has earned 10 consecutive superior ratings from annual DSS assessments. Our policies and procedures go above and beyond the NISPOM. One of the keys to this success is organization. I maintain a facility binder to keep current copies of facility-related documentation required for assessments. Part of this binder includes documentation to support security enhancements.

Separate from the binder are electronic personnel and contract (DD254s, consultants, subcontractors, etc.) files. Having electronic files helps to locate files quickly and maintain configuration control. Keeping everything current at all times makes preparing for an assessment easier as we are always audit-ready.

Documentation of security education and training is important, both the training itself and acknowledgement of completion. Senior management support committed to security excellence is imperative. Employees are engrained in this culture from their hire date throughout their employment at Jacobs.

Jacobs' strong focus on security and the relationships fostered between DSS, our employees, our customers, and other security professionals enables us to maintain our superior program. Policies and procedures are reviewed often to determine effectiveness. We are constantly learning from our bi-annual self-inspections, annual assessments, and seeking new enhancement opportunities.

Jacobs is ready to competently adapt to the challenges that lie ahead in the field of security. Having a successful security program ultimately benefits everyone and ensures the protection of the U.S. warfighter and our nation's classified information.

IN THEIR OWN WORDS

We invited a representative sampling of the 2015 Cogswell winners to share their formula for success with ACCESS readers. The following are tips and lessons learned from facilities with proven track records on how to establish and maintain a high-quality security posture.

by Andy Lewis
Facility Security Officer
Raytheon Missile Systems, Tucson, Ariz.

For those able to attend the Cogswell presentation ceremony this past June in Las Vegas, you may remember DSS Director Stan Sims' comments about the Raytheon Missile Systems' (RMS) Tucson plant site. He shared a brief history of his organization's role when RMS started on its "March to Superior" in 2008. At the time, no one really understood what path the facility and its employees would need to take to make the necessary improvements for a superior facility.

While several of RMS' smaller locations had received superior ratings in the past, Tucson was a significantly larger campus with far more complexity and challenges. That, coupled with a history of less than satisfactory security ratings, made the task seem nearly insurmountable.

It was a partnership and open dialogue with DSS, along with the commitment of a workforce of over 12,000 employees that made our 2015 Cogswell possible.

After receiving several scores below what was considered acceptable, Dr. Taylor W. Lawrence, president of RMS, challenged the RMS security organization to raise the bar on meeting DSS requirements. Nothing short of a superior rating from DSS was acceptable. The goal could not be just passing the assessment. Instead, each of our 12,000-plus employees would have to become a part of security, creating a culture where "Living Superior" and performing at the highest levels year-round, every day and in every situation, were woven into the fabric of the business.

To do so, RMS recognized that it needed to form a new security program from both the ground up and the top down. One of the key drivers to becoming superior was having dedicated executive leadership to champion the process and make the necessary changes a priority.

Almost overnight, leaders across the business became more engaged in security, performing leadership "walkabouts," conducting security briefings, attending security fairs and events, and working closely with embedded security professionals to ensure the highest security standards at all times.

Furthermore, leadership's newfound attention to security created a peer-to-peer partnership between industry and DSS. This partnership was, and continues to be, instrumental in RMS' success in earning a superior rating. Through open, honest and transparent communications with DSS, RMS has developed a much stronger understanding of DSS' expectations regarding security and what it means to actually perform as a superior organization.

This knowledge, combined with Raytheon's Six Sigma approach to continual process improvement, corrective action and accountability tracking resulted in several innovations to our security practices. The business implemented a full-time security audit team to ensure standards put in place for the DSS assessment remained after the assessment team provided their outbrief. Additionally, multiple roles were formalized and moved into the security organization, raising the competence and professionalism to new heights.

To shift the culture, change could not just occur at leadership and security organization levels. Each employee had to make security part of his or her daily life. Through a thorough and comprehensive education and training program, employees were exposed to security messaging everywhere they looked.

From regular messaging in the business' daily email newsletter to digital signage to morning "stand-up" meetings, security was seemingly everywhere overnight. Employees were provided badge appendages that explained what to do and whom to contact for suspicious activities, as well as "Security Excellence" handbooks to ensure everyone understood the expectations of "Living Superior."

These changes didn't only occur at the RMS Tucson site. Maintaining a competitive edge requires standardization. RMS employees made these same changes at all RMS sites to ensure that each facility was operating at a superior level. Recognized for our internal processes and improvement, RMS security professionals have also cultivated external relationships and partnerships both within and outside of the defense industry; offering guidance and best practices for similar processes.

Living Superior is not a destination, it's a journey — it will take continued commitment by all of us to stay the course and travel well.

Several years have passed since Raytheon's "March to Superior" moved to "Living Superior," but the focus and emphasis on being superior remains. RMS continues to partner closely with DSS, other Raytheon businesses and industry partners to raise standards to the next level and safeguard the important information and technology the government has entrusted to us in an ever-evolving threat environment.

The Raytheon Missile Systems security culture has developed a continual drive toward improvement and innovation. We all have the same mission in this respect, and it is incumbent upon those who have achieved a certain level to continue to innovate, communicate and educate other organizations working toward the goal of "Living Superior."

Living Superior is not a destination, it's a journey — it will take continued commitment by all of us to stay the course and travel well.

Saab's Syracuse-based Sensor Systems division — part of the recently established Saab Defense and Security USA LLC (SDAS) — is honored to receive its third Cogswell award since 1999 and its first as part of the new SDAS company.

Launched in 2012, SDAS combines several of Saab's U.S.-based defense units into a single company operating under a Special Security Agreement (SSA) with DSS. This new organization allows us to take the best practices established within the Sensor Systems division and apply them across the rest of SDAS.

SDAS operates under the premise that the following five items are crucial to maintaining our company's security:

- Full compliance with the base NISPOM requirements
- A good working relationship with our DSS representatives
- Management support from our internal business and our foreign owner
- Frequent employee training and communication
- A fully trained and well-versed security team

Operating under an SSA also requires that SDAS take additional security measurements, such as:

- Documenting and auditing all electronic communication between SDAS and foreign affiliates
- Submitting meeting requests for approval, and providing contact reports that summarize the meetings
- Implementing and maintaining an approved electronic communication plan that:
    - documents how our network is configured
    - demonstrates how we maintain electronic separation from our foreign owner
    - outlines processes and procedures for how we control and audit all electronic communication
- Various other associated plans for how we control and protect our classified and controlled information

While these measures require additional bandwidth, they have also enabled SDAS to address security items that may not have received appropriate attention otherwise. Our security staff is constantly engaged with management, employees, program teams and customers to ensure that security is visible and included early in business and program planning. This allows us to anticipate and address any security issues or concerns before they become a problem.

To ensure compliance, DSS conducts an annual security assessment of our company. SDAS prepares for this continuously throughout the year by conducting multiple self-inspections and comprehensive inventories.

We cross-reference our operations against a checklist and conduct employee interviews, basing our questions on information gathered from previous self-inspections. We then review and address any identified issues before starting the self-inspection process again. Additionally, we notify DSS of any questions and invite them onsite for an "advise-and-assist" session, if appropriate.

Approximately 60 days prior to the DSS assessment, SDAS begins to assemble three binders, including:

- **DSS assessment binder, containing:**
    - Security policies, violations, self-inspections, pre-assessment forms, closed area records, information systems records, key management personnel list, inventory records, shipments, etc.
- **FOCI-specific binder, containing:**
    - Electronic Control Plan, Technology Control Plan, Affiliated Operations Plan, Facilities Location Plan and associated approval letters, visit records, certificates, board meeting minutes and FOCI metrics
- **Enhancement binder, containing:**
    - Each category of enhancement and records documenting each one

Following the DSS assessment, SDAS develops a post-assessment document, which includes notes and comments from DSS representatives, as well as input from employees interviewed during the assessment. Once we have reviewed the collected information, we generate a plan to fix vulnerabilities and implement recommendations within 30 days.

Our security staff is constantly engaged with management, employees, program teams and customers to ensure that security is visible and included early in business and program planning.

By conducting meticulous self-inspections throughout the year, constantly monitoring and updating policies and procedures and implementing post-assessment recommendations from DSS, SDAS is able to maintain a robust security program.

We attribute our success to this thoroughness, as well as our strong relationships with our DSS representatives, other members of the security industry, our employees, and our internal and foreign affiliate management.

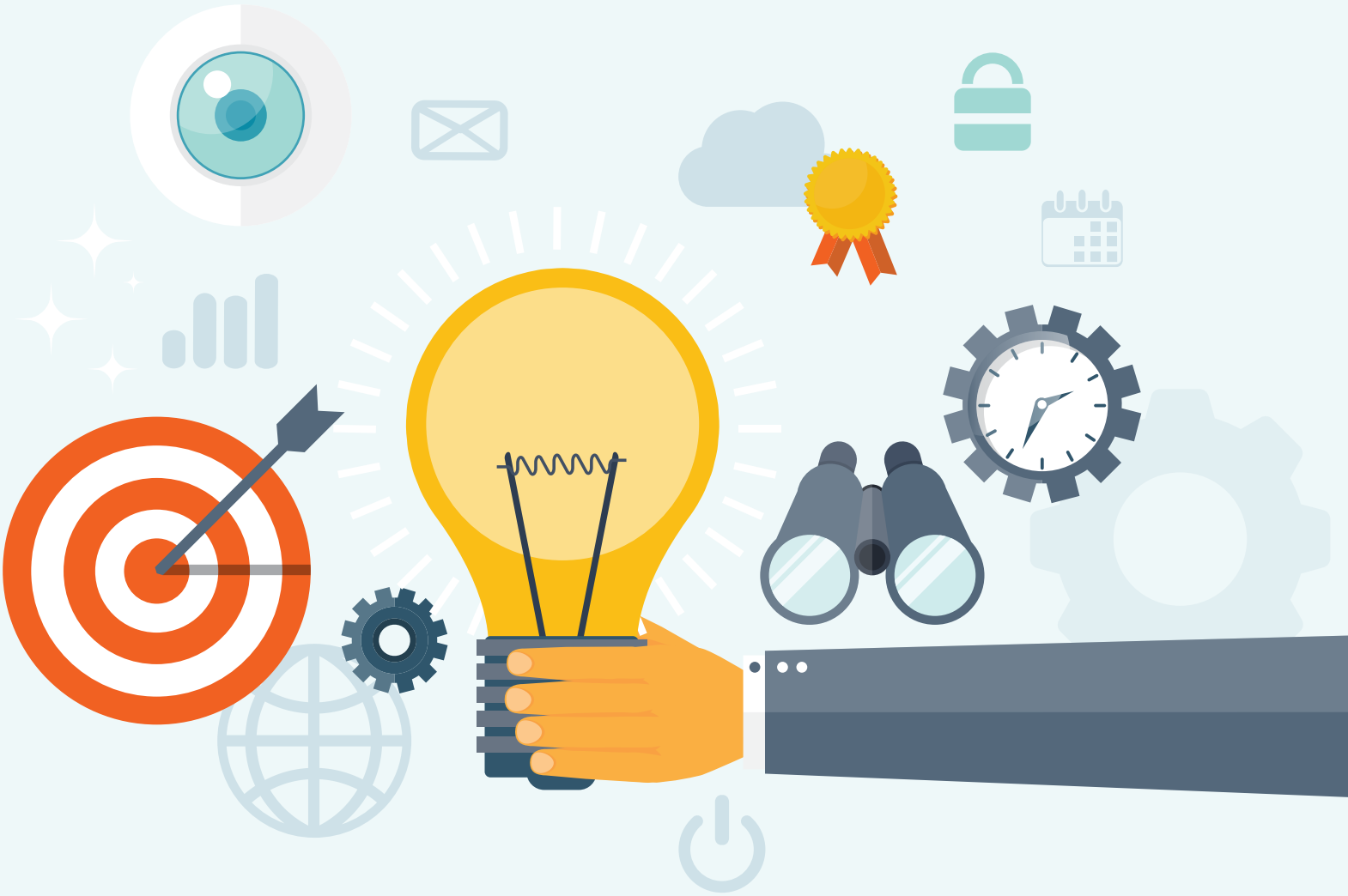
IN THEIR OWN WORDS

We invited a representative sampling of the 2015 Cogswell winners to share their formula for success with ACCESS readers. The following are tips and lessons learned from facilities with proven track records on how to establish and maintain a high-quality security posture.

by Scott Peterson
Corporate Security Officer
Saab Defense and Security, East Syracuse, N.Y.

IN THEIR OWN WORDS

We invited a representative sampling of the 2015 Cogswell winners to share their formula for success with ACCESS readers. The following are tips and lessons learned from facilities with proven track records on how to establish and maintain a high-quality security posture.



by Celena Spry
Facility Security Officer
Force 3, Crofton, Md.

In security, we've all heard the phrase, It's not if, but when something bad will happen so often that it's become something of a cliché. But that doesn't mean it's not true.

At Force 3, we take this message to heart. We know that at some point, our employees will experience a security incident. It's up to us to decide whether they will be prepared to handle the situation properly and in accordance with our security principles, or, if the incident will spiral into a security crisis.

As a network security company, we've come down strongly on the side of preparedness, awareness, training and proactive prevention of security risks. This company-wide commitment is what's led to our superior ratings, and the honor of receiving the prestigious James S. Cogswell Outstanding Industrial Security Achievement Award.

Our commitment starts in training. All employees, cleared or not, receive the same in-depth security training as part of their onboarding process. We do this because we believe that all our employees are the cornerstones of facility security success. As Force 3 has a large percentage of sales and marketing professionals who don't necessarily have a security-focused background, concepts that might seem rudimentary to security professionals are brand new to many of our employees.

All employees are given FACTS sheets reminding them of their reporting obligations. Our FACTS sheets simplify what needs to be reported (Foreign information, Adverse information, Changes in status, Termination of access and Suspicious contacts), and include my contact information, as well as how to report to DSS and the FBI.

Keeping open lines of communication with other security professionals is a great first step in establishing your own outstanding security program. I've found that most are very willing to share insights that will help boost security across both government and private industry.

These sheets, along with Force 3-created posters, are hung on employees' desks, around the office and even in the bathroom stalls! These reminders prepare the organization for the "when, not if" scenario.

Beginning on Veterans Day, Force 3 hosts our annual Security Week. During this week, we involve our large number of military veterans to help reinforce why security is so important. Ultimately, it goes beyond Force 3 or any company. We're protecting national security.

Our Security Week features briefings from organizations such as the FBI, along with fun games and activities to help employees sharpen their security know-how and recall their initial training. You'd be surprised at how motivated our professionals are by the promise of cupcakes!

While I am humbled at receiving this award, I must acknowledge those who have helped me along the way. I belong to several local security officer groups, and am a member of the National Classification Management Society and the Industrial Security Awareness Council of Southern Maryland.

These groups are invaluable resources for sharing best practices or finding answers to my questions. They help me keep on top of all the changes in the security community and implement them at Force 3 even before they take effect.

Keeping open lines of communication with other security professionals is a great first step in establishing your own outstanding security program. I've found that most are very willing to share insights that will help boost security across both government and private industry.

It's also important to have great communication with your senior leadership. They are championing a security policy and can make or break it with the rest of the company. At Force 3 I've been lucky to have very supportive leadership who won't settle for average. Every day they push the company and me to deliver superior security.

The strong relationship I have with my DSS representative is imperative to our program's success. Her many years of expertise gives me another source of knowledge I can tap if I have any questions or experience something new or unknown.

Lastly, focus on the unexpected. I've been involved in security since 2001, and every day I learn something new. Threats will always evolve and crises will arise out of nowhere. The best way to combat them is to constantly train, focus on your fundamentals and engage your employees.

One person can't secure a whole organization. You must instill a security mindset into each and every employee.

The Texas A&M University System has participated in the National Industrial Security Program for more than 40 years. With a statewide network of 11 universities, seven state agencies, two service units and a comprehensive health science center, the A&M System's externally funded research expenditures exceed $820 million annually and help drive the state's economy.

Our flagship, Texas A&M University in College Station, is one of only 17 institutions in the nation to hold the triple designation as a land-grant, sea-grant, and space-grant university.

Having achieved international recognition as a leading research and teaching institution and as one of only 62 invited members of the Association of American Universities, Texas A&M is a top tier public research university.

The cutting edge research being conducted within the A&M System covers every category listed in DSS's Industrial Base Technology List. Our researchers are world renowned in areas ranging from software to aeronautic systems, and from marine systems to nuclear, chemical, and biological research. We understand this makes us a target of those who would like to illicitly acquire the results of our research.

The 2014 edition of DSS's *Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting*, lists academic solicitation as the top method of operation for foreign collection attempts. This should not surprise anyone when you consider that the free flow of people and ideas is essential to the functioning of a great university. A research university is literally an open book. While this helps make an academic institution great, it also presents challenges for protecting the intellectual property of our researchers and the technological standing of the United States.

Maintaining a security program in an academic environment presents some unique challenges, but the A&M System is using the same qualities that are essential to effective teaching and research to form the foundation of our industrial security program. The success of our security program is based upon our ability to communicate, collaborate, and innovate.

Effective communication is essential to everything we do in our security program. We developed a monthly security update targeted specifically at our faculty and staff members. The update includes summaries of three security-related articles of specific interest to the academic community every month.

The update provides more in-depth coverage of a single topic from the NISPOM such as "need-to-know," personnel reporting requirements, or material that will help faculty members identify and counter academic solicitation. The updates are concise and targeted to the specific needs of busy faculty members. Over the course of the year, the monthly updates provide a solid foundation in security training for our faculty and staff.

With a significant number of U.S. Government organizations operating with competing interests on our campuses, interagency collaboration is extremely important to our success. We host a dozen U.S. Government agencies for a working lunch on a quarterly basis. This forum has two purposes: first, it is an opportunity for these organizations to coordinate and deconflict on–campus activities. Secondly, we use this as an opportunity to showcase some of the research being conducted on campus. This provides the government representatives with an introduction to our faculty members, insight into their research, and is a first step in building relationships between the researcher and the government agencies that are available to help protect their intellectual property.

While a typical cleared defense contractor can use a number of physical security procedures to harden their facilities and keep adversaries out, a university campus is necessarily open. Navigating the NISPOM and ensuring compliance within academia often requires the collaboration of other Facility Security Officers (FSOs) who are concerned with the same challenges.

In an effort to foster collaboration between university FSOs across the country, we implemented and host a list-serve that currently has over 90 university FSOs as members. This has proven to be a tremendous tool for collaboration in the three years since it was implemented.

We recently expanded on this concept with development of the innovative Academic Counter Exploitation (ACE) Program. The ACE Program is a community of interest hosted on DHS' Homeland Security Information Network.

The ACE Program provides an opportunity for University FSOs and DSS Counterintelligence Special Agents to communicate and collaborate virtually, and securely, on issues unique to the academic community. It also provides a portal to share threat information, best practices, and innovative ideas that are specific to the needs of the academic community.

We have also developed strong collaboration with our DSS counterintelligence representative. This collaboration recently resulted in development of an informational briefing entitled "Handle With Care: Best Practices for Protecting Yourself and Research in a Connected World."

This presentation is targeted specifically at university faculty members who are conducting research in areas of interest to our foreign adversaries. It provides insight into academic solicitation and gives the faculty members practical advice on how they can protect their intellectual property in an academic environment.

Maintaining a credible security program in an academic environment definitely presents some unique challenges — but it also presents great opportunities to contribute to the security of the United States. The Texas A&M University System is using the same qualities that make us one of the best systems of higher education in the country to form the foundation of our industrial security program. We are continually striving to communicate, collaborate, and innovate.

IN THEIR OWN WORDS

We invited a representative sampling of the 2015 Cogswell winners to share their formula for success with ACCESS readers. The following are tips and lessons learned from facilities with proven track records on how to establish and maintain a high-quality security posture.

by Kevin R. Gamache, Ph.D., ISP®
Facility Security Officer
The Texas A&M University System, College Station, Texas

Partnership is defined as two or more coming together for a joint interest. It is a critical and valued aspect of security. Partnerships should be formed within your company, with other Facility Security Officers (FSOs) and with the government. Building these relationships will enhance your security program by sharing lessons learned, developing broader perspectives, and gathering best practices.

Partnerships will enhance your security program because you will increase your communication, while gathering more information for your security program. Partnership, communication, and security all work hand in hand, allowing the partners to raise their game and improve their security capabilities, rather than just following a checklist mentality. Successful security programs should include a substantial element of partnering to make them successful.

As a law firm within the National Industrial Security Program (NISP), we do often face different challenges, especially in the intellectual property arena. Through our partnerships both within our firm and with our government clients, we have been able to tackle these unique issues much more effectively.

For example, every Monday morning I meet with our Security Chair to review all security relevant actions and initiatives for the week. This provides me with management support and partnership. Often it also helps in identifying additional parties who could help make our security program more targeted and effective.

Relationships and partnerships with government are also essential. Building a partnership with your government client and DSS requires just a phone call or email to initiate. As a previous DSS employee, I've seen how building relationships and partnerships can be advantageous to all involved.

With a unique background where I have been honored to be both a DSS employee and a private industry employee, I cannot stress enough the importance of partnership with DSS. A partnership can begin with a simple email, and can be further established by extending or requesting a Counterintelligence briefing from your Counterintelligence Special Agent.

DSS has consistently supported us by engaging our facility with training, guidance, and quick responses. We have found the many DSS resources and readily-available guidance to be extremely helpful to bolstering the security posture at our facility.

Also key is building relationships with other FSOs. This can be done through various organizations like ISACs, NCMS, ASIS, along with other security-focused organizations. It will be important to build a core group of security professionals with whom you can interact, ask questions, receive advice, and assist each other. These collaborations can be extremely helpful to building and developing your security program.

A simple way to establish a partnership with other security professionals is through attendance at workshops or by volunteering as a mentor or mentee. The mentorship relationship will be rewarding and helpful to all involved.

Finding a place to start is only a phone call or email away, as many security professionals are ready to provide guidance and assistance. It is a simple act that will pay great dividends for a better security program and a more rewarding security career.

Through our relationships and partnerships, our security education program has undergone additional development and growth. We have hosted various events with DSS and other government and security organizations. We have engaged in mentorship and an exchange of ideas with other FSOs.

Finding a place to start is only a phone call or email away, as many security professionals are ready to provide guidance and assistance. It is a simple act that will pay great dividends for a better security program and a more rewarding security career.

As Director Sims shared with us at the NCMS Conference, "Partnership with industry is a principle I strongly believe in."

We encourage you to follow Director Sims' guidance and engage with DSS and industry to enhance the security at your facility.

IN THEIR OWN WORDS

We invited a representative sampling of the 2015 Cogswell winners to share their formula for success with ACCESS readers. The following are tips and lessons learned from facilities with proven track records on how to establish and maintain a high-quality security posture.

by Shelly Kozacek
Facility Security Officer
Crowell and Moring, Washington, D.C.

IN THEIR OWN WORDS

We invited a representative sampling of the 2015 Cogswell winners to share their formula for success with ACCESS readers. The following are tips and lessons learned from facilities with proven track records on how to establish and maintain a high-quality security posture.

by Sally Marinelli
Facility Security Officer
The University of Rhode Island, Kingston, R.I.

The University of Rhode Island (URI) has carried out classified studies for 30 years and is globally recognized as a distinctive world-class university. One of the university president's transformational goals is to internationalize and globalize URI. Our philosophy is "Think Big — We Do."

Our world is shrinking as technology breaks down borders and time zones, allowing businesses and communities, large and small, to develop new relationships on the other side of the globe. Our students must be prepared to live and work in an increasingly globalized economy.

By expanding the scope of our international research and education partnerships, increasing the number of graduates fluent in languages other than English, encouraging more URI students to study abroad, and tripling our population of international undergraduate and graduate students, we break down our own borders, strengthen everyone's knowledge of the cultures, politics, and history of other peoples, and enable our students to prosper in this expanding global marketplace.

With this in mind, as you can imagine, being the Facility Security Officer (FSO) at a research university comes with the challenge of integrating the international environment at our academic institution with the required protection of restricted information.

With academic solicitation being the fastest growing method of collection of classified, sensitive and export-restricted research, we have had to place importance on educating faculty and staff about suspicious contact reporting requirements and on foreign travel vulnerability. In the case of our student interns, our briefings always include additional emphasis on security tips in the use of social networking sites.

Six years ago, as a new FSO, I was fortunate to be mentored with the wisdom and guidance of the previous FSO. I remember how proud we were when our annual DSS review rated our security posture as "commendable."

I came away from that assessment with encouraging suggestions for improvement and networking ideas from our DSS Rep. We applied those new ideas to enhance our security program and strive toward an even higher level of excellence. That fall, I joined NCMS and began attending meetings and training sessions to keep pace with the latest news in the realm of security. This resource proved to be an invaluable opportunity to network with peers and learn best practices.

With the help of these resources, we received a "superior" rating the subsequent year. As a result, my excitement and desire to maintain that status propelled me to become involved in more networking forums.

What I have learned is that becoming knowledgeable of National Industrial Security Program Operating Manual (NISPOM) requirements and progressive changes is fundamental, and I found that most of the relevant educational resources were free.

So, I joined a list-serv for University FSOs, became an FBI Infragard member, signed up for email updates from the National Security Institute (NSI) and Homeland Security, and joined AICWG (a local RI contractor working group of FSOs who meet monthly to discuss current topics of security interest).

All of these connections are instrumental in our ability to stay on top of the latest news and security guidance. And now, four consecutive "superior" ratings later, here we are, receiving the prestigious Cogswell Award!

Besides the value of networking, other main elements to our program's success are support and professional development which often go hand-in-hand. Our security program has the backing of our senior leadership starting with our Vice President for Research and Economic Development on up to the President of the University and even the Chair of the Rhode Island Board of Education, all of whom have attended our security briefings and events.

It is this modeling that shows the rest of the campus community that protecting national security and our intellectual property is a priority. I also give considerable credit to our DSS IS Representative and Counterintelligence Special Agent for their incredible patience and support over the years. It has enabled us to develop a mutual trust and respect that keeps the lines of communication open.

Our growing relationship with other government agencies such as the FBI and Naval Criminal Investigative Service is mutually beneficial and these organizations regularly provide us with useful and informative briefings and presentations.

A successful security program involves cooperation between all of the various university departments, so we engage as many as possible: Human Resources, Purchasing, Campus Police, Sponsored Projects, Legal, Information Technology Services, our Office of International Students and Scholars, our Compliance Office and, of course, the Deans of the Academic Colleges.

Additional support that our security program receives is financial support for professional development. So much can be learned from the education and training received at conferences like the NSI IMPACT Conference and the NCMS Annual Training Seminar which also facilitate excellent new resources and contacts. These events are essential, but are not always easy to fund while balancing the budget restrictions that come with being a state-supported university. As the FSO, I take advantage of no-cost NCMS webinars and online learning opportunities from DSS whenever possible.

My best advice to new FSOs is to prepare well for your DSS vulnerability assessment. Be highly organized with your documents and paperwork. Do several self-inspections in between DSS reviews and use those inspections to identify problem areas. Then, cooperatively discuss ideas for solutions with your DSS IS Representative. Following this advice will ensure a comprehensive and effective security program.

iGov Technologies has supported classified contracts for the U.S. government in its integration facility in Tampa, Fla., since 2006. There are approximately 60 employees at this facility supporting several different government contracts, and each employee contributed in some way to iGov being recognized as a Cogswell Security Award winner.

I have been the Facility Security Officer (FSO) for iGov's Tampa facility since 2006. I am proud and humbled to receive the DSS James S. Cogswell Outstanding Industrial Security Achievement Award on behalf of the facility, our employees and iGov.

Our Tampa facility has received five consecutive "Superior" ratings over the last six years. Our security practices and procedures are focused toward training not only the cleared employees but also the employees not holding active security clearances.

The success of any security program hinges on quality training for both the individual employees and the security staff. Effective training is a challenge due to the constant changes in industry as well as the evolving security environment. Insider threat, counterintelligence and cybersecurity are just a few areas requiring additional attention from a security standpoint over the last few years.

Every opportunity to provide formal training is made available to all members of the iGov team. Our company has always had a strong security education program to include posters, websites, newsletters, email reminders with security tips, initial security briefings, etc.

I involve all our employees with the security policies and procedures by getting out of the office and visiting the different areas in our facility including the Engineering Lab, Production Lab, Logistics Warehouse, and the various Program Management staff areas. I also converse with the employees to identify any security issues. This enables me to respond to any questions or concerns they have and, at the same time, gives me an opportunity to address any security issues we may have in a particular area of our facility.

There are no shortcuts when building an outstanding security program. Attitude is an important factor in achieving Superior DSS ratings and the Cogswell award. Professional development is endorsed and supported by iGov's senior management, and security staff members attend DSS, FBI, NCMS, and other professional training events on a regular basis.

Additional events and resources we utilize to ensure the success of our security program are:

- Engaging the support of iGov senior management and, along with their willingness and active participation in the NISP;
- Coordinating with my DSS representative on a regular basis for advice and guidance as well as using the DSS website and the mobile FSO toolkit;
- Conducting formal self-assessments every six months, and having other team members assist in these inspections;
- Getting out of the office and walking the facility, interacting with the iGov employees, and making myself available to answer any questions or concerns employees may have;
- Adjusting security levels and procedures intermittently as threats and concerns evolve;
- Constantly evaluating security practices and procedures to ensure we maintain security in depth and to validate the effectiveness of our program.

The iGov Security team attends and participates in the Florida Industrial Security Working Group (FISWG) meetings, and NCMS meetings. I conducted a presentation at the FISWG and the NCMS meeting in 2014.

The security team provides security education to our employees via pamphlets, posters, conference room briefings, one-on-one briefings, group meetings, monthly newsletter, and a SharePoint-based website that enables all employees to review DSS flyers, FBI newsletters and all iGov training presentations at any time.

I have established an FSO/DSS binder for every classified contract we currently support. This binder is organized with all the information that the DSS representative requires for his/her security vulnerability assessment, such as facility clearance forms, DD forms 441, 441-1, and 254, sub-contractors DD254, Facility Standard Practice & Procedure, technology control plan, OPSEC plan, and all employee training records conducted during this period.

A second binder is dedicated for counterintelligence information, such as employee training, suspicious contact information that has been forwarded to our Counterintelligence Special Agent, CI briefings and training presentations conducted for CI, OPSEC, and cybersecurity.

A third binder is for our DSS enhancements categories, along with the required information to support each enhancement for that specific category.

I believe it is important to build a trusting relationship with your DSS/CI representative, and effective communication is a key ingredient. Additionally, being organized and keeping meticulous records makes it easy for DSS and the CI representatives to conduct the assessment and to build the trust between the FSO/security team and the DSS representatives that results in a more effective partnership.

We continue to learn new ways to provide training to our employees to not only satisfy our NISPOM requirements, but to keep our employees involved and make them want to improve our security procedures and practices while taking a more active role in our security program. It's a mutually beneficial formula for iGov, DSS and industry.

IN THEIR OWN WORDS

We invited a representative sampling of the 2015 Cogswell winners to share their formula for success with ACCESS readers. The following are tips and lessons learned from facilities with proven track records on how to establish and maintain a high-quality security posture.

by Michael T Kalinowski
Facility Security Officer
iGov Technologies, Tampa, Fla.

Stan Sims (right), DSS Director, receives the Lonnie R. Buckels Presidential Award from NCMS President Leonard Moss. *(Photo courtesy of NCMS)*

DSS Director receives President's Award at annual NCMS training seminar

The Defense Security Service partners with NCMS each year to deliver training during the annual NCMS training seminar. One of the highlights of the week-long seminar is the President's Dinner where a number of awards are presented. This year, DSS Director Stan Sims received the Lonnie R. Buckels Presidential Award from NCMS President Leonard Moss.

The Presidential Award is presented each year to an individual within the industrial security community who made significant contributions to education, training, information systems, and teaming with government and industry partners on a local or national level. The individual must also have made the contributions for five years or more to the security community as a whole.

In presenting the award, Moss said Sims was selected for the award for his extraordinary leadership transforming the Defense Security Service in delivering exceptional training and tools, a strong counterintelligence program, a risk-based/cost effective security vulnerability program, as well as significantly enhancing the government/industry partnership.

"Since being appointed Director of DSS in 2010, Mr. Sims has been a true champion for our industry and has led the transformation of DSS," said Moss. "Under his leadership, DSS has truly become an industry partner in every sense of the term."

Moss cited the agency's success in delivering training to both government and industry and improving the security assessment process by implementing a risk-based approach. That approach helped industry reduce risks to national security by being more strategic in applying resources and focus.

The security rating matrix process, said Moss, eliminated subjectivity and helped to ensure a fair and more objective assessment for all cleared contractor facilities.

"When I was elected President of NCMS," Moss said, "Stan was one of the first leaders to provide a hand to me and offered unfettered access to their organization to address real challenges. I have witnessed his commitment first hand."

Moss noted that Sims leads and supports numerous industry functions and collaborative efforts to include being a keynote speaker at NCMS annual seminars; hosting a quarterly industry/government stakeholder meeting; and attending and participating in a number of government/industry forums as either a speaker or participant.

Sims has also encouraged and empowered the DSS team to support these same organizations and has brought critical support to local NCMS chapters and events to strengthen the national security landscape.

"It is because of these many contributions to both our industry and our society, as well as a lifetime of service to our nation, that Mr. Sims received the NCMS Presidential Award" said Moss.

In accepting the award, Sims said, "While you are recognizing me today, it's really the men and women of DSS who deserve the award. I may have set the goals and vision for them, but they executed it. They have embraced partnership with industry and fundamentally changed how DSS does business. On behalf of everyone at DSS, I am honored and humbled to accept this."

DSS Chief of Staff retires after 34 years of federal service

ABOVE: Former Chief of Staff Rebecca Allen (left) and her aunt Joanne Harley have their photo taken after the ceremony.
(Photo by Hollie Rawl, CDSE)

Rebecca "Becky" Allen, DSS Chief of Staff, retired from federal service as a member of the Senior Executive Service (SES) in April 2015, with more than 34 years of federal service.

Allen's first federal job was as a security intern working for the Army; she then moved to the Military Traffic Management Command for a permanent position. From there, she joined the Defense Logistics Agency where she was selected as chief of DLA's Intelligence and Security Team. Allen then transferred to the Defense Contract Management Agency to become the agency's first Security Director and later Chief of Staff.

Prior to coming to DSS, Allen was Deputy Director of Security in the office of the Deputy Under Secretary of Defense (HUMINT, Counterintelligence and Security), Under Secretary of Defense (Intelligence). In this position, she was responsible for the development, promulgation and oversight of Department of Defense policy for personnel security, physical security, industrial security, information security, operations security, chemical/biological security, special access program security, and research and technology protection.

She joined DSS in 2011 as the Deputy Director of Industrial Security Field Operations (IO) and was selected as Chief of Staff in 2012.

Allen received a number of awards during her retirement ceremony including the Intelligence Community coin from the Director of National Intelligence and the Intelligence Community medallion. The Intelligence Community seal medallion is an official award within the national intelligence community suite that can only be authorized by the Director of National Intelligence, James Clapper.

DSS Director Stan Sims also presented Allen with the DSS Distinguished Service Award for her tenure as Chief of Staff and as Deputy Director of IO. While assigned to IO, she led the development and implementation of field process improvements including a new security rating matrix and an expanded risk category for contractor facilities of interest.

As the DSS Chief of Staff, she consolidated headquarters support activities into an integrated enabling capability, empowered her leaders and people across headquarters to increase efficiencies, improve workforce diversity, and advance internal human capital and security services.

Allen was also presented with the SES logo, a U.S. flag flown over the Capitol in her honor, and a plaque for outstanding leadership.

Editor's Note: *The following is the fourth in a series of features on the four DSS regions. In each, the regional director discusses what makes their region unique, the challenges they face and how they address them.*

Cheryl V. Matthew assumed her duties as the Northern Region Director in May 2014. As Regional Director, Matthew is responsible for the industrial security oversight of approximately 2,800 National Industrial Security Program (NISP) facilities across 21 states, east to west from Maine to Minnesota and south covering portions of Northern Virginia and Maryland.

She began her federal career in 1980, working for the Department of the Army, U.S. Army Natick Research and Development Center, in Natick, Mass., as a co-op student and administrative assistant in the Security Office. In 1985, she went to work for the Defense Investigative Service, now DSS, as a special agent in the Boston Field Office.

She became a Senior Industrial Security Representative in 1989 working in several offices in Massachusetts (Waltham, Boston, and Wilmington). In 2008, she was promoted to the Region Operations Manager position where she was responsible for all operations and the quality assurance program across the Northern Region.

In 2013, she was the Acting Field Office Chief of the Boston Field Office and was then selected for that position. The Boston Field Office covers southern and western Massachusetts, Rhode Island and Connecticut.

ASK THE LEADERSHIP

A Q&A with **Cheryl Matthew**, *Director of the Northern Region*

Tell us about the Northern Region.

The Northern Region is comprised of seven field offices — Andover, Boston, New York, Philadelphia, St. Louis, Detroit, and Mt. Laurel. Additionally, there are eight resident offices located in Minnesota, Illinois, New York, New Jersey, Pennsylvania, Connecticut, and Ohio.

What makes the Northern Region different from the three other regions?

The Northern Region has the most Category AA and A facilities (Category AA and A are designated as the most complex facilities in the NISP). In order to review the security posture of these facilities, a team of individuals will spend one to two weeks a year conducting a security vulnerability assessment.

To put that into context, the Northern Region has roughly 45 weeks of team assessments taking place throughout the year. These assessments require much planning and coordination between the facility and all field elements (industrial security representatives, counterintelligence special agents, and information systems security professionals). These facilities individually could have thousands of employees, hundreds of classified contracts, and scores of approved computer systems and areas. The advice and assistance provided throughout the year is also very substantial.

The Northern Region has the largest number of excluded parent facilities, many of which are located in New York. These companies own or control other entities that need a facility clearance to perform on classified contracts. These facilities do not need to be cleared for access themselves but need to be formally processed to ensure material at these locations will be properly protected. A large number of these excluded parent companies have complex legal and corporate business structures, many of which are financial, equity, or holding firms whose structures need to be analyzed and evaluated before classified contracts can be granted to the entity that will perform the work.

The Northern Region has the most arms, ammunition and explosives facilities and these are located in many remote places across the region. We have a dedicated cadre of folks who provide support to these entities and perform new surveys on short notice. We have designated folks in the region and in every office assigned to this mission. These individuals work to support each other especially when a short suspense survey is requested.

We have over one hundred facilities that are under a foreign, ownership, control or influence (FOCI) mitigation or negation agreement. The Region Office is the focal point for all assessments and annual meetings held at these facilities. If we do not have the signatory facility, we work closely with the region that does as well as with the FOCI Operations Division to ensure foreign aspects to these facilities has been thoroughly reviewed at our sites.

The Northern Region is home to two large shipbuilding facilities in Maine and Connecticut that build destroyers and submarines. In Missouri we have a large aircraft manufacturer. We have freight forwarders in New Jersey and New York that move classified freight within and outside the United States. The Northern Region has corporate home offices, research, development and manufacturing facilities,

educational institutions, and trusted foundry facilities. Each of these facilities has unique needs and challenges.

What are the challenges in the Northern Region?

The Northern Region has its share of challenges. Covering the territory between Maine and Minnesota means we are affected during winter months from a travel and logistics scheduling standpoint. This past winter, parts of the region received over nine feet of snow!

The western part of the Northern Region is very geographically dispersed, which means a great deal of windshield time for our folks getting to and from facilities. Temporary duty is not periodic but constant.

This past year we sought and filled field office chief vacancies in two of our offices and just completed the process of hiring two ISSP team leads. These are critical positions within the Northern Region and DSS. Having more than one vacancy at the same time posed challenges to the offices and to the region, as we needed to ensure proper coverage and leadership in our offices. It was refreshing to see personnel taking on extra responsibilities across the region to help out and we were also very fortunate to receive assistance from the other regions which sent volunteers TDY to these offices as well.

Northern Region has the reputation of having seasoned personnel which has made us extremely successful. The challenge here is that a large number of these individuals will retire in the next five to 10 years and succession planning is critical to maintain our success. We need to ensure the institutional industrial security knowledge of these individuals is transferred to our newer folks to maintain that perfect mixture of experience with new ideas.

How did your background prepare you for the job of Regional Director?

I held several field and region positions that absolutely prepared me for this position. For example, coming to DSS as a special agent early in my career gave me the experience needed to talk to people from diverse backgrounds. In that position, I developed listening skills which are so important in communicating, understanding and addressing the needs of our personnel.

As an industrial security representative, I experienced firsthand the core mission of DSS. That experience was very rewarding and I learned a great deal, not just about the industrial security program but how to work with our industry partners and government stakeholders to identify and mitigate risks to classified programs.

As a field office chief, I experienced the rewards and challenges in managing an office of dedicated field personnel, and I also expanded my relationships with support personnel from other DSS Directorates. As the Region Operations Manager, my role was to provide operational support to the Regional Director, field office chiefs and team leads, and I served as a vital conduit for communications between the field and headquarters.

My philosophy has always been to work hard, be the best you can be in the position you are currently in, and take that experience with you to the next assignment. I believe my field experience continues to drive me, and when making decisions and working with my colleagues throughout the agency, I am truly representing the field.

What changes have you made / seen in the region since arriving?

Since becoming the Regional Director, I have focused my attention on hiring new employees, integrating all field disciplines, and finding ways to capture best practices that can be shared across the country.

I hired two new field office chiefs and team leads, and these folks are going to do great things for the region and DSS. We are very fortunate to have seasoned personnel who have the tacit knowledge and fundamentals that security professionals need to address the threat to national security.

A recent initiative is three training events across the region that almost all Northern Region personnel attended. The goals were for employees to know where they fit into the DSS Strategic Plan 2020; understand each other's roles in providing risk management services to industry; and how the quality of our actions in a budget-constrained environment is essential for our mission success.

The DSS Office of Innovation helped us develop a workshop at these events that would identify what constitutes a thorough security vulnerability assessment; what should a risk based vulnerability assessment look like; ways to capture and share best practices; and how to work cohesively to provide the best oversight and support to our industry partners. Personnel from field operations and counterintelligence participated and I believe everyone learned integration is an essential piece to our oversight mission.

I have seen many changes in the industrial security program but the one constant has been the outstanding technical expertise and leadership in our offices. We have never been better poised to provide the risk management services needed to assist our industry partners in addressing emerging threats to their programs and it is my priority and responsibility to ensure our personnel have the tools needed to achieve success.

DSS students train at FBI Academy

by Dana Richard
Counterintelligence Directorate

Recently, 24 DSS employees gathered at the FBI Academy on Marine Corps Base Quantico to participate in a unique training experience. The training, facilitated by FBI instructors, was a pilot program to develop and improve interviewing, writing, and public speaking skills with the intent of improving the collection, processing and reporting of information that could be of counterintelligence (CI) value across DSS. The students were a mix of CI special agents, industrial security representatives, information system security professionals, and CI analysts.

During the course of his/her regular duties, a DSS employee — whether a CISA, ISSP or ISR — may encounter potential threat information of value to DSS, thus making each individual a potential CI collector. This pilot course was conceived to develop skills that can increase and improve CI collection. While these skills are designed primarily for CI personnel, the techniques can also increase the effectiveness of vulnerability assessments.

The course began as a series of conversations between Special Agent Michael Van Meter and Dr. Cynthia Lewis of the FBI Academy's Investigation Training Unit about ways to fill specific training gaps. A writing refresher course, conducted by Lewis in September 2014, was considered very effective and beneficial to CISAs, ISRs and ISSPs who attended. Looking to build upon that success, follow-up discussions envisioned a course concept incorporating information-gathering techniques — primarily interviewing.

Further conversations between DSS directorates led to an agreement to run a pilot program that would include students from across DSS. The course was unique in that it provided technical skills training of a scope and duration not previously offered to an integrated CI and industrial security audience.

Since it was a pilot, the course was something of a "buffet," as described by Van Meter, to allow DSS to see what the FBI Academy can do and to determine what is of most use to DSS students. Topics covered during the course went beyond interviewing, writing and public speaking skills, to also include the intelligence cycle and where DSS employees fit into it, elements of statement analysis, and identifying deception. Students universally lauded the quality of the instruction and the instructors, and their feedback provided valuable insights to improve future iterations.

"This is a good start to creating consistency and establishing realistic expectations across the organization," said Russ Reynolds, CI special agent in the New York Field Office. "Whether you are an industrial security representative conducting a security vulnerability assessment, a CI special agent debriefing a foreign traveler, or an information systems security professional interviewing an information systems security manager about a classified information system, the skills provided in the training can be directly applied on a daily basis."

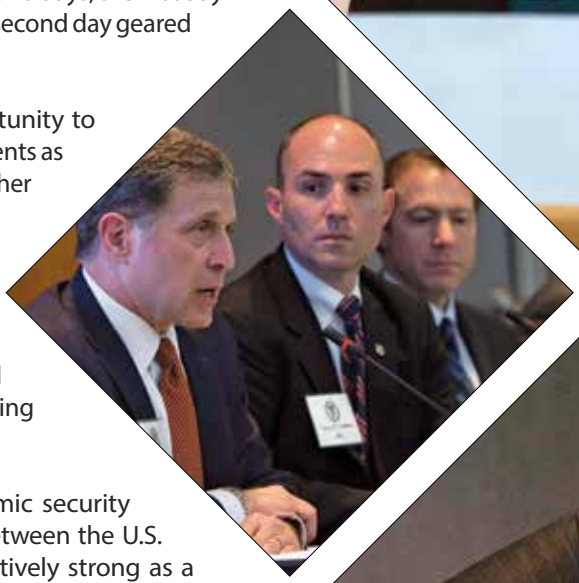
"This was an excellent first iteration of this class, and it will only get better," said Gary Morris, ISSP in the Philadelphia Field Office. "The interviewing and writing material presented will be useful in my work and would be beneficial to all DSS employees. The FBI instructors were great, and I would surely recommend others attend this training."

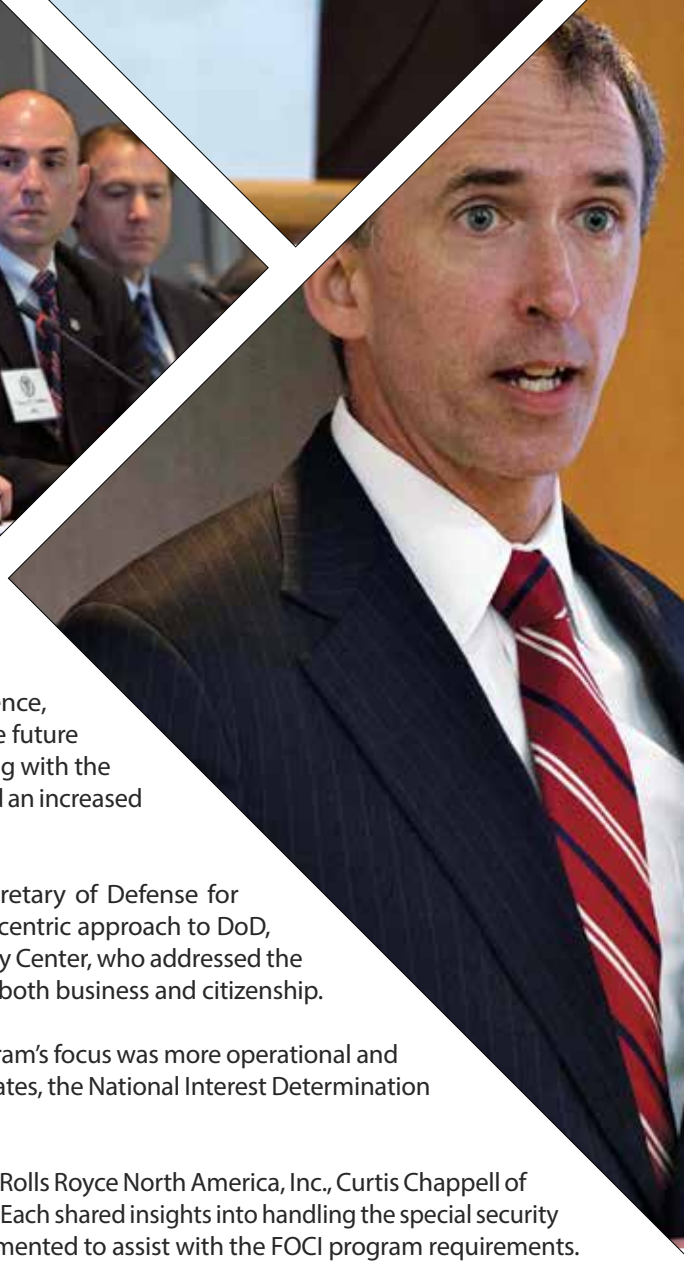
Planning is under way for the next iteration, and anticipated changes include an expansion of interviewing techniques and the addition of strategic debriefing and CI support to the areas of research, development and acquisition. The team is also looking to incorporate training from the Defense Intelligence Agency's Joint CI Training Academy and panel discussions featuring members of the FBI, Air Force Office of Special Investigations, Naval Criminal Investigative Service, and the Army Criminal Investigation Command.

CLOCKWISE FROM TOP: Gary Morris, information systems security professional in the Philadelphia Field Office, gives a presentation. | Twenty-four DSS employees from various regions attended training. | As the presentations were timed, students received warnings based on the color of the bulb. | Susie Miller, industrial security representative in the Virginia Beach Field Office, makes a point during a presentation.

Outlining strategy for the future focus of the FOCI conference

by Juliana Gabrovsky and Jessica Henson
Industrial Policy and Programs





DSS held its 19th annual Foreign Ownership, Control or Influence (FOCI) Conference on April 14-15, 2015, for companies operating under DSS FOCI mitigation. The conference was presented over two days; the first day aimed at outside directors and proxy holders and the second day geared toward facility security officers.

The FOCI conference provided DSS with an opportunity to educate industry on FOCI program-related developments as well as allow industry to communicate with DSS and other FOCI companies on their DSS FOCI program oversight and related questions and issues.

On the first day of the conference, DSS Director Stan Sims welcomed the attendees and shared updates to the FOCI program, and the ongoing and future role of the agency in the context of the changing national security and globalized environment.

He emphasized that national security and economic security are truly one and the same, and the partnership between the U.S. government and industry is what makes us collectively strong as a country. He also introduced two new DSS directorate personnel: Fred W. Gortler III, director of Industrial Policy and Programs, and Gus E. Greene, Sr., director of Industrial Security Field Operations.

Keynote speaker Marcel Lettre, acting Under Secretary of Defense for Intelligence, provided a general overview of Secretary of Defense Ashton Carter's focus for the future of the Department of Defense. Lettre also spoke about his own strategy for coping with the shifting landscape of intelligence, including a push for global satellite coverage and an increased emphasis on cybersecurity and counterterrorism.

Also speaking the first day were Andre Gudger, acting Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy, who spoke about bringing a business-centric approach to DoD, and Daniel Payne, deputy director of the National Counterintelligence and Security Center, who addressed the unprecedented threat levels facing the nation, due in part to the globalization of both business and citizenship.

During the second day of the conference, designed specifically for FSOs, the program's focus was more operational and presentations featured DSS subject matter experts on topics including policy updates, the National Interest Determination process and Affiliated Operations Plan, to name a few.

Finally, the conference featured a panel of industry security experts: Stan Borgia of Rolls Royce North America, Inc., Curtis Chappell of DRS Technologies, Inc., Frank Husker of MBDA, Inc., and Richard Ramsey of Serco, Inc. Each shared insights into handling the special security concerns and processes, procedures and program development they have implemented to assist with the FOCI program requirements.

In all, more than 250 outside directors, proxy holders, and FSOs attended the two-day event. Launched in 1989, this conference originally included only outside directors and proxy holders. In 2010, DSS added a second day to include the FSOs. DSS has tentatively scheduled the next FOCI conference for the spring of 2016.

CLOCKWISE FROM TOP: Nicoletta Giordani, FOCI Operations Division, presents a briefing. | Principal Deputy Under Secretary of Defense for Intelligence Marcel Lettre was the keynote speaker. | Stan Borgia of Rolls Royce North America Inc., gave insight as part of a panel with Curtis Chappell, DRS Technologies Inc. (center) and Frank Husker, MBDA Inc. (right). *Photos by Derik Bland, IP*

DSS partners with Department of Homeland Security

DHS becomes fifth Cognizant Security Agency

On Feb. 13, 2015, the President signed Executive Order (EO) 13691, "Promoting Private Sector Cybersecurity Information Sharing," which lays out a framework to be overseen by the Department of Homeland Security (DHS), for expanded cybersecurity threat information sharing to help companies work together and with the federal government to quickly identify and protect against cyber threats.

With cyber-sharing responsibilities afforded to DHS, this new EO amends EO 12829, "National Industrial Security Program," and designates the Secretary of Homeland Security as a Cognizant Security Agency (CSA) for the National Industrial Security Program (NISP).

The issuance of the EO brings the number of CSAs to five, including:

- Secretary of Defense (DoD); serves as the Executive Agent
- Director of National Intelligence (DNI); retains authority over access to intelligence sources and methods including Sensitive Compartmented Information
- Nuclear Regulatory Commission (NRC)
- Secretary of Energy (DOE); in addition to the NRC, retains authority over access to information under their respective programs classified under the Atomic Energy Act
- Secretary of Homeland Security (DHS); responsible for classified information under the critical infrastructure protection program.

Though designated as a CSA and responsible for classified information sharing pertaining to cyber-sharing under the new EO, DHS will continue to rely on DoD for its industrial security services.

DHS will only clear and oversee cleared contractors for its area of responsibility under this EO; specifically, DHS will only clear individuals within companies in cases where there is no requirement to possess classified information at the companies' location related to cyber-sharing activities.

DHS will not grant facility clearances to any company that requires the possession of classified material or is outside the scope of the parameters of this EO. These companies will continue to be cleared under DoD cognizance and the requirements set forth in the NISP Operating Manual.

To support DHS in its new role and facilitate implementation of the EO, DSS hosted DHS in April 2015, for a two-day intensive overview of DSS' processes related to its responsibilities pertaining to overseeing the NISP on behalf of DoD.

Specifically, DSS staff discussed its processes for facility clearances, field operations, methodology to assess, mitigate, and oversee foreign ownership, control, or influence, and policy implementation.

This was the first meeting, with future meetings planned to assist DHS in assuming its role in the NISP as a CSA to perform oversight responsibilities for entities under DHS' cognizance.

CDSE goes international: SAP training in Rome

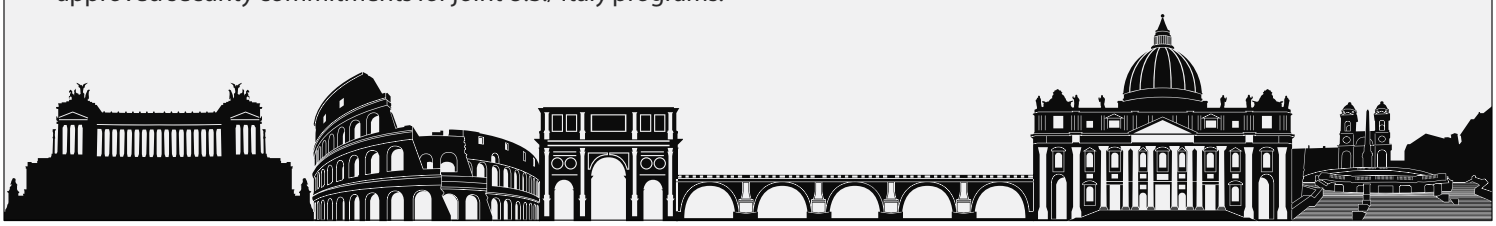
In April 2015, the Center for Development of Security Excellence (CDSE) delivered its first iteration of the Introduction to Special Access Programs (SAPs) Course to 13 Italian Navy and Air Force military members in Rome, Italy.

The course was provided to Italian personnel in support of the Joint Strike Fighter Program.

The goal was to offer more cost-effective training and establish the foundational strength in SAP security needed to honor approved security commitments for joint U.S./ Italy programs.

The Italian military is setting up its first SAP facility in Italy and found the course to be interesting and useful in developing the "worker bees" of the program. All 13 students successfully passed the training with an exam score of 80 percent or better.

The course was beneficial in helping students learn the pillars of SAP security. In the future, the Italian military anticipates periodically sending students to in-house training at CDSE in Linthicum, Md. They are also considering a request for refresher SAP courses on a biennial basis.



DSS OBSERVES MEMORIAL DAY

REMEMBRANCE: Stan Sims (center), DSS Director, salutes the wreath placed in honor of Memorial Day during a ceremony held May 21, 2015, at the Russell-Knox Building. Providing Honor Guard support for the event were Lance Cpl. Valiant Cocchi (left) and Cpl. Emmanuel Webb (right) from Marine Corps Base Quantico. *(Photo by Hollie Rawl, CDSE)*

WHAT A SUCCESS!: Participants of the Take Your Child to Work Day express their feedback at the end of the day's activities.

DSS observes "Take Your Child to Work Day"

by Dahlia Thomas
Office of Public and Legislative Affairs

DSS, along with Russell-Knox Building tenants Defense Intelligence Agency (DIA), Air Force Office of Special Investigations (AFOSI), United States Army Criminal Investigation Command and Naval Criminal Investigative Service, sponsored Take Your Child to Work Day (TYCTWD) on April 23, 2015. Approximately 280 boys and girls, ages six through 18 years, accompanied their parents to work to learn how their parents contribute to the nation's security.

The event kicked off with an opening ceremony attended by senior leaders James Kren, DSS Deputy Director; Coleen Kolina, DIA chief, Office of Counterintelligence; and Jeffrey Specht, AFOSI executive director. Each greeted the children and challenged them to learn how they can contribute to the nation's security through government service. They also encouraged them to take full opportunity of the planned activities and not be afraid to ask questions.

Acting as master of ceremonies for the event was d'Art Richard, 12-year-old son of Dana Richard, DSS Counterintelligence. A third time attendee of the Take Your Child To Work Day event, d'Art said he was excited to be the MC because it was a job his father occasionally performs for the agency. Alexandra and Victoria Woodruff, daughters of Diane Brooks-Woodruff, DSS Program Integration office, sang the national anthem.

In keeping with this year's theme of #MPOWR (knowledge + choice = strength), the day's events were filled with information and useful presentations. Children ages 6 and 7 years toured the Data Center and viewed the various agencies' artifacts prominently displayed throughout the building. The children ages 8 and older participated in interactive, age-appropriate educational sessions covering topics such as Forensics, Cyber Awareness, Tech Services, Surveillance and Career Planning. The children learned first-hand the important role their parents play in collecting evidence for crime scenes and the importance of protecting personally identifiable information on social media. During another session, children saw the importance of preparing for a job interview and were given the opportunity to interview several RKB employees about their careers.

The event closed with several outdoor activities, to include tours of a Prince William County Sheriff's Office vehicle and United States Marine Corps Fire Department emergency vehicles. Representatives of the Marine Corps Martial Arts Center of Excellence showed hand-to-hand combat tactics, and the Marine Corps provided a military working dog demonstration, which kept the audience's attention and sparked excited comments.

When the TYCTWD participants were asked to name their favorite activity, the responses were mixed. Answers ranged from "Cyber Awareness," to "the interviewing portion," to "the hacking presentation [Surveillance]," and finally to the "K-9 demonstration."

When queried about the jobs highlighted during the day's events, participants varied in picking a job they would like after finishing their education. One respondent wants to be "advertising director of an agency," while another "wants to work with my dad and DSS," and yet another would like to be "a firefighter."

The children of Drew Woods, DSS CI, speak with a Prince William County sheriff during a tour of his vehicle as part of Take Your Child to Work Day.

Julia Fellows, daughter of Jonathan Fellows, DSS Office of Public and Legislative Affairs, tours an emergency vehicle.

TELL ME ABOUT IT: Alpha Bund-Contech (left), Bowie State University student, relates what he learned during the HCMO Shadow Day event, while Shon Todd, DSS HCMO, listens.

First student shadow day provides opportunity to discover DSS

In April 2015, the DSS Recruitment Office conducted its first Student Shadow Day, where college students were given the opportunity to discover DSS by shadowing a senior leader.

Participating in this pilot event were six undergraduate and graduate students from Bowie State University, who were selected by the university's career development center for involvement in the event.

The purpose of the Shadow Day was to give students an opportunity to learn about the agency's mission and obtain a "day in the life of" perspective of how federal employees support the oversight of national security by going through an average day with DSS senior leaders.

Supporting the event from DSS were Corey Beckett, comptroller; Tim Harrison, chief of Security; Selena Hutchinson, deputy director of the Office of the Designated Approving Authority; La Shawn Kelley, chief of Human Capital Management Office; Paul Murph, deputy Chief Information Officer; and Richard Stahl, chief of the International division of Industrial Policy and Programs.

Additionally, the students listened to remarks from Kelley and then DSS Chief of Staff Rebecca Allen, received a tour of the Russell-Knox Building, and were instructed on how to use the USAJobs website during a Lunch-N-Learn session conducted by Laura Szadvari of the Recruitment Office.

MEET & GREET: Gus Greene Sr. (far right), director of Industrial Security Field Operations, visits with Raytheon employees (from left) Terry Hardy, facility security officer, Integrated Air Defense Center; Matt Rhind, director, Global Security Services – IDS; Nancy O'Neil, senior industrial security manager, Raytheon Company (corporate headquarters); Laura Schaffer, manager, Information Systems Security; Mike Demers, senior industrial security manager, IDS; and Beth Shea, Northern Region action officer.

New field operations director visits Andover Field Office

Gus Greene, Director of Industrial Security Field Operations (IO) made his first trip to the Northern Region in early June. During his visit to the Andover Field Office, Greene addressed the region and field office staff where he shared his vision for IO and discussed the future of DSS. He also took time to meet individually with field personnel to learn about their particular job duties, and to discuss areas where operational efficiency can be improved.

Greene's itinerary included a visit to Raytheon Company, Integrated Air Defense Center (IADC), where he met with Dan Schlehr, Vice President, Global Security and other senior Raytheon security leaders. Raytheon is one of the largest defense contractors in the Northern Region and falls under the cognizance of the Andover Field Office.

Greene received a guided tour of the IADC plant, which encompasses seven buildings housing more than 1.7 million square feet of manufacturing and office space. IADC is the main manufacturing and circuit card assembly site for Raytheon and supports numerous classified programs to include the Patriot Missile System, Joint Land Attack Cruise Missile Defense Elevated Netted Sensor System, Terminal High Altitude Air Defense, Aegis, Zumwalt, AN/TPY-2 and Cobra Judy Replacement radar systems.

The visit to Raytheon demonstrates the ongoing partnership between DSS and industry and provided Greene with a greater understanding of Raytheon's business model, their security successes, and the continuing challenges they face.

Partnership with industry: A first hand account

*(**Editor's Note:** The following article is a first-person account of a DSS employee's participation in a Partnership with Industry program.)*

by Jason Howard
Tampa Resident Office

Every year when updating our Individual Development Plans, our field office chief encourages members of the Melbourne Field Office to identify continuing education and training opportunities we are interested in pursuing. In recent years I participated in Export Compliance, Counterintelligence, and Command Cyber Readiness Inspection (CCRI) training.

This year, I volunteered for a different type of continuing education experience — the Partnership with Industry (PWI) program. DSS field personnel, particularly industrial security specialists, spend a great deal of time supporting and educating cleared industry through advice and assistance visits, briefings, and security assessments. However, sometimes we lose sight of the challenges our industry partners face, and the lessons they have to teach us.

The PWI program is designed to benefit both DSS personnel and industry. It provides an opportunity for DSS employees to gain exposure and perspective on cleared contractor operations, while also giving industry employees an opportunity to view business operations from our perspective, and get a glimpse into our insights and experiences.

A couple of months after volunteering to participate in the program, I was advised that I would be visiting Raytheon Missile Systems in Tucson, Ariz. My Raytheon point of contact would be their manager of Industrial Security Awareness, Dr. Anita Archer.

This division is one of the largest defense contractor facilities participating in the National Industrial Security Program (NISP). Upon arrival at the facility I was greeted by several members of the security staff to include Andy Lewis, Facility Security Officer. The Raytheon staff crafted a three-day agenda that included tours of the facility, a comprehensive overview of the security program, and presentations regarding the numerous defense programs supported onsite.

The size and scope of the facility in terms of NISP involvement is impressive. This location currently has almost 200 closed areas, three large offsite locations, and more than 9,000 cleared employees under DSS cognizance. Touring the perimeter of the main campus alone takes a Raytheon Security Services guard two hours or more. In addition to traditional NISP compliance, the security staff is responsible for the physical protection of the military installation [Davis-Monthan Air Force Base], and dealing with conventional law enforcement issues such as drug runners attempting to smuggle large quantities of narcotics through rural outskirts of the campus.

A few areas of the facility that were particularly impressive were the Immersive Design Center and the Rita Road facility. The Immersive Design Center allows engineers to wear 3-D glasses to view, modify, and design defense technology in a completely virtual environment.

Using this impressive state-of-the-art technology, an engineer can either collaborate with or train peers located locally or at remote locations. The technology was even used by Raytheon to design and lay out its factory in Huntsville, Ala.

The Rita Road facility is largely used for production and integration. This portion of the facility demonstrates the many challenges that a large production facility — home to a couple thousand employees — must meet, including safety, international compliance, operational security, and internal Raytheon policies. This offsite location truly demonstrates the partnership that industry and DSS must maintain to successfully and securely provide defense technology to our warfighters.

Shortly after my PWI experience, members of the Raytheon security team traveled to Las Vegas to receive the James S. Cogswell Award for Industrial Security Achievement. The security staff of Raytheon was very proud of this achievement, and worked hard to attain this level of success.

Throughout my visit they routinely emphasized the importance of their partnership with DSS, and gratitude to their local industrial security representative and field office for the robust support they receive.

I strongly encourage DSS personnel, particularly new employees that may have limited exposure to large-scale production facilities, to participate in the Partnership with Industry experience. Although classrooms and computer-based training are essential to our professional education and development, I am a firm believer that there is no substitute for the hands-on learning experience that PWI provides.

Capital Region field offices convene for blended

by Pamela Hunter
Maryland Field Office

The field offices within the Capital Region took integration to another level recently, collaborating with peers and colleagues during a three-day blended training session offered to 25 industrial security professionals within the seven Capital Region field offices.

Given today's constrained budget environment, the training allowed the region to make the most of training dollars while including a larger audience. The field offices partnered with the Center for Development of Security Excellence (CDSE) to host an outside course conducted by Reid & Associates, Inc., in Linthicum, Md.

The "Interviewing and Interrogation" course taught attendees different strategies for conducting interviews of cleared and uncleared employees at cleared defense companies. Talking to contractor employees is a critical piece of the DSS assessment model.

"The class helped me realize how body language and voice tone can reveal the attitudes and principles of not only the person being questioned but also of the person who is asking the questions," said Shelby Oros, an industrial security specialist in the Chantilly Field Office. "The videos shown during the three-day class depicted verbal and non-verbal channels of communication across several scenarios so that we could see the role that the interviewer plays in keeping the subject's attention and that by asking open-ended questions or questions that solicit more than a yes/no answer, attendees learned how to achieve a detailed response."

Huntsville CI-focused working group explores threats to classified information systems

by Mark Schoenig
Huntsville Field Office

What began as a vision shared by the counterintelligence special agents (CISA) and information systems security professionals (ISSP) of the Huntsville Field Office evolved into a CI-focused working group that explores threats to classified information systems from both the insider and advanced cyber threat perspectives.

The concept leverages both CI and information systems security disciplines working together to identify and mitigate real-time threats to classified information systems in industry.

The first Information Systems Security and Counterintelligence (ISSC) Working Group formed in November 2012, and has garnered high interest and participation within the Huntsville industry community, as attendance regularly totals 50 or more participants. The working group was designed for the information system security managers (ISSM) working with classified systems/networks, other government partners, and DSS ISSPs and CISAs.

Industry attendees normally range from companies with highly complex classified networks and systems to smaller multi-user standalone systems.

Also included are technical specialists who benefit from the information to senior officials and security personnel looking to gain a broader perspective of the risks and to better understand defensive policies.

The meetings, organized by DSS, supported by the local NCMS Mid-South Chapter, and hosted by Lockheed Martin Space Systems in Huntsville, begin with formal presentations on insider and cyber threat information provided by DSS CI and other government partners, presentations from industry partners, and DSS ISSPs.

The agenda then opens up for discussions with a focus on common interests to proactively mitigate risks and threats with an "outside-the-box" approach. The focus in on what make sense and to share good ideas; not requirements.

Recent meetings focused on insider threat and the ways to monitor and control "output" from classified systems, which results in a huge benefit to mitigating the insider threat. The group has also shared such varied ideas as user profile audits, output control, insider threat indicators, importance of cross communication, supply chain risk, external media risk, patch management, hardware spot checks, auditing, incident response actions, and operational security concerns in initial reporting.

DSS adjourns each meeting with a tasking for everyone to continue researching ways to accomplish the various objectives within their environment which inspires the group to share ideas during the next meeting.

What started as a vision in 2012 has received growing attention from the Huntsville security community, with individuals asking to be added to the group, resulting in opening the 2015 agenda to a broader ISSM/ISSO group.

training on how to conduct effective interviews

Gaining additional suspicious contact reports has always been a challenge. We often wonder if we're asking the right questions during our assessment and how can we get more reporting from industry. The instructor helped the participants to rethink or improve the way they currently conduct interviews.

As a result of this training, employees developed new ways to pose questions while some revamped the way they conduct interviews during security vulnerability assessments. The training enabled individuals to learn different techniques on how to evaluate one's attitude and verbal and non-verbal behaviors as well as how to develop positive confrontations. The secret to a successful interview is to be prepared, develop questions beforehand, and put the interviewee at ease (i.e., engage in casual conversation before jumping right into the interview).

One industrial security specialist volunteered to do a mock interview at a cleared company using the techniques learned from this training in hopes of gaining more information from industry as it pertains to suspicious activities and identifying potential insider threats.

"The training administered by Reid & Associates provided me with additional skills in the areas of interviewing techniques, as well as reading body language," said Dessie Howard, industrial security specialist with the Hanover Field Office.

Integration through this training touched all DSS disciplines, directly and indirectly, while leveraging the support and subject-matter expertise of internal and external partners to further enhance the knowledge and skills of the DSS workforce.

REMAINING VIGILANT: John Wetzel, CI special agent, leads a group discussion on behaviors of the insider threat.

"The PSMO-I presentation was very informative. We have so many questions, and this was a great forum to ask questions and learn from what others have experienced." – **Nicole Gray**, *FSO*

"The Counterintelligence Insider Threat briefing was great! It helped me gain better insight as to what DSS is looking for and what the mission entails." – **Kevin Perry**, *FSO*

Andover Field Office partners with industry

by Kathryn Kimball
Andover Field Office

On June 16, industrial security representatives, information systems security professionals, counterintelligence special agents and the leadership of the Andover Field Office, collaborated with two cleared contractor facilities to host the 2nd annual Partnership with Industry (PWI) Day.

The event, which included approximately 73 security staff representing 60 cleared contractor facilities, was led by Industrial Security Representative Clement LaShomb.

The event originated in 2013, as a day for the security staff of smaller cleared facilities to come together and ask questions, network with other facility security officers, and discuss best practices. The PWI Day featured a full agenda of speakers from the Andover Field Office, covering a variety of topics to include insider threat, social media awareness, certification and accreditation process, common deficiencies in security plans, and DSS history.

Additionally, Larry Paxton, of the Personnel Security Management Office for Industry, provided information on Data Quality Initiatives and what they mean, personnel security clearance statistics, and the FSO role in personnel security. The NCMS New England Chapter president also spoke.

The day concluded with a panel of DSS subject matter experts answering questions from the audience.


BAE SYSTEMS LAND & ARMAMENTS, LP;
Clara, Calif.
CHARLES STARK DRAPER LABORAT
DCS CORPORATION; Shalimar, Fla.
Cambridge, M
DRS POWER TECHNOLOGY; Fitchburg,
LOCKHEED MARTIN CORPORATION – MISSION SYSTEMS & TRAINING; Orlando, Fla.
GENERAL DYNAMICS ADVANCED INFORMATION SYSTEMS, INC.; Oakton, Va.
THE PRO
GROUP
Miami La
TEXAS
UNIVE
College Sta
ALLIAN
GENERAL D
LOCKHEED M
RAYTHEON COMPANY; Arlington, Va.
L-3 SYSTEMS COMPANY; Camden, N.J.
SCIENTIFIC RESEARCH CORPORATION; Atlanta, Ga.
IGOV TECHNOLOGIES; Tampa, Fla.
CROWELL & MORING
VENCORE SERVICES & SOLUTIONS, INC.; Brook Park, Ohio
GENERAL DYNAMICS C4
RAYTHEON COMPANY; Tucson, Ari
L-3 UNIDYNE; Middletown, R.I.
JACOBS TECHNOLOGY; Tullahoma, Ten
DRS SENSORS & TARGETING SYSTEMS, INC.; Cypress, Calif.
BAE SYSTEMS TECHNOLOGY SOLUTIO
BATELLE COLONIAL PLACE OPERATIONS; Arlington, Va.