



DSS

ACCESS

OFFICIAL MAGAZINE OF THE DEFENSE SECURITY SERVICE

Volume 3, Issue 3

Best of the Best

2014
Cogswell
Recipients



FALL 2014

Volume 3, Issue 3



SPOTLIGHT

The Best of the Best: DSS Recognizes 2014 Cogswell Recipients 4

Inside

DSS Supports Annual NCMS Training Seminar, Nets Itself Two Awards in the Process! 12

DSS Office of Innovation: Open for New Ideas 22

Future-Scenario Planning Workshop Looks Over the Horizon 24

Third Trip Down Under 26

CDSE Makes Toolkits Mobile 27

Final Certification Program Submitted for National Accreditation 27

CDSE Advanced, Graduate Courses Reaching a Wide & Diverse Audience 28

DSS Hosts Second Annual Take Your Child to Work Day 30

DSS Kicks Off Non-Paid Student Volunteer Internship Program 31

DSS Remembers

Oklahoma City, Police Week and Memorial Day 14

Ask The Leadership

A Q&A with Randy Riley, Office of the Designated Approving Authority 16

Deciphering the Acronym

What is a CSO? 19

Transformative Military Technologies

Third in a Series: Landships 20

Around the Regions

Alexandria Field Office Chief Retires from Air Force Reserve 32

Bath Iron Works Hosts DSS Deputy 33

Hittite Microwave Corporation Receives DSS Counterintelligence Excellence Award 33

Adverse Information: A Story of Personal Impact 34

DSS ACCESS

Published by the Defense Security Service Public Affairs Office

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

DSS Leadership

Director

Stanley L. Sims

Deputy Director

James J. Kren

Chief of Staff

Rebecca J. Allen

Chief, Public Affairs

Cindy McGovern

Editor

Elizabeth Alber

Graphics

Steph Struthers

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

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

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

FROM THE DIRECTOR



This issue of ACCESS features a lengthy section on the DSS support to NCMS and the presentation of the 2014 James S. Cogswell Awards. This annual NCMS training is one of the largest and most important events DSS supports each year. We had many subject matter experts from across the agency provide training sessions during the week as well as employees attend the training sessions to advance their professional development. With over 1,500 security professionals in attendance, it was a perfect opportunity to share information, network and learn from each other.

In addition, the Center for Development of Security Excellence (CDSE) and the San Antonio Field Office were both recognized by NCMS for their support to the industrial security community. CDSE received the 2014 Donald B. Woodbridge Award of Excellence, which is presented to organizations in recognition of excellence in the general field of classification management and industrial security. The San Antonio Field Office received the NCMS Industrial Security Award, which is presented to organizations whose contributions improve security procedures, practices or policies of national interest. Both awards were well deserved and reflect the DSS embrace of partnership with industry and commitment to excellence.

During the week-long event, we presented the Cogswell Award to 40 facilities. Since I arrived at DSS, the number of companies recognized with a Cogswell Award has increased each year, and this year's group of 40 award recipients was the largest in recent years. I want to again congratulate each of the recipients and thank them for their commitment to the National Industrial Security Program. Several of the recipients have contributed articles on how they achieved the award and offered insights into successful security programs. Their advice is applicable to any organization seeking to establish and maintain a high quality program.

Finally, I draw your attention to the article on the Oklahoma City Memorial and our participation in the annual memorial marathon. This is the first time DSS employees — on their own time — supported the marathon, and I hope this becomes an annual event, just as our attendance at the annual ceremony has. We have an obligation to never forget our colleagues killed in the bombing of the Alfred P. Murrah Federal Building on April 19, 1995. Events such as these serve to keep their memory alive and ensure each DSS employee knows and continues to honor their sacrifice.

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



THE BEST OF THE BEST

DSS Recognizes 2014 Cogswell Recipients

On June 17, 2014, the Defense Security Service presented the annual James S. Cogswell Outstanding Industrial Security Achievement Award to 40 cleared contractor facilities. The winning facilities represent the "best of the best," and their security programs stand as models for others to emulate. These 40 facilities represent less than one percent of the over 13,500 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. This year's training event was the 50th for NCMS. In his remarks announcing the Cogswell winners, Stan Sims, DSS Director, hailed the 50-year milestone, as well as changes in the security environment during that time.

Sims noted that in 1964, IBM rolled out the OS/360, the first mass-produced computer operating system. Using the system, all computers in the IBM 360 family could run any software program. At that time, IBM controlled 70 percent of the computer market worldwide, and Steve Jobs and Bill Gates were still in elementary school.

Today, Sims said that computers — in some form or another — help drive our cars, direct us to work, allow us to download books and newspapers, will be small enough to fit on our glasses, and are taught in elementary school. The prevalence of computers led the Department of Defense (DoD) to establish U.S. Cyber Command, a military command dedicated to strengthening DoD cyberspace capabilities and integrating and bolstering DoD's cyber expertise.

President Barack Obama has declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation," and that "America's economic prosperity in the 21st century will depend on cybersecurity."

"I share this trip down memory lane to again laud NCMS on this

milestone," said Sims, "but also to set the stage for today's security environment. The environment we face is complex, multi-faceted and immediate.

"The James S. Cogswell award is presented each year to those facilities that have achieved outstanding success in implementing the National Industrial Security Program within their facilities. These are the companies who understand the complexity of the environment I just described," continued Sims. "They go above and beyond the minimum requirements expected of them to serve as



leaders in the community. They are actively positioning themselves to address the next 50 years of change."

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

2010 — 9 facilities
2011 — 17 facilities

2012 — 26 facilities
2013 — 24 facilities

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

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 in the running for the award.

Of the 13,500 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 leadership 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 2014 award recipients include a balance of both large and small companies, including two category "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.

In closing, Sims said, "I can say that each of these recipients show clear management and corporate commitment for 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 because of your willingness to be a partner with DSS that we honor you as well as your achievement."

The 2014 Winners:

DSS is proud to recognize the following recipients of the 2014 Cogswell award:

- **Aerospace Corporation** *Albuquerque, N.M.*
- **Alliant Techsystems, Inc.** *Arlington, Va.*
- **Alliant Techsystems Operations LLC** *Elkton, Md.*
- **Aptima, Inc.** *Woburn, Mass.*
- **Arcata Associates, Inc.** *Las Vegas, Nev.*
- **BAE Systems Information Solutions, Inc.** *Bellevue, Neb.*
- **BAE Systems Land & Armaments L.P.** *Louisville, Ky.*
- **BAE Systems Land & Armaments L.P.** *Arlington, Va.*
- **BAE Systems Technology Solutions & Services, Inc.** *Fort Walton Beach, Fla.*
- **Bechtel National, Inc.** *Reston, Va.*
- **The Boeing Company** *Huntington Beach, Calif.*
- **Booz Allen Hamilton, Inc.** *Norfolk, Va.*
- **General Dynamics C4 Systems, Inc.** *Taunton, Mass.*
- **Honeywell International, Inc., Aerospace** *Minneapolis, Minn.*
- **Jacobs Technology, Inc.** *Oxnard, Calif.*
- **L-3 Communications Corporation** *New York, N.Y.*

- L-3 Fuzing and Ordnance Systems, Inc.
Cincinnati, Ohio
- Lockheed Martin Corporation — Center for Innovation
Suffolk, Va.
- Lockheed Martin Corporation — Information Systems & Global Solutions
Papillion, Neb.
- Lockheed Martin Corporation — Information Systems & Global Solutions
King of Prussia, Pa.
- Lockheed Martin Corporation — LM Security Operations Center
Orlando, Fla.
- Lockheed Martin Corporation — Missiles & Fire Control
Goleta, Calif.
- Lockheed Martin Corporation — Missiles & Fire Control
Ocala, Fla.
- Lockheed Martin Corporation — Mission Systems and Training
Fort Worth, Texas
- ManTech Systems Engineering Corporation
Panama City Beach, Fla.
- The MITRE Corporation
Huntsville, Ala.
- Northrop Grumman Systems Corporation
Middletown, R.I.
- Northrop Grumman Systems Corporation
Charlottesville, Va.
- Northrop Grumman Systems Corporation Information Systems (Cyber & SIGINT Systems)
McClellan Park, Calif.
- QinetiQ North America, Inc.
Reston, Va.
- Raytheon Company
Omaha, Neb.
- Raytheon International, Inc.
Arlington, Va.
- Retlif Testing Laboratories
Ronkonkoma, N.Y.
- Rockwell Collins, Inc.
Cedar Rapids, Iowa
- Rockwell Collins Simulation & Training Solutions LLC
Orlando, Fla.

Cogswell Award Redesigned

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

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

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

The award itself was largely unchanged since its implementation and included certificates for the security staff as well as a plaque that was presented on-site at each facility. In recognition of the 50th anniversary of NCMS, DSS updated the award to represent excellence in security and the partnership between government and industry.

The final 2014 award is a plaque design that contains a cherry wood-color finish with the DSS agency's emblem in gold. In addition, there is a gold plated eagle abstract design that individually highlights each Cogswell winner.

The design creates a powerful consistent look and continues the legacy of the DSS Cogswell story tradition.

** Images depicted on the cover and throughout this article are photoillustrations and do not represent the actual Cogswell award.*

- Securitas Critical Infrastructure Services, Inc.
Springfield, Va.
- Signature Science, LLC
Austin, Texas
- Smartronix, Inc.
Hollywood, Md.
- Spectral Sciences, Inc.
Burlington, Mass.
- The University of Texas at Austin, Applied Research Laboratories
Austin, Texas

How They Did It

A representative sampling of the 2014 Cogswell winners were invited 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. >>

Neil Fox

Facility Security Officer
Applied Research Laboratories

The University of Texas at Austin

Applied Research Laboratories at the University of Texas in Austin (ARL:UT) has been conducting classified research for the U.S. Government since 1946. There are approximately 700 employees at ARL:UT, each of whom contributed in some way to this achievement.

Our security practices and procedures are tailored for ARL:UT but aren't necessarily unique; they contribute to the success of our security program but only in part. To a larger extent, I believe the success of our security program and the achievement of this award can be attributed to training and organizational climate.

Simply stated, there is no substitute for good training. The success of any security program hinges on quality training for both the individual employee and the security staff. Security training for employees must be more than an "X" in the block or a one-time event to meet an administrative requirement.

Effective training is a challenge and requires considerable effort on the part of security, as well as strong support by upper management. Our approach has been to provide employees with interesting events, informative briefings, captivating speakers as well as informative emails and periodic newsletters throughout the year. Training and professional development for those who work in security is also very important; it establishes credibility.

At every opportunity, formal training is made available to members of the security staff. Professional development is endorsed and supported by upper management. Security staff members regularly attend NCMS, DSS, FBI, CIA and other professional training events. Memberships in professional organizations (to include NCMS) are paid for by ARL:UT, and the Facility Security Officer (FSO), Information System Security Managers and Contract Program Security Officers are each certified industrial security professionals.

Training alone, however, is not enough; in order to have a good security program you must also have an organizational climate that is conducive to security, or 'security-minded'. Security must be an integral part of the behaviors, attitudes and feelings of the employees.

ARL:UT scientists have come to understand that security is an enabler rather than a barrier, a positive rather than a negative. They know and understand that the purpose of the security office is to support their research and that the folks who work in security are dependable, knowledgeable and above all, credible.

There are no shortcuts when it comes to building an outstanding security program; it takes time and patience. And by patience, I mean it has been 30 years since ARL:UT last achieved this award.

Attitude is an important factor in achieving the Cogswell. It begins with the FSO and his/her approach to the job. For me, attaining the Cogswell Award has always been a goal but never an obsession. As an FSO, you have to believe it's achievable and then instill that belief in your security staff, even after receiving a grade of less than 'superior' on your Security Vulnerability Assessment.

Over the years, we have learned from our inspections, reviews and assessments, using the results to consistently improve 'satisfactory' ratings to 'commendable' and 'commendable' ratings to 'superior'.



Lee Folsom

Facility Security
Officer,
Lockheed
Martin Missiles
and Fire Control

Ocala, Fla.

I've been the Facility Security Officer (FSO) for Lockheed Martin's Ocala, Fla., facility for 16 years, and I am both proud and humbled to receive the James S. Cogswell Outstanding Industrial Security Achievement Award for the second time on behalf of the facility and security organization. As a full-service manufacturing operation with a highly skilled production workforce, success involves clear objectives and a lot of people working together in the pursuit of security excellence. Today, we need to be flexible and proactive in our applications, yet unbending in meeting the security requirements placed upon us.

Over the years I've had the pleasure of working with many different DSS personnel. While working with them, I've learned the value of communicating clear objectives, building partnerships and developing meaningful working relationships.

The Ocala facility has received 13 consecutive "superior" ratings. How did we achieve such a record? Our goal is not to obtain the "superior" rating or "Cogswell Award," it's about doing the right thing; the recognition is an added bonus. It is hard to put a finger on just one contributing factor for our success. Understanding our products and customer's needs, remaining audit ready at all times, and knowing the information that needs to be protected and the risk of unauthorized disclosure has aided us in ensuring a successful security program.

Listed below are additional events and resources that allowed our security program to be successful:

- I conduct self-assessments every six months plus host an enterprise self-inspection team prior to my DSS assessment.
- I attend and participate in the Florida Industrial Security Working Group (FISWG) meetings and readily share the information with the Ocala workforce.
- We provide security education to the workforce via pamphlets, posters, TV screens, counterintelligence briefings, one-on-ones and group meetings, etc.
- I have the support of the senior management team, which creates the ability to share company-wide tools to track our audits, share enhancements and contact subject matter experts throughout the corporation when needed.
- I walk the floors, interacting with the workforce, making myself available to answer any questions or concerns.
- My best assets are the Ocala employees themselves, from top management to assemblers on the production line. Many employees have family members in the military who use our products every day. We do what is right and never forget who we are working for — the warfighter.
- I use the training tools on the DSS website, which has improved a lot over the last few years.

Two key items I use that could benefit all:

The first is my "**FSO book**," which is a binder I organize with proof of all compliance-related items such as: facility clearance forms, personnel security documentation, authorizations, computer security plans, communications security information, past DSS and self-assessment results and many other items.

The second is a "**Matrix book**." The book has a tab for each enhancement category along with its definition and examples of implementation. We use this information as a guide to implement various security tools and programs for the Ocala workforce. I also include documentation to validate the tools and programs are in place, thus creating a more effective security program.

It is very important to build a trusting relationship with your DSS representative. You should know what and how your representative wants to communicate, receive reports, etc. It's my belief that the organizational skills of the FSO and matrix books makes it easier for DSS to conduct the assessment and helps build trust between the FSO and the DSS Representative resulting in a great partnership.

Having all of your required data prepared and organized prior to your DSS assessment creates a one-stop shop, saving time during the assessment and providing a good tracking system to ensure you have enhancements for applicable categories and that your security program is effective and compliant.



Sam DeSante

Facility Security Officer
Lockheed Martin Corporate

Orlando, Fla.

DSS presented the annual James S. Cogswell Outstanding Industrial Security Achievement Awards on June 17, 2014. During opening remarks, Director Stan Sims stated, "Companies don't win Cogswells, people win Cogswells." This certainly is true in the case of Lockheed Martin.

The Lockheed Martin Security Team brings unparalleled experience in protecting classified information, systems, facilities and personnel clearance processing to support our customers' classified missions.

Lockheed Martin has a number of security working groups designed to collaborate and develop enterprise-wide tools and processes to aid our security professionals. Our security team supports 113,000 employees and 160 facilities around the world.

The team's passion from top to bottom is second-to-none. Senior leadership is committed to security excellence and sends a clear message to all employees and customers; we are dedicated to providing the highest level of support. By leveraging enterprise-wide tools and infrastructure, Lockheed Martin has established a best-in-class industrial security program.

The combination of our Orlando Security Operations Center, which processes and maintains more than 63,000 clearances across the corporation, and our Security Management and Reporting Tool (SMART), which provides an enterprise-wide approach to sharing audit data, allows Lockheed Martin to identify audit trends and areas of risk, and share best practices.

It also allows me to leverage consolidated personnel security management and traditional National Industrial Security Program compliance and provide a security program consistently recognized as one of the best in industry.

To maintain a successful security program, all members of the security team and leadership must be dedicated and believe in the mission. To be successful, our security team communicates and executes the proper training to ensure the message our security program has established starts from the moment an employee signs an offer letter to the day they retire.

Our security team is there to guide and educate our employees and we continue to ask ourselves, "What threats may affect our facilities and our program? How can we improve our processes and procedures? If a security program is as strong as its weakest link, what is that link?"

Our constant focus on these questions, coupled with a strong partnership with our DSS representative, programs, customers, and security community, allows Lockheed Martin's security program to function at a superior level on a daily basis.



Ellen Bertuccelli

Northrop Grumman
Security Manager/
Facility Security Officer

Sacramento, Calif.

To prepare for the annual DSS assessment, our facility completes a very thorough annual self-inspection. We utilize the NISP self-inspection checklist and provide evidence and examples for each answer. The key to a good self/pre-inspection is to be thorough and self-critical.

I divide up the self-inspection sections, giving each staff member a section not in line with their normal daily responsibilities. As staff members complete their assigned sections, they interview their coworkers on their assigned responsibilities, asking for evidence and compiling data. This adds a degree of objectivity, since staff members are not responsible for inspecting their own area of expertise. This also has proven to be an excellent and efficient means of providing cross-training. The key is to document all results — positive and negative — and provide them to the DSS representative before or at the beginning of the assessment.

Our employee population is involved in our security program year-round and especially during the self-inspection. One tool we developed is a security questionnaire that we send to all employees. The responses reveal a great deal about our program and show areas where we need to pay more attention. The questionnaire also reveals possible misunderstandings and identifies areas that we need to address.

Our employees also are involved during container checks and document inventories, which helps them understand and buy into the processes. We also hold an open house where we provide information and personnel to answer questions. We invite representatives from our local Sheriff's Department, DSS and our FBI counterintelligence group. It is very well received and supported.

Self-inspections should not be the only time that security employees are seen or heard. Security staff must interact with all employees — both cleared and uncleared. Having employees as an everyday part of the security program is essential to a successful self-inspection, inspection and program as a whole. I am proud to say that our employees are a vital part of our successful security program.

Our company has always had a strong security education program, including posters, websites, newsletters, daily reminders, briefings, re-indoctrinations, etc. But even with all of those efforts, we realized that we needed to step up our game to really get the attention of our employees.

To accomplish this we turned our security reindoctrinations into game show challenges. Our first was "Are you Smarter than a Security Person?" We held several sessions where we carefully selected our contestants and divided the room into two teams. The security staff was at the front and the challenge was on.

While the sessions were fun, we realized after that they had a serious result. Employees were reporting things that they hadn't reported in the past and were proactively discussing issues with us. Through the game we had created a new relationship with our employees. After that, the biggest challenge was to keep the games fun and fresh. We followed with a takeoff of Jeopardy and Family Feud.

We also purchased life size people to hold our security messages. We have characters such as The Godfather, John Wayne, Captain America, Wizard of Oz, Anchorman and Austin Powers. We change the messages and move them throughout the building often to keep interest high.

Our latest activity was held earlier this year when we held an awareness event called "Catch Me If You Can" — an interactive game where employees tried to figure out who in the crowd was playing the role of foreign intelligence officer, insider threat, suspicious person and social engineer. Everyone received a card describing each character and voted on who they thought was playing each role.

An effective security education program must appeal to employees and, more importantly, include employees as participants, not just passive observers. Making it entertaining and interactive is a great way to communicate important security messages and raise awareness in a way that will not be easily forgotten.

QinetiQ North America, Inc., is foreign-owned and operates under a Proxy Agreement, which introduces additional security requirements and complexities. Consequently, we concentrate on traditional and FOCl [Foreign Ownership Control or Influence] areas of security that are high-value/high-reward. These areas are reinforced with our core principles of mandatory compliance and risk-based methodology, which are essential to the success of our program.

Training and awareness is one of our primary focus areas because the benefits and return on investments are perpetual — especially with cyber security. Arguably, cyber is the most dynamic and daunting challenge we face today; therefore, we refresh our training program regularly to include trending threats generated from social media and current events. Government-required training is also conducted to ensure compliance.

Our security program is further strengthened by requiring our Facility Security Officers (FSOs), Technology Control Officers (TCOs) and cyber security team to participate in their respective training programs, conferences and seminars. This enables them to stay current with government compliance standards and industry best practices.

Additionally, our parent organization plays a key role in our compliance program. They demonstrate their commitment by delivering initial/refresher proxy training to their employees who communicate with QinetiQ.

Electronic communications are the centerpiece of our proxy program and generate a lot of attention because of their high-volume activity levels. To preempt potential FOCl issues, we exceed minimum requirements by reviewing all electronic communications between the company and our parent vice only conducting a "sampling" of that traffic.

Information systems assurance presents the highest risk area for all of us, regardless of sector — defense or commercial. While our security controls are consistent with industry standards (NIST 800-53, ISO 27001), it is equally important how they are deployed and integrated into and throughout our environment. As such, we employ a defense-in-depth (or layered) approach — implementing defensive controls at the perimeter and working our way to the innermost asset in a layered manner. Furthermore, we continually look for enhancement opportunities.

Site visits/audits are paramount to ensure all the security controls and processes put in place are actually working. Visits are conducted by our FSOs/TCOs to assess the security posture at our facilities, and we use this information to make necessary corrections/adjustments. Additionally, our Chief Executive Officer, Chief Operating Officer and Proxy Holders conduct site visits to show commitment and support from the very top and put compliance in the forefront of company goals.

Lastly, policies/procedures/processes are regularly reviewed to determine if they are effective, still relevant, or if new ones are needed to properly address issues and mitigate risk.

Given the intricacies of securing a FOCl company that is submerged within a threatened global digital landscape, it is imperative to have a security program capable of combatting current, emerging, and future threats in a formidable manner.

Editor's Note: Since the writing of this article, QinetiQ North America, Inc. (QNA) has been sold to The SI Organization, Inc. and has changed its name to Vencore Services and Solutions, Inc. (Vencore™). As a subsidiary of The SI, Vencore is no longer foreign owned or operated under a proxy agreement.

Chilly Williams

Senior Vice President &
Chief Security Officer

QinetiQ North America, Inc.





Photo courtesy of NCMS

Kevin Jones (left), Director, DSS Center for Development of Security Excellence, accepts the the highest honor NCMS bestows for outstanding contributions to the profession of classification management/information security, the 2014 Donald B. Woodbridge Award, from Leonard Moss, NCMS President.

DSS SUPPORTS ANNUAL NCMS TRAINING SEMINAR

Partnership with industry has been a guiding force at DSS since the arrival of DSS Director Stan Sims in 2010. Evidence of that partnership was clearly exhibited at this year's annual NCMS training seminar. NCMS, The Society of Industrial Security Professionals, hosted its 50th Annual Training Seminar at National Harbor, Md., in June.

Since its inception, NCMS has hosted an annual conference where members and other security professionals from both government and industry gather to learn the latest in the protection of national security information. As NCMS celebrated "50 Years of Excellence in Security Education," the program exceeded all expectations and benefited a great deal from its partnership with DSS.

The event included more than 1,500 participants who attended a wide range of seminars and training sessions for the new and seasoned security professional. The topics covered included: Facility Security Officer best practices, personnel security, insider threat, counterintelligence, adverse information reporting, emerging threats, and critical unclassified information.

The sessions were further divided into workshop tracks such as

Facility Security Officer; professional growth; International Program; SCI/SAP training; security application tools; cybersecurity and Information Security. DSS subject matter experts presented training sessions on the rating matrix, the personnel security clearance process, Office of the Designated Approving Authority Business Management System and foreign intelligence targeting of cleared industry and participated in a number of panel discussions.

In recognition of this continued support to not only NCMS but the larger industrial security community, two DSS offices were presented with awards during the seminar.

The San Antonio Field Office, with Rick Hibbs as the Field Office Chief, received the Industrial Security Award. The office was nominated by the Texas Gulf Coast Chapter of NCMS. The San Antonio Office is the second field office to receive the award — the Virginia Beach Field Office was recognized in 2013.

The Industrial Security Award is awarded to an individual or organization that has significantly contributed to industrial security and meets a minimum of two of the following criteria:



Photo courtesy of NCMS

The San Antonio Field Office received the 2014 NCMS Industrial Security Award. Representing the San Antonio Field Office are (from left) Field CI Specialist Pete Henning, Senior Industrial Security Specialist Dawn Martin, Field Office Chief Rick Hibbs, and Senior Industrial Security Specialist Betsy Bruinsma.

AND NETS ITSELF TWO AWARDS IN THE PROCESS!

- Individual or organization that has materially and beneficially affected the security community (i.e., functional areas include education, training, operations or like activities which improves or enhances individual, organizational or corporate performance);
- Individual or organizational contribution which improves security procedures, practices or policies of national interest (i.e., develop partnerships between industry and government, involvement in Industrial Security Awareness Councils, industry teams, etc.);
- Individual or organization continuing contributions to the Society by enhancing the mission, vision, and goals of the Society;
- A member or associate member in good standing.

The Center for Development of Security Excellence (CDSE) was recognized at the President's Dinner with the Woodbridge Award. The Woodbridge award is named for Donald B. Woodbridge, past president of NCMS and is the highest honor NCMS bestows for outstanding contributions to the profession of classification management/information security.

In presenting the award, Leonard Moss, President of NCMS said the award recognized the development and delivery of stellar training programs that are relevant and cutting-edge and that effectively address the critical needs of government and industry national security professionals around the world.

"CDSE's strong commitment to excellence and long standing partnership with industry has made exceptional contributions to the national security landscape," Moss added.

Stan Sims, DSS Director said in acknowledging the award, "This recognition is a testament to the superior efforts CDSE has put forth to develop a top-notch security education and professionalization program.

"I want to personally congratulate the CDSE team on this achievement; you are blazing trails for the entire security community as well as for DSS. I appreciate and value the tremendous amount of effort you have put into making CDSE a model, not only for the Department, but also for the entire U.S. Government."



The Field of Empty Chairs at the Oklahoma City Memorial commemorates those lost in the bombing of the Alfred P. Murrah Federal Building.

OKLAHOMA CITY

Since the bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995, DSS has marked the occasion in a number of ways.

There is a cherry tree planted along the Tidal Basin in Washington, D.C. in honor of the victims. An Oklahoma red bud was planted outside the agency headquarters at Braddock Road. The addition to the Russell-Knox Building at Marine Corps Base Quantico will feature a memorial to the five employees killed that day.

Since arriving at DSS, Chief of Staff Rebecca Allen has made attending the annual memorial service for the victims a priority. She has also reached out to, and kept in touch with, surviving family members to let them know DSS has not forgotten their sacrifice.

This year was no different and Kevin Jones, Director, Center of Development for Security Excellence, represented DSS at the 19th Anniversary Remembrance Ceremony.

Jones was the chief of the Investigations (i.e., personnel security investigations) Division of the DSS Personnel Investigations Center (PIC) in 1995. "I had direct interaction with the various field offices that produced reports of investigation from around the country. We, at the PIC, personally 'knew of' the individuals who were killed and interacted with them professionally on a routine and recurring (weekly) basis."

It was Jones' first visit to the memorial and the museum. "I'm glad I was able to attend," he said. "I remember that day very vividly. I was honored to represent the agency and meet with the family members."

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



DSS employees and family members from the Irving Field Office gather before the race (from left): Jennifer Norden, field office chief; Steve Runyan; Kathi Runyan, senior industrial security representative (SISR); Brian Murphy, senior action officer; Darren Dennard, SISR; and Tom Vaughan, ISR.

Employees of the Irving Field Office and Southern Region opted for a more rigorous show of support by running in the Oklahoma City half-marathon and five kilometer race held on April 27, 2014. The races, which also include a full marathon, marathon relay and kid's run options, raise funds for the Oklahoma City National Memorial and Museum.

Brian Murphy, Regional Action Officer of the Southern Region, organized the runners and was the catalyst behind the entries. "We planted a simple seed, and it's been growing ever since," he said.

Murphy and the team arranged to meet the daughters and grandchildren of Norma 'Jean' Johnson who were also participating in the events. "I can say without hesitation all of us that participated had a great experience and plan to do it again next year," Murphy said. "It was truly moving standing on the grounds of the Murrah Federal Building and bonding with the family of Norma Jean Johnson in the wee hours of race morning."

Murphy also threw down the gauntlet for next year's race. "Next year's 20th anniversary events are supposed to be the biggest ones to date, so we're also hoping to make DSS' participation bigger and better as well! We saw this year's runs as a 'warm up' for next year, so we'll start bugging everyone around January 2015 to consider joining us!"

Running the half-marathon for DSS were Murphy and Darren Dennard, Senior Industrial Security Specialist. Running five kilometers for DSS were Jennifer Norden, Field Office Chief, Kathi Runyan, Senior Industrial Security Specialist and Tom Vaughan, Industrial Security Specialist. Also running were family members Lisa Murphy (spouse of Brian Murphy) and Steve Runyan (spouse of Kathi Runyan).

Acknowledging that not all supporters could travel to Oklahoma City, Murphy asked DSS employees to commit to running or walking any challenging distance on either April 19th (anniversary of bombing) or April 27th (date of marathon) in remembrance the DSS employees. Ben Richardson, Chief, FOCI Division, did just that and completed his own marathon run on April 27.

POLICE WEEK

The Naval Criminal Investigation Service (NCIS) led the Russell-Knox Building community in a building-wide recognition of Police Week on May 13. President John F. Kennedy signed a proclamation in 1962 that designated May 15 as Peace Officers Memorial Day and the week in which that date falls as Police Week.

The nationwide observance recognizes the federal, state and municipal officers who have been killed or disabled in the line of duty.

Participating in the ceremony were Deputy Director Mark Ridley, NCIS; Air Force Brig. Gen. Keith Givens, Director, Air Force Office of Special Investigations; Army Col. Timothy Chmura, Deputy Commander, U.S. Army Criminal Investigation Command; and from DSS, Barry Sterling, Chief Financial Officer/Director, Business Enterprise.

A representative from each organization recited the names of their fallen as part of an end-of-watch roll call. The dates and stories of the fallen spanned decades and included Army CID Special Agent Walter Edward Snyder, who was killed in Germany in 1948 by a 17-year-old boy during an attempted prison escape.

More recently, AFOSI Special Agents Thomas Crowell, David Wieger, and Nathan Schuldheiss, were killed in 2007 when their vehicle was struck by an explosive device while on assignment near Balad Air Base in Iraq. Mike Monroe, a former NCIS agent now working in DSS Counterintelligence, recited the names of the five DSS employees killed in Oklahoma City, all with an end of watch of April 19, 1985.

MEMORIAL DAY

Stan Sims, DSS Director, led the Russell-Knox observance of Memorial Day with a wreath-laying ceremony on May 22. The ceremony continued a tradition started in 2012 year by DSS with invitations extended to the entire Russell-Knox workforce.

In his remarks Sims said, "Today, and on Monday, we will honor the memories of every man and woman who died in service to the Nation. The men and women for whom we lay this wreath were real people: sons and daughters, mothers and fathers, brothers and sisters, wives and husbands. They were young and full of promise, hope, and plans for their future. They were strong and vibrant. They loved and were loved. And they are missed."



Marine Corps Sgt. Jonathan Staples renders Taps during the Memorial Day observance ceremony.

Sims also read the epitaph that is engraved on the War Memorial to commemorate the men of the British 2nd Division who fell in the Battle of Kohima (Burma) in 1944.

***"When you go home
Tell them of us and say;
For your tomorrow
We gave our today"***

"By gathering here today," said Sims, "we are continuing that centuries-old tradition of honoring our fallen, and thanking them for their priceless gift.

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

Adding solemnity to the ceremony from Marine Corps Base Quantico were Cpl. Lloyd Boyde and Lance Cpl. Dennis Hillyer, who served as the Honor Guard and assisted Sims in placing the wreath, and Sgt. Jonathan Staples who rendered "Taps."



Randall (Randy) Riley has held the position of Assistant Deputy Director, Office of the Designated Approving Authority (ODAA), Industrial Security Field Operations, since August 2011. His staff is responsible for assisting with policy development, managing various aspects of the agency's National Industrial Security Program (NISP) certification and accreditation (C&A) program, and other projects in support of DSS Field Operations..

Prior to this position, Riley served as DSS southern region designated approving authority from 2006 until 2011. He was responsible for implementing and managing the NISP C&A program across the region's seven field offices covering 19 states.

In addition to managing the C&A program, Riley supervised a staff of more than 20 subordinate employees and first-level supervisors. Riley served as an Information Systems Security Professional in the southern region from 2004 until 2006.

Riley's Federal service also includes serving as an IT specialist with the Naval Security Group, Pensacola, Fla., and a number of assignments while on active duty in the United States Navy. Riley holds a Master of Science in Information Assurance and a bachelor's degree in Health Physics.

Since DSS began preparing to assume the Command Cyber Readiness Inspection (CCRI) mission in 2009, we have sponsored training and assumed a greater role in the inspections. Can you give us an update on where we stand with CCRI's? Any lessons learned and next steps?

DSS has obtained team certification from the Defense Information Systems Agency (DISA) and U.S. Cyber Command (USCYBERCOM) for two CCRI teams. DSS is now considered an "inspectable" agency and will be tasked directly by USCYBERCOM to conduct future CCRI's.

To date, 20 DSS Information Systems Security Professionals (ISSPs) and Industrial Security Representatives (ISRs) have completed training and received certifications for a variety of CCRI reviewer team positions. DSS and DISA will continue to work together and continue to offer training to certify additional team members.

DSS has begun conducting CCRI's separately from DISA and will continue to transition future CCRI's from DISA as our capacity grows. DSS will lead approximately 40-50 (50 percent) of the scheduled NISP contractor site CCRI's scheduled in FY15.

By far, the greatest "lesson learned" has been that system security must be viewed as an ongoing requirement, not

something to focus on just for a CCRI. All systems are required to be properly maintained from the beginning of life (i.e. initial accreditation) until the end of life, or disestablishment.

DSS has also captured additional "lessons learned" along the way in a document that identifies ways to streamline the SIPRNet circuit acquisition process as well as helpful hints regarding system configuration and other requirements.

Cleared contractors and sponsors may request a copy of the "DSS Lessons Learned" document by emailing disn@dss.smil.mil (on SIPRnet). When requesting the lessons learned, please include the following information in the body of the request:

- Company Name and address
- Cage Code
- Name of Requestor (FSO/ISSM/ISSO)
- Requestor's corporate email address
- Reason for the request

DSS will continue to train and certify staff to transition NISP CCRI work from DISA over the next year. Our ultimate goal is to establish dedicated DSS CCRI teams to enable efficient scheduling and execution of CCRI's while providing the best possible support for our industry partners and government sponsors.

DSS has directed all ISSPs to achieve Certified Information Systems Security Professional (CISSP) or other certifications that meet the DoD 8570 IAM Level III and IAT Level II requirements. How is that going? Do you see additional certifications or training that will be required for ISSPs?

All DSS information assurance personnel are required to obtain and maintain certifications in accordance with DoD 8570 requirements.

As a result, ISSPs are required to obtain and maintain DoD 8570 Information Assurance Manager Level III, and Information Assurance Technician Level II certifications.

Most ISSPs pursue the CISSP certification since it meets both requirements while others pursue two separate certifications.

Over the past three years, we have focused on workforce development, training, and professional certification across ODAA. As a group, our ISSPs have been very successful in obtaining the required certifications with over 85 percent of the ISSPs having already met the requirement and the remainder on track to complete the process over the next few months.

In addition, ISSPs and ISRs are also required to complete a rigorous training and certification program to conduct CCRI. The training process for each team role requires pre-requisite course work, on-the-job training, and finally an on-the-job "check-ride" during which a senior DISA reviewer monitors the DSS CCRI team member conducting a live CCRI as the final qualification check.

The training and certification requirement for conducting CCRI is always evolving and requires a significant investment of time and energy to remain certified.

The ODAA and the Center for Development of Security Excellence (CDSE) collaborated to create a new ISSP training curriculum, which kicked off in January 2014.

New and existing staff will complete the program, which includes elements from the traditional or physical side of the mission, as well as topics related to technical information systems.

The new curriculum offers a streamlined pathway to guide new ISSPs through training from entry on duty to full-performance. The training provides a consistent foundation for each ISSP to build upon as she/he progresses to more advanced roles within DSS.

The training curriculum was designed to be completed with little or no travel required with the exception of a future one- to two-week instructor-led capstone.

Like any agency or company, we experience turnover in our IT specialists due to the availability of other opportunities. Self-paced training allows new employees to enter on duty, complete training, and begin work in six months or less, thus minimizing turnover.

We are taking a close look at turnover and developing plans to offer career growth for and retention of our ISSPs.

The ODAA Business Management System (OBMS) just came online this summer. How will this affect the work of the ODAA? What do you see as the biggest benefit?

After the ODAA Business Management System (OBMS) was deployed in July, we entered into a six-month transition period. During the transition, each user of the system will activate an account and begin using OBMS.

Once a user account has been established, Information Systems Security Managers (ISSMs) should use either OBMS or the email attachment submission method during transition, not both.

OBMS training is available to familiarize users with the application based upon user role. All stakeholders will be required to obtain and utilize DoD Public Key Infrastructure (PKI) or acceptable External Certification Authority (ECA) credentials to log onto OBMS.

OBMS will streamline our Certification and Accreditation Process by providing a web-based portal for System Security Plan (SSP) submissions, a centralized repository to store official copies of SSPs, and an enhanced ability to produce program metrics and reports. >>

What are you seeing in industry that DSS will have to address in the next year or two, i.e. cloud computing? More sophisticated networks?

Yes, to all of these. Technological advances are occurring at a pace quicker than associated policy. Each new technology provides benefit, but also introduces new security challenges.

Across the NISP, programs and information systems are becoming more interconnected, which leads to more complex networks. In addition, convenient and cost-effective cloud computing services introduce new challenges for DSS and industry partners.

Although cloud technology may be convenient and easy to use, it introduces new security concerns requiring mitigating measures that may eliminate the perceived benefits and/or savings.

The NISP will also begin evolving over the next three-to-five years toward the "risk management framework" for system accreditation and oversight. Transition to the new processes will require training for internal and external stakeholders.

There used to be a lot of attention on timelines — IATO, ATO approval, etc. Are you still seeing challenges in meeting timelines?

Most systems receive a final authority to operate (ATO) within approximately 100 days from submission for accreditation. Over the past few years, we have been holding steady and providing an initial accreditation decision within approximately 30 days of submission for most systems.

We are also working to increase the number of straight to ATOs (SATO) issued for systems. A system going SATO bypasses the interim approval process, thereby avoiding not only the additional administrative work associated with processing an interim authority to operate (IATO), but also helping to reduce the potential security risk accepted when granting an IATO prior to visiting the site. We are currently processing SATOs on average of 24 days.

Any other topics you want our readers to know?

An updated ODAA Process Guide and accompanying SSP templates became effective on May 15, 2014. ISSMs use the Process Guide as a desk reference and "how to" guide during completion of the many complex tasks associated with obtaining and maintaining DSS accreditations for information systems.

The updated ODAA templates use a dynamic PDF design to make documenting system security configurations easier and more complete.

The templates serve as a simplified, easy-to-use structure for ISSMs to follow when documenting security configurations and special procedures applicable to their information systems.

The process guide, used in conjunction with the templates, guides the ISSM through the requirements for obtaining accreditation for information systems ranging from a simple desktop computer to a complex wide area network (WAN) spanning the country.

The resulting documentation is the government's official record of a system's configuration and the procedural requirements that users of the system are required to follow. Both the ODAA process guide and SSP templates represent a significant collaborative effort between DSS and our industry partners.

The NISP SIPRNet Connection Approval Process (NSCAP) v3 was released May 16, 2014. The NSCAP, formerly called DSS SCAP, was developed to provide step-by-step guidance for cleared contractors and their sponsors with contractual requirements to establish a connection to the DISN SIPRNet.

The NSCAP is based on established policy and guidance for non-DoD DISN (e.g. cleared contractor) connections documented in the DISA connection process guide. The updated NSCAP will provide industry with contact information and updated guidance on how to successfully obtain and maintain a compliant SIPRNet system.

The updated templates and NSCAP can be obtained by request from the ODAA mailbox (ODAA@DSS.MIL) by following the procedure outlined in the ODAA process guide. In addition, these documents (and others) are available for download by logging into OBMS.

WHAT IS A CSO?



By Keith Minard

Industrial Policy and Programs

National Policy defines a Cognizant Security Office or the CSO as the organizational entity delegated by the head of the Cognizant Security Agency or CSA to administer industrial security on behalf of the CSA (Amendment to 32 CFR, Part 2004, National Industrial Security Program (NISP) Directive No. 1).

What does this mean for DSS? In the case of DoD, the Secretary of Defense, the CSA, has delegated the CSO role to DSS.

As a result, DSS administers the NISP on behalf of the Secretary of Defense for the DoD components and 27 Federal agencies which have entered into agreements with the Secretary of Defense for industrial security services.

In this role, DSS serves as the face to industry in its oversight mission of over 10,000 contractors, licensees, and grantees that require access to classified information in the performance of their contracts at over 13,500 locations.

As the CSO for the Department of Defense, DSS ensures that facilities are eligible to receive classified information by ensuring measures outlined in the DoD 5220.22-M, "National Industrial Security Program Operating Manual," or NISPOM are in place to protect classified information in the possession of industry.

LANDSHIPS

HOW THE ADVENT OF TANKS CHANGED 20TH-CENTURY WARFARE

By Jeremiah Anderson

Protecting classified information and technology to maintain military superiority over our adversaries is of paramount importance to the United States. That edge today is represented by technologies such as the electromagnetic railgun and hypersonic and unmanned vehicles. These programs seek to extend capabilities already achieved via existing platforms, or to counter potential or emerging threats.

But battlefields exist in a constant state of flux, and during wartime, new technology can sometimes emerge out of necessity. Indeed, the last 15 years have seen an incredible evolution in vehicle armor technology. In

many cases, the material itself was not sensitive, but rather it was the manner in which it was arranged, manufactured, or fabricated.

Such was the case with the advent of the tank during the First World War. Both the Allied and Central Powers began with similar technology levels and capabilities. Britain's development of the tank did not bring a swift conclusion to a struggle that had degenerated into seemingly intractable trench warfare. However, the need to repel the new British weapon forced the Germans to respond with massive troop concentrations, which they could not sustain indefinitely.

If the tank's development had not been successfully kept secret, Germany might have been able to maintain parity by developing tanks or weapons and tactics to counter the tanks.

The Advent of the Tank

The British Landships Committee, formed by then First Lord of the Admiralty Winston Churchill, began work in February 1915, with the objective of developing a 'land battleship' to break the stalemate created by trench warfare. The British practiced disinformation by referring to the prospective vehicle as a "tank" to give the impression they were manufacturing water cisterns.

Britain's War Office prescribed that the Mark I tank, nicknamed 'Big Willie', should traverse a trench eight feet wide and climb obstacles four feet high. Big Willie was constructed of boiler plating, weighed 28 tons, and could travel only four miles per hour. The Mark I needed a crew of eight to 10 soldiers to fire the guns, steer the vehicle, and maintain and operate the finicky engine. After the Mark I was demonstrated to the Admiralty, the British Government placed an order for 100 tanks.

The tanks were given genders. Male tanks had a six-pound cannon (57mm) on either side of the tank, housed in half-turrets called sponsons, while female tanks had machine guns. The two types were to work together: the male tanks would use their cannon to target enemy machine gun positions and obstacles, and the female tanks would target troops with their machine guns. Tanks of the two genders were produced in roughly equal numbers, with an additional few armed with both cannon and machine guns.

The British first employed tanks during the Battle of the Somme on Sept. 15, 1916. Although 49 tanks were intended to join the fighting, many broke down and had to be left behind. Despite the low effective numbers of these early armored vehicles, the psychological impact on the enemy and potential for improvement validated them.

The tanks also provided British infantrymen with cover from enemy fire and with cannon fire to support their advance. Several tanks overran machine gun emplacements, causing German soldiers to flee in panic. The British deemed the tanks sufficiently successful to order 1,000 more immediately after the Somme.

Wartime Improvements

The British applied several lessons learned during the Battle of the Somme to subsequent designs. Although

some Mark II and III tanks participated in battles during 1917, the British produced them in limited numbers and used them primarily for training.

Mark IV tanks, however, incorporated the bulk of the improvements over the Mark I and were widely fielded. The British built 1,220 Mark IVs, making it the most-produced tank variant of the war. Improvements included thicker armor, a more powerful engine, and an improved transmission. The Mark IVs first saw combat on June 7, 1917, during the attack on Messine Ridge.

It was during the Battle of Cambrai that the Mark IVs proved their worth. At dawn on Nov. 20, 1917, the British attacked at Cambrai with 476 tanks — the most concentrated use of tanks to that point in the war — across a 10-kilometer front.

British aircraft, cavalry, and artillery joined the tanks to support the advance of six infantry divisions — one of the first large-scale uses of combined arms in modern warfare. Within hours, the British had pushed the Germans back six kilometers, penetrating the Germans' defensive Hindenburg Line. The Allies captured 8,000 German prisoners and 100 guns on the first day.

However, the British advance soon outran itself and lost momentum. Without sufficient forces in reserve, depleted British units were forced back by wave after wave of German counterattacks. The battle ended Dec. 7, 1917, neither side having achieved any significant advantage — at a cost of nearly 100,000 dead.

Aftermath

Although the British at Cambrai failed to achieve a sustained breakthrough of the German defensive lines, the battle showed what the new tanks and complementary tactics could achieve.

Ironically, it would be German tanks, employing more advanced combined arms tactics during the early days of the Second World War, that would validate the innovations the British had tested at Cambrai in 1917.

The tank, in its time, significantly changed how wars were fought. In contrast, the "next big thing" may constitute an evolutionary rather than a revolutionary technological advance.

Via a myriad of efforts, the United States continues to seek new ways to achieve and maintain both strategic and battlefield superiority. DSS continues to partner with industry to preserve the resultant technological edge on which our national security depends.

DSS OFFICE OF INNOVATION: OPEN FOR NEW IDEAS

To meet the mission needs of DSS in a rapidly changing world, the agency established the Office of Innovation (DOI) in August 2012. DOI was assigned the mission to pursue innovation in people, processes, and technology to enhance the efficiency and effectiveness of the DSS workforce.

The first step for the DOI team was to conduct an assessment of innovation within DSS and then developed an Innovation Master Plan (IMP) to guide its activities. Building on this foundation, DOI also created a Stage-Gate Innovation Process. Stage-Gate theory is based on the premise that innovation begins with ideas and ends once a product is successfully launched.

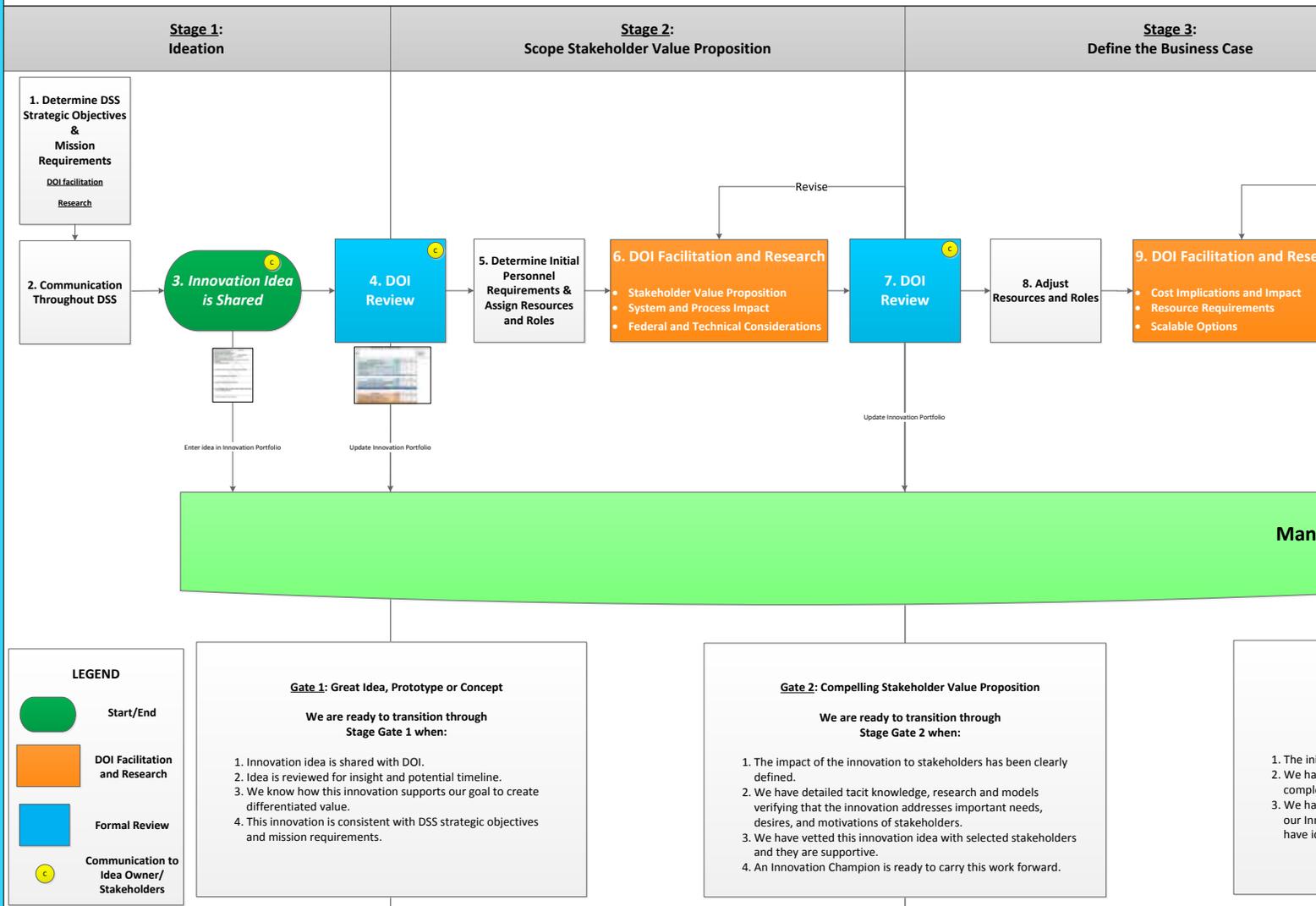
The DOI Stage-Gate Innovation Process (pictured below) takes a typically complex and chaotic process and breaks it down into manageable steps to capture, document,

and evaluate specific information at periodic decision points. It includes 22 steps and six unique stages with each stage defined by its activities and progressively reduces uncertainty and risk.

By following this methodology, the DOI Stage-Gate Innovation Process promises to:

- Increase organizational discipline on the right projects
- Allocate scarce resources more efficiently and effectively
- Improve communication, coordination, and engagement with idea owners and DSS personnel across the organization

In addition, the business case developed during the DOI Stage-Gate Innovation Process will provide stakeholders with detailed market research, technical design specifications, and development plan projections for launching and scaling ideas.



The current DOI portfolio focuses on three principal areas: (1) collaboration workshops, (2) proofs of concept, and (3) research and recommendations. For example, the DOI team has designed, coordinated, and facilitated seven collaboration workshops covering a wide range of issues, to include future scenario planning workshops for both the Center for Development of Security Excellence (CDSE) and the Strategic Management Office (SMO).

The DOI also is working on a proof of concept for an Industrial Security Facilities Database Mobile Application. The idea was submitted by a DSS Industrial Security Representative and has been marked for potential use in the field.

Moreover, the DOI recently completed research on commercially available virtual conferencing platforms and made best provider recommendations to CDSE. The research validated parallel findings and helped guide CDSE's acquisition decision. Both initiatives address critical issues in DSS and support the agency's ability to meet mission requirements.

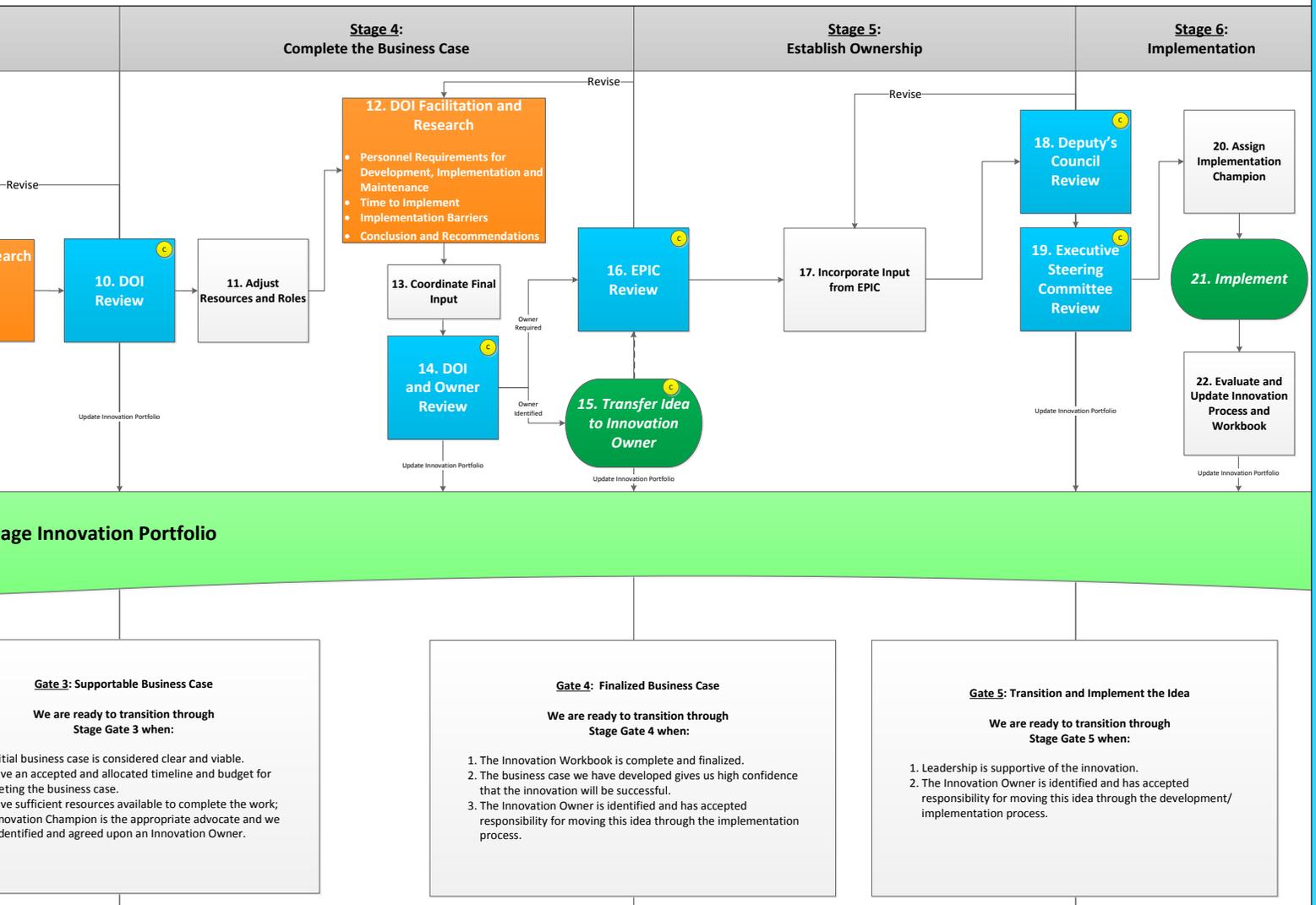
Looking ahead, the DOI has just launched an Idea Submission Form (ISF) which provides DSS employees an easy, convenient, and fast way to submit ideas for review, comment, and possible

“ THE COLLABORATION WORKSHOPS ARE A STRUCTURED AND HIGHLY EFFECTIVE WAY TO LEVERAGE THE BACKGROUND, EXPERIENCE, AND EXPERTISE WITHIN THE ORGANIZATION TO PRODUCE ACTIONABLE SOLUTIONS TO REAL DSS PROBLEMS.”

Brian Miller, CDSE, Chief of Training

development. Recognizing that the best ideas can emerge from anywhere and often address everyday challenges, the ISF provides an open portal for nurturing and pruning ideas throughout DSS.

For more information about the DOI, email Innovation@dss.mil.





FUTURE-SCENARIO

“ Given the current U.S. defense budgetary environment, industry has expanded their global market share. Therefore, future scenario planning is critically important to DSS International as it allows us to be better situated for the rapidly changing landscape.”

Richard Stahl,
Chief, International Branch,
Industrial Policy and Programs

PLANNING WORKSHOP LOOKS OVER THE HORIZON

The Strategic Management Office, in collaboration with the DSS Office of Innovation (DOI), held the agency's first future scenarios workshop in February. The purpose of this event was three-fold: 1) Look at ways in which the various scenarios might impact DSS; 2) Look through a lens of varying perspectives; and 3) Collaborate and engage the workforce.

Scenario planning provides a lens to view changing dynamics in the world today, such as demographics, globalization, technological change and environmental sustainability that could possibly impact the way in which we do business.

In addition, the security environment in which DSS operates is changing rapidly as well as a result of the Washington Navy Yard shooting, Edward Snowden leaks and cyber hacking at Target/Neiman Marcus. Thus, future scenario planning is important because in the event the scenarios play out, DSS will be better situated to respond and adjust manpower, resources or training.

The workshop was facilitated by the DOI and included representatives from all DSS directorates. The attendees were divided into teams that worked together to understand the "future operating environment" themes, determine impact to the agency, address strategy, and explore how to best prepare for the scenario.

The teams were presented with 11 future operating environment themes that were aligned around four driving factors of relevance to the DSS mission:

1. Industrial relationships and influences
2. Loss of U.S. information and technology
3. Budget and adjustment constraints
4. World alliances

Through the guided exercises, the teams learned the need for clear policy and authority, continued education of stakeholders and workforce; importance of partnerships, and the need to better use and leverage them, and finally, the need for organizational structure/cultural change.

As the agency moves forward with its 2020 Strategic Plan, the information gleaned from this event will help form the future operating environment section. It also provided important feedback for the goals and objectives with themes emerging in information sharing, mission creep, and succession planning.

Future scenario planning is a fluid process that will be revisited annually.

TOP: Richard Stahl, DSS IP International Division chief, provides input in relation to a scenario. **BOTTOM:** DSS employees review various scenarios during the workshop.



THIRD TRIP DOWN UNDER



In spring of 2014, two instructors from the Center for Development of Security Excellence (CDSE) travelled to Canberra, Australia, for their third successful mobile training course.

The instructors delivered two Special Access Program (SAP) courses to 28 Australian Department of Defence employees. The course was the culmination of a coordinated process with the endorsement of the U.S./Australian Counsel in response to a request from the Australian Department of Defence for the United States to provide training assistance.

The goal of the training was to assist with establishing an educated SAP staff required to support the U.S./Australian F-35 Lightning II Joint Program Office. The trip also executed cost-effective training by sending two trainers to Australia rather than 28 students to the United States.

To prepare for the course, students completed nine prerequisite courses and carefully studied the read-ahead material that CDSE provided. All 28 students successfully completed the SAP course and clearly demonstrated their knowledge of accessing, controlling, handling, marking and processing SAP material, as required in U.S. doctrine.

The Australian Program Manager for the program met with CDSE personnel following the training event and expressed his desire to continue the partnership with CDSE for future training.

CDSE MAKES TOOLKITS MOBILE

CDSE continues to stretch the boundaries of innovation in its efforts to get the tools into the hands of the professionals who use them.

In September 2013, CDSE launched a new resource tool known as a toolkit. Toolkits are web-based tools that provide access to a variety of training products, job aids, videos, briefings, templates, and resources geared toward particular roles and responsibilities within the various security disciplines.

The first toolkit was tailored for Facility Security Officers (FSOs) and was followed by toolkits for Information Security, Personnel Security, and Physical Security. With over 89,265 views during the first year, the toolkits have been overwhelmingly successful.

CDSE has taken the process a step further and transformed the FSO Toolkit into a web application (web app). In the web app

format, the toolkits cater to the demanding pace of the workforce by remaining mobile and agile.

Now the FSO Toolkit can be loaded and accessed from any Smartphone, iPad, or other Android/Apple device. This provides direct access for FSOs in the field.

Web apps can be accessed on the CDSE Toolkit Splash page at <http://m.cdse.edu>. Currently, the toolkit web app is only available for the FSO and Physical Security Toolkits, but CDSE is developing web apps for all toolkits, placing the security professional tool literally in the hands of the security professional.

Take time today to become familiar with the toolkit designed especially with you in mind. Visit www.cdse.edu and click on your appropriate role under "Access Toolkits."

FINAL CERTIFICATION PROGRAM SUBMITTED FOR NATIONAL ACCREDITATION

The Security Professional Education Development (SPêD) Certification Program is comprised of three core certifications: Security Fundamentals Professional Certification (SFPC), Security Asset Protection Professional Certification (SAPPC), and Security Program Integration Professional Certification (SPIPC), as well as multiple specialty certifications.

Per Department of Defense Manual 3305.13-M, "DoD Security Accreditation and Certification," all certifications must be accredited and maintain accreditation by meeting the published standards of the nationally recognized certification accreditation body, the National Commission for Certifying Agencies (NCCA).

The SFPC and SAPPC were conferred NCCA accreditation in December 2012 and January 2014, respectively.

SPIPC was submitted for accreditation in April 2014 with accreditation expected to be conferred in the last quarter of fiscal year 2014.

What is accreditation?

Accreditation is the process by which the SPêD certifications are evaluated against defined standards and, when in compliance with these standards, are awarded recognition by the NCCA.

Accreditation is proof the program has been reviewed by a panel of impartial experts and has met the stringent standards set by the NCCA.

How did the SPêD Certification Program receive accreditation?

The NCCA uses established standards to assure programs meet threshold expectations of quality and assure they improve over time. The NCCA assesses the certifying organization's role and scope of practice; that is, it evaluates the assessment content, and the certifying organization's ability to provide proper assessment administration and scoring. For each accreditation application, the SPêD Certification Program documented it met the 21 NCCA standards. Key areas include:

- Purpose, Governance, and Resources
- Responsibilities to Stakeholders
- Assessment Instruments
- Recertification
- Maintaining Accreditation

Why seek accreditation?

The SPêD Certification Program is an essential element of the Department of Defense's initiative to professionalize the security workforce. Along with DOD 3305.13-M requirements, accreditation was sought to increase value, credibility, and recognition of the SPêD Certification Program within the security workforce. Accreditation is a way of demonstrating the certification has achieved a standard of excellence.



CDSE ADVANCED, GRADUATE COURSES

By Julie Wehrle

Center for Development of Security Excellence

For two years, the Center for Development of Security Excellence (CDSE) has been offering semester-long advanced and graduate courses to prepare security professionals in the federal government and U.S. military for security leadership positions and responsibilities.

These courses are offered in a virtual instructor-led environment, where students access the courses online and asynchronously, meaning they access their weekly lessons of lectures, presentations, reading assignments, and group discussions or forums when it fits their schedule.

Offering graduate courses to security professionals in a collaborative learning environment has allowed a diverse group of students to participate in the CDSE Education Division program.

How are they diverse?

Without seeing or hearing each other, as would happen in a resident classroom, CDSE Education students quickly discover during their student introductions that not all classmates are alike or even on the same continent.

They work for different agencies or military services, have different work experiences, educational backgrounds, and reasons for taking the courses. They meet through the training and have an opportunity to share their unique perspectives with each other in the online classroom. One student, Valerie Lucier-Diaz, a U.S. Army civilian at Fort Benning, Ga., said she really enjoys listening to other perspectives in the class forums and that it widens how you look at the world.

Where do they live?

These students are working, stationed, and living across the United States and around the world, to include Europe, Asia, and Africa. They work in offices, on ships, in the desert, and telework.

One student noted that compared to other graduate courses he has taken, CDSE graduate courses are more accommodating for work and life schedules, with their structured 16-week semesters. While not physically sitting together in a classroom, these students get to know their classmates and information about their locations as well.

Posting salutations in the class discussion forums such as, “How’s the weather over where you are?” or even, “Are you okay there?” after an incident or emergency, helps foster a classroom community outside of the computer screen. Lucier-Diaz said that she has become friends with several classmates through the “camaraderie” of the online classroom and they plan to meet with each other when on travel.

Who do they work for now? Where have they worked before?

Most of the CDSE Education Program students come from the target audience of DoD security specialists. As of April 2014, over 60 percent of the students directly supported the military, as shown in the “Completions by Agency” graphic at right.

Over 80 percent of the students are in civilian positions, with the remainder active duty military personnel. Students serving in the military reserves often also hold positions as civilian employees or contractor employees with our industry partners. In addition to the DoD students, employees of the National Aeronautics and Space Administration, Department of State, Office of Personnel Management, U.S. Coast Guard, and Federal Aviation Administration have also taken these courses.

The students bring a wide array of experience and expertise as well. Students include interns; program directors; information, personnel, physical, and information system security specialists; supervisory security specialists; attorneys; and many more.

One student, who is earning college credit from these classes with the benefit of a 20-year military career and 10 years of civilian experience, said he would have liked to have taken these courses 20 years ago. He added that while he has other certifications for his position, these courses provide the “bona fides to back up” his opinions.

Patrick Ganley, a CDSE training instructor and career DSS employee, who previously held positions as a DSS special agent/investigator, industrial security specialist, and a retired U.S. Coast Guard reservist, will complete his third course in August 2014.

Ganley said that he would have benefited from these courses during his previous positions because they enhance recognition, interpretation, and assessment of the threat to facilities and



REACHING A WIDE & DIVERSE AUDIENCE

enable collaboration efforts during advise and assist actions with our partners in industry.

What are their educational backgrounds?

The educational backgrounds of these students also varies from no previous college experience to some college classes, to students having one or more bachelor's or master's degrees, or even a doctorate degree or Juris Doctor. CDSE courses are available to anyone who qualifies, regardless of their level of education.

While some students are new to college courses, there are some who have been working on their college degree for years, and others who are returning to college for the first time in many years. Many of the CDSE Education Program students have completed more than one of these Education Program courses and are working on one or more of the five certificate offerings.

One student who has a bachelor's degree said that while he works on earning the program certificates, he hopes CDSE will someday be able to offer a master's degree program. Lucier-Diaz, who has both a bachelor's and master's degree, said she

planned to complete the requirements for the Certificate in Security Leadership by August 2014.

Ganley, who has two bachelor's degrees, said he waited years to resume his academic pursuit, until CDSE marketing got his attention while he was still in the field as a DSS industrial security representative. He said these courses help apply knowledge to the threat and tie the adversary to the widget. He sees direct application of what he has learned to everything we do.

Why are they taking these courses?

The CDSE Education Program students have offered many reasons for taking these courses. Some take classes because they are directly related to their positions or work, or they are looking for personal enrichment. Some students admittedly just love to learn.

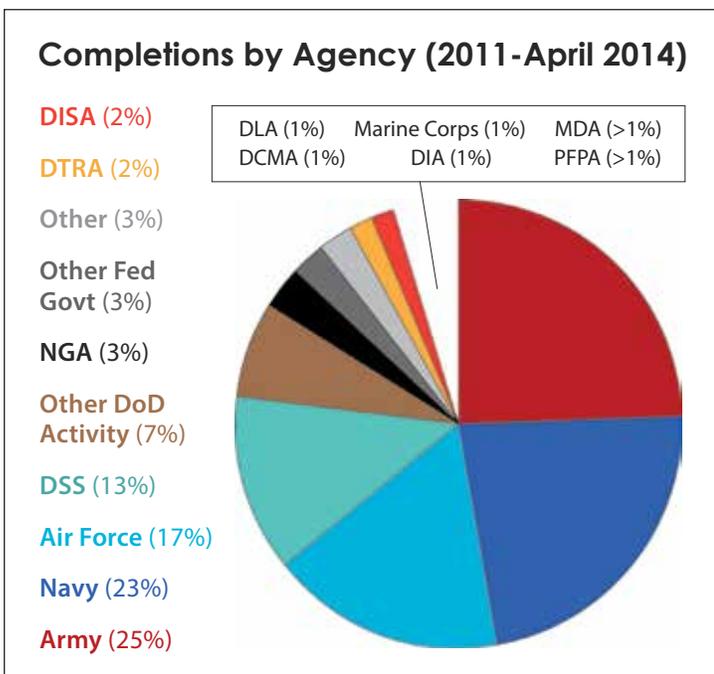
Since all of the courses currently have college credit equivalency recommendations through the American Council on Education, many students are excited about earning college credit that is tuition-free and applicable toward a college degree. Many mid-career students see the value of these courses in their professional development and career advancement.

Lucier-Diaz said that when she first registered for the courses, she hoped that her courses would help her earn a supervisory position, and that is exactly what happened.

Ganley said that these courses offer more insight into how everything is integrated and how the success of a security program hinges on balance, collaboration and cooperation. He added that the courses promote analytical and reading skills and the assignments are cerebral training activities that exercise the brain.

The diverse group of students who participate in these advanced and graduate courses already demonstrate leadership characteristics when they balance work, school, family, health, and other commitments to successful completion.

While their employment and educational backgrounds and career pursuits vary, these students, who may be miles or continents apart, grow as security professionals in these classes. In this online collaborative learning environment of security professionals, students can see and hear the professional and personal growth of future leaders.





DSS HOSTS SECOND ANNUAL TAKE YOUR CHILD TO WORK DAY

By Nicole Graham

Office of Public and Legislative Affairs

On April 24, 2014, DSS hosted the second annual Take Your Child to Work Day at the agency headquarters. To kick off the event, every child received a special T-shirt and goody bag, thanks to DSS fundraising efforts.

The children and their parents then gathered for the opening ceremony where DSS Deputy Director Jim Kren provided remarks to the attendees. Kren encouraged the children to observe and learn from their parents and grandparents. He also urged parents to “plant the spark” and encourage kids to consider a career in public service. Following the opening ceremony, the children were divided into three groups by age.

The 6-7 age group, led by Franklin Caul, Human Capital Management Office (HCMO), Deborah Collins, Industrial Policy and Programs (IP), and Naimah Ewing, Business Enterprise (BE), had an array of activities to keep the children occupied for the morning, to include special DSS-themed coloring books and puzzles.

The children were very excited to see where their parents worked. Logan Zakour, son of Omar Zakour, Office of the Chief Information Officer (OCIO), said that he “wants to find out what his dad does at work.” He was also very excited for the canine presentation later in the day.

This age group also received a tour of the DSS Data Center led by Eric Corbin, Luis Garcia, Hosul Kang and Dave Hobbs. The children enjoyed the tour, especially when they were asked to check the servers to ensure the system was still operating by detecting any flashing red emergency lights. Corbin and his team enjoyed participating in the event and engaging with the kids. Next year, they hope to make the tour more hands-on and interactive.

The other two groups, the 8-12 year olds and 13-18 year olds, had a structured schedule of presentations. The morning sessions started with an overview of forensics by U.S. Army Criminal Investigation Command. Elijah Begab, grandson of Kathleen Branch, IP, enjoyed the forensics briefing because he was able to witness a crime in progress and discuss the crime scene afterwards.

Following the session on forensics, the Defense Intelligence Agency (DIA) provided the children with an overview of counterintelligence and cybersecurity operations. The Air Force Office of Special Investigations (AFOSI) then presented various polygraph techniques.

The lie detector presentation made a big impression on Tristin Harkema, daughter of Scott Harkema, IP. She told her parents that they do not need a polygraph device in their household.

The 13-18 year old age group then received a class on weapon safety by AFOSI and a seminar on the interviewing process by DSS. The presentation by Shon Todd, HCMO, included a dialogue on what to include in a resume and a presentation about the interview process.

Deidre Brogan and Anique Toris, both from HCMO, acted out a skit on the interview process. The children were asked to watch the presentation and later discuss the right and wrong things that occurred during the interview. The session closed with a mini-career fair where DSS, AFOSI and DIA set up booths to answer questions about national security and military professions.

All of the children from DSS gathered for the activity, “Who We Are,” led by Dana Richard, DSS Counterintelligence. The children were divided into 10 groups; each group was given a certain identify like a cleared facility, foreign visitor, counterintelligence, insider threat or spy.

DSS KICKS OFF NON-PAID STUDENT VOLUNTEER INTERNSHIP PROGRAM

By **Shon Todd**

Human Capital Management Office

DSS launched the Non-Paid Student Volunteer (NPSV) Internship pilot program in June 2014, marking the return of student internships to the agency. DSS previously hosted paid summer interns, but due to budgetary constraints and sequestration concerns, the agency has not had the opportunity to bring students on-board since 2010.

Since then, the Human Capital management Office (HCMO) has been brainstorming creative approaches to developing a program that did not require federal funding or full-time billeting, and the result of those ideas is the NPSV pilot program.

In early 2014, the HCMO recruitment office marketed the NPSV program to select universities based on academic program offerings and geographical proximity to participating DSS offices.

The internship program targeted those students who were United States citizens and enrolled at an accredited college or university as a part-time or full-time student with a cumulative GPA of 3.0 or higher in majors directly related to the positions for which they were applying.

Interested students who met all program requirements were interviewed by managers and selected to participate during this pilot phase of the program.

The program is a win-win for both the students and DSS managers. The NPSV Internship program offers opportunities to students who desire meaningful work experience in their chosen academic field, wish to develop and hone their professional skills for today's competitive job market, and want to create a network of associates within the federal government.

Students will not only be presented with challenging work assignments within their academic area of focus but will also obtain and maintain a security clearance, which is a critical component to success in today's federal workplace environment.



Jenna Kingsbury, a Towson University student, is assigned to the Multimedia Productions Division at the Center for Development of Security Excellence.

The internship program will include routine performance evaluations by managers to help students benchmark and track their professional development throughout their participation in the program.

For managers, the NPSV program provides the opportunity to assess students' skill level and ability to develop professionally within DSS. This program is also a great platform for managers to develop and shape the future federal workforce.

DSS recently welcomed its first four NPSV interns:

- **Jenna Kingsbury**, from Towson University, Courseware Design position working under the direction of William Howard, Chief, Multimedia Productions Division at CDSE
- **Dominique Bishop**, from Bowie State University, Instructional Systems Designer position working under the direction of Erika Ragonese, Deputy for Training at CDSE
- **Nathan O'Neill**, from University of Texas San Antonio, Information Systems Security Professional under the direction of Richard Hibbs, San Antonio Field Office Chief
- **Emerson Bahr**, from California State University Long Beach, Industrial Security Representative under the direction of Clarence Hollingsworth, Pasadena Field Office Chief.

The NPSV pilot program runs through summer and concludes at the end of September 2014. At that time, it will re-open across all components of the agency for FY15. Further information and program updates are provided on www.dss.mil.

The contractors had to protect their "secrets," counterintelligence had to deter intrusions while the visitors, insider threats and spies had to gain access. The activity provided the children with a hands-on example of how DSS is working to protect classified information in cleared contractor facilities.

During the afternoon sessions, all of the children gathered outside to tour emergency vehicles. Kayla Hector, daughter of Jaideysh Hector, Industrial Security Field Operations, said she was most

looking forward to seeing the fire engines and ambulances.

They children also received a presentation by the Prince William County Sheriff's Office and watched a canine demonstration by the U.S. Marine Corps military working dogs.

An ice cream social closed the day's events. Like last year, the ice cream social provided the children the opportunity to talk about their favorite events of the day with their parents and new friends.

Alexandria Field Office Chief Retires From Air Force Reserve

By Sarah Laylo

Alexandria Field Office, Industrial Security Field Operations

Sharon Dondlinger, Alexandria Field Office Chief, retired from the United States Air Force on May 20, 2014, after serving over 20 years on active duty and in the Air Force Reserve.

Dondlinger enlisted in the U.S. Air Force in 1994, serving as a Security Policeman. During her enlistment, she held assignments at Hanscom Air Force Base, Mass., and Robins Air Force Base, Ga, and deployed multiple times to the Middle East.

Dondlinger deployed to the 4404th Expeditionary Security Police Squadron at King Abdul Aziz Air Base, Dhahran, Saudi Arabia, and on the night of June 25, 1996, she responded to the attack on Khobar Towers, where 19 Airmen lost their lives. For her actions that evening, she was awarded the Air Force Achievement Medal with Valor.

In September 1998, Dondlinger joined the Air Force Reserve and was commissioned a second lieutenant in September 2000. She progressed through the officer ranks and, in May 2007, was selected as the commander of the 445th Security Forces Squadron (SFS), Wright Patterson Air Force Base, Ohio, where she served until her retirement in May 2014.

In that capacity, she was responsible for the training and readiness of approximately 90 assigned personnel. The mission of the 445th SFS is to maintain readiness for forward deployments to conduct force protection, counterinsurgency, base defense, law enforcement, and security operations world-wide.

The highlight of Dondlinger's career came during a deployment to the International Zone, Baghdad, Iraq, from September 2005 to April 2006.

During this deployment, she served as the operations officer of the 732nd Expeditionary Security Forces Squadron, Detachment 3. This detachment provided law and order for U.S. equities in the International Zone and supported forward operating base commanders in the immediate area.

The detachment's performance was notable and led to a request for support by the U.S. Marshal Service during the trial of Saddam Hussein and other infamous prisoners. Airmen assigned to the detachment provided escort security for witnesses and suspects and conducted personnel screening operations at the court house.



Additionally, the squadron implemented a robust community policing program alongside Iraqi Police counterparts that built a level of trust between local national residents in the International Zone and law enforcement.

Dondlinger, who retired as a major, had two retirement ceremonies. The official retirement ceremony on May 3, 2014, was held at American Legion Post 526 in Fairborn, Ohio, right outside the gates of Wright-Patterson Air Force Base. The event was attended by members of her unit — the 445th SFS, family, friends and DSS representatives.

During a second ceremony at the DSS Capital Region headquarters on May 9, 2014, DSS presented Dondlinger with a U.S. flag that had flown in her honor over the Air Force Memorial and been unfurled in her honor in the Hall of Heroes at the Women in Military Service for America (WIMSA) Memorial in Arlington Cemetery. Dondlinger is a founding member of the WIMSA Memorial.

During her remarks, Dondlinger noted that throughout her career in the Air Force she had been lucky to have excellent leaders, peers, and Airmen. She said that "...while I'm sad to be leaving a great unit and a great group of people, I am excited for the next chapter and the next challenges. I am looking forward to spending time with my daughter and husband."

Bath Iron Works Hosts DSS Deputy

During a recent visit to the Andover Field Office, DSS Deputy Director James Kren and DSS Counterintelligence (CI) Director William Stephens were invited to tour the General Dynamics — Bath Iron Works (BIW) shipyard located in Bath, Maine.

During the visit to BIW, Kren, Stephens and personnel from the DSS Andover region and field offices met with senior BIW management to discuss the latest DSS initiatives and CI trends that could have an impact on BIW's operations.

The DSS delegation was given a tour of the Security Operations Center recently established by BIW to monitor threats to their unclassified network.

The highlight of the visit to BIW included a tour of the ship building process used at the shipyard, along with an on ship tour of the Zumwalt destroyer (DDG 1000), which is moored at the shipyard on the Kennebec River.

On April 12, 2014, BIW made history with the christening of DDG 1000, the lead ship of the Zumwalt class of destroyers. The ship is named for Admiral Elmo R. "Bud" Zumwalt Jr., who was chief of naval operations (CNO) from 1970 to 1974.

Zumwalt was the first commanding officer of the Bath-built USS Dewey (DLG-14), the first vessel built from the keel up as a guided missile ship. The DDG 1000 is the first of three Zumwalt-class destroyers under contract at BIW.



A stop during the Bath Iron Works facility tour.



Hittite Microwave Corporation Receives DSS Counterintelligence Excellence Award

The DSS Counterintelligence directorate presented Hittite Microwave Corporation, of Chelmsford, Mass., with the DSS Excellence in Counterintelligence Award on May 12, 2014.

DSS established the Excellence in Counterintelligence Award in 2010 to recognize cleared contractors that achieve extraordinary results in helping to thwart foreign-directed theft of U.S. technology over the preceding fiscal year.

Reporting by the company needs to demonstrate measurable counterintelligence (CI) results, a solid commitment to CI practices, and cooperation with DSS and other U.S. government agencies.

Rick Hess, President and Chief Executive Officer, accepted the award, which was presented to Hittite for its work in identifying and reporting suspicious contacts and inquiries that could have led to foreign theft of U.S. defense technology.

Hess thanked James Kren, DSS Deputy Director, and Bill Stephens, Director, DSS CI, for their partnership and the support DSS provided in helping his team to build a stronger and more effective CI program.

In presenting the award, Kren discussed the importance of the cleared defense contractor community in identifying possible threats and reporting those threats to DSS in a timely fashion.

The award is not given lightly, and the CI program established at the cleared company must show an overall increased level of commitment and sensitivity to the CI program. The overall quality and quantity of the reports submitted by Hittite were mentioned, as well as the strong commitment Hittite's management has to their CI program.

This can largely be attributed to the ongoing professional relationship and communication established between DSS employees Frank Bonner, CI special agent, and Virginia Morrissette, senior industrial security representative, and Hittite employees Shaun Neylon, Facility Security Officer, and Terry Borges, Export Compliance Manager. This partnership has resulted in many of the submitted reports being evaluated as having a high value in the intelligence community.

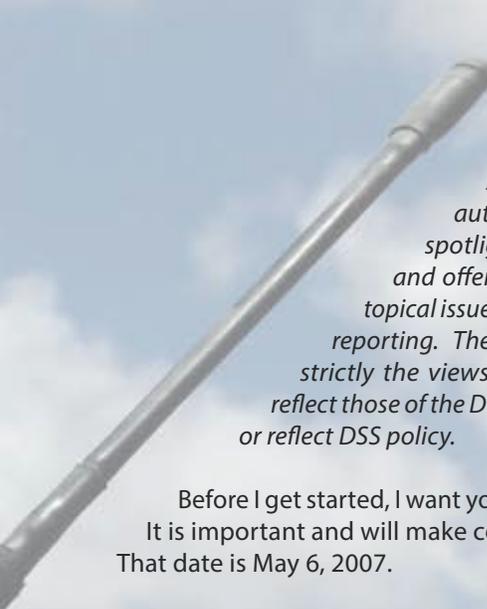
ADVERSE INFORMATION

— A STORY OF PERSONAL IMPACT —

“ Always take care of your soldiers ... this will mean tough training and many days in the field, but ultimately it will bring them together as a team and may ... save their lives.”
Col. James W. Harrison, Jr.

By Braden Harrison
Virginia Beach Field Office





Editor's Note: *The following is a personal account of an event of significant importance to the author. The article is shared to spotlight the author's experience and offer a first-person account of a topical issue, that of adverse information reporting. The views expressed herein are strictly the views of the author and do not reflect those of the Defense Security Service (DSS) or reflect DSS policy.*

Before I get started, I want you all to keep a date in mind. It is important and will make complete sense in a minute. That date is May 6, 2007.

We have all seen a dramatic change and focus on the reporting of adverse information by cleared personnel over the past several months. While DSS, in the four years I have been employed with them, has always focused on ensuring it was reported, that hasn't always been true of the larger defense community.

From incidents such as the shootings at Fort Hood and the Washington Navy Yard, we have seen various reports of information that should have been reported, or that were reported but nothing was done with. This has caused a ripple effect, as we have now created a climate of hyper vigilance, which includes a spike in the reporting of adverse information by contractors. In some cases, it appears this is out of fear that they will be penalized for not reporting information that could be related to a future incident.

This brings me back to the date that I asked you to remember. You see, for me, I already had a strong sense of the need to report adverse information before I was hired by DSS. While it was not categorized as that specific terminology, the underlying theme was there. This could have been attributed to my being raised overseas on a military base, which is partially true, especially in an environment of "See something. Say something." But, alas that was not the case.

May 6, 2007, was a date that forever changed my life when, at 2230, I received a knock on the door from an Army Casualty Notification Officer that my father, Army Col. James W. Harrison, Jr., had been killed in a blue-green incident in Afghanistan.

Along with all the emotions of losing your father at 23, I really wanted to know what happened. This was not a simple case of a person being killed during combat operations, and the details surrounding my dad's death were very vague to begin with. So I asked questions of those who worked with my dad in Afghanistan and who knew of the ongoing investigation here.

Eventually details would come out that my dad and his Command Sergeant Major had been ambushed coming out of their work location that day. The perpetrator was an Afghani guard, who two days prior had returned early from what was supposed to be a two-week vacation back home.

When he returned, it seemed his whole personality had changed. He was more reserved, kept away from the rest of the group, began talking to himself and, the day before the incident, specifically requested the guard assignment that put him in perfect position to attack the convoy my dad was traveling in.

Even as a 23-year-old, I knew something didn't add up, and I wondered why no one had caught on to these warnings. This continued to ring true to me when I heard of the signs reported about Maj. Nadal Hassan and Aaron Alexis. The remarks they made, behaviors that occurred, and yet it seemed no one reported them or took action.

I use this as motivation to drive me forward, to ensure something like this does not happen to another family. I've even used it as an example with my contacts. Is it an extreme example? Yes. But sometimes an extreme example is needed to get the point across that no issue is too small, no action too insignificant, to report.

By neglecting to report something in the early stages, you may be allowing something larger to fester and grow, which can eventually lead to an extreme situation.



