DSS ACCESS

Official Magazine of the Defense Security Service | Volume 6, Issue 3

THIS ISSUE

Thirty-six facilities achieve highest industrial security recognition

DSS ACCESS

Published by the
Defense Security Service
Public Affairs Office

27130 Telegraph Rd.
Quantico, VA 22134

dsspa@mail.mil
(571) 305-6751/6752

DSS LEADERSHIP

Director | Dan Payne

Chief of Staff | Troy Littles

Chief, Public Affairs | Cindy McGovern

Editor | Elizabeth Alber

Layout and Graphics | Marc Pulliam

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 Department of Defense, or DSS.

All pictures are DoD photos, unless otherwise identified.

COVER STORY: THIRTY-SIX FACILITIES ACHIEVE HIGHEST INDUSTRIAL SECURITY RECOGNITION

INSIDE

From the Director

This issue of ACCESS features a wide variety of topics, that clearly show the breadth of the agency's mission and the value we place on partnership and collaboration.

Most notably, we feature the annual recognition of the Cogswell Award winners. DSS again partnered with NCMS during their annual training event to present the awards. The Cogswell awards continue to serve as the model for industrial security excellence for the National Industrial Security Program. In keeping with a tradition established in 2014, we invited a representative sample of this year's 36 Cogswell winners to contribute to this issue. I encourage all security professionals to read the articles from these facility security officers as they describe in their own words how they define and achieve continued success. Congratulations again to our 2017 Cogswell winners for setting the bar for others to emulate.

During NCMS, three DSS employees received Industrial Security Awards. This award is presented to an individual or organization that has significantly contributed to industrial security, and for three DSS employees to be recognized in one year is a significant achievement. I commend their efforts to seek opportunities to engage industry and other government agencies to bring the counterintelligence and security communities together.

We also have an article on the strategic engagement our Counterintelligence (CI) Directorate is doing to develop, consolidate, execute and expand industry and government CI partnership and collaboration efforts. One of my primary goals as the DSS Director is to ensure a seamless integration of counterintelligence and security and this directorate is a perfect example of how we can achieve that goal.

Another example of that integration is the DSS Excellence in Counterintelligence Award, which recognizes cleared contractors that achieved extraordinary accomplishments in helping to thwart adversary theft of U.S. defense technology. This year we recognized three companies that focus on CI and how it can be integrated into their overall security programs.

As we continue to face new missions, new challenges and a constantly evolving security landscape, I want to build on these successes and achievements. Our focus on risk and tailored security programs will only further enhance our efforts.

Thank you for your continued support.

Dan Payne
Director

DSS recognizes the best in industrial security; 36 facilities receive COGSWELL AWARDS

by Beth Alber
Office of Public and Legislative Affairs

On June 22, 2017, the Defense Security Service presented the annual James S. Cogswell Outstanding Industrial Security Achievement Award to 36 cleared contractor facilities during the 53rd annual NCMS training seminar in Anaheim, Calif. The Cogswell awards represent the "best of the best," and the winning facility's security programs stand as models for others to emulate. These 36 facilities represent less than one-tenth of one percent of the over 13,000 cleared facilities in the National Industrial Security Program (NISP).

Each year, DSS partners with NCMS to host the Cogswell Award presentations during its annual training seminar. In presenting the awards, DSS Director Dan Payne noted that DSS has been a participant at each of the 53 national seminars – ranging from keynote speaker to the collaborative relationship of providing workshops and help desk participation. "Thank you to NCMS for its effort in delivering security education and providing these training forums," Payne said. "As an organization that provides industrial security seminars, it is very closely aligned with DSS' core mission."

Information Systems Security Professionals Luciana Rodrigues (left), Andover Field Office, and Joe Webb (center), Cypress Resident Office, assist NISP Authorization Office Help Desk customers at the annual NCMS Conference. *(NCMS photo)*

The Cogswell Award was established in 1966 in honor of the late Air Force Col. James S. Cogswell, who 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.

During his remarks, Payne described the Cogswell selection process as rigorous. The process begins with a DSS industrial security representative who nominates a facility. That facility must have achieved two consecutive superior ratings just to be considered for the award. "This just gets you in the door, but demonstrates a consistent, committed program over time," Payne said.

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

"Historically the number of companies receiving Cogswell awards ranges between 10 and 40; and this year it was 36," Payne said. "Over the years, we've seen a steady growth in the number of

recipients; however this year, the number decreased. That shows you just how hard it is to achieve this honor and the significance of the achievement. It demonstrates the commitment of the awardees in maintaining the highest standard in securing our nation's assets."

In closing, Payne said, "In light of the threats to our nation, it is critical that all facilities attempt to achieve the highest standard possible and those displayed by our Cogswell awardees over several assessments."

Congratulations to the 2017 Cogswell Award Winners!

Adams Communication and Engineering Technology, Inc.
Aberdeen Proving Ground, Md.

BAE Systems Technology Solutions and Services, Inc.
California, Md.

Black River Systems Company, Inc.
Utica, N.Y.

Camber Corporation, a subsidiary of Huntington Ingalls Industries, Inc.
Farmers Branch, Texas

CGI
Huntsville, Ala.

Chugach Management Services
Anchorage, Alaska

Concurrent Technologies Corporation
Johnstown, Penn.

DCS Corporation
Ridgecrest, Calif.

DCS Corporation
Alexandria, Va.

Fincantieri Marinette Marine
Marinette, Wisc.

General Dynamics Information Technology
Chesapeake, Va.

Georgia Tech Research Institute, Warner Robins Field Office
Warner Robins, Ga.

Hankins and Anderson, Inc.
Glen Allen, Va.

Harris Corporation
Columbia, Md.

Integrity Applications Incorporated
Ann Arbor, Mich.

Jacobs Technology Inc.
Ridgecrest, Calif.

Jacobs Technology, Federal Network Systems
Reston, Va.

L3 Platform Integration
Waco, Texas

Lockheed Martin Corporation -- Aeronautics
Marietta, Ga.

Lockheed Martin Corporation -- Aeronautics
Palmdale, Calif.

Lockheed Martin Corporation – Missiles & Fire Control
Chelmsford, Mass.

Lockheed Martin Corporation – Missiles & Fire Control Raytheon/Lockheed Martin JAVELIN Joint Venture
Orlando, Fla.

McLaughlin Research Corporation
Middletown, R.I.

MDA Information Systems, LLC
Gaithersburg, Md.

Meggitt Defense Systems, Inc.
Irvine, Calif.

Mercury Defense Systems, Inc.
West Lafayette, Ind.

Modern Technology Solutions, Inc.
Alexandria, Va.

Northrop Grumman Corporation - Marine Systems Sector
Sunnyvale, Calif.

Northrop Grumman Corporation - Mission Systems Sector
Beavercreek, Ohio

Northrop Grumman Corporation - Mission Systems Sector
Orlando, Fla.

Paragon Systems, Inc.
Herndon, Va.

Rally Point Management, LLC
Fort Walton Beach, Fla.

Raytheon Company
Arlington, Va.

Raytheon Company
Camden, Ark.

Spirent Federal Systems, Inc.
Pleasant Grove, Utah

Telos Corporation
Ashburn, Va.

IN THEIR OWN WORDS

A representative sampling of the 2017 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.

DCS Corporation

by Terri Weadon
Vice President of Security

DCS Corporation | Alexandria, Va.

DCS Corporation is a privately held, employee-owned technical services company operating primarily in the government services sector. DCS was founded in 1977, and specializes in addressing challenging and complex engineering and management issues in defense systems research, development, test and evaluation; acquisition; and sustainment. DCS's nearly 1,100 employee-owners, located at our Alexandria, Va., headquarters and 16 offices nationwide, are extremely dedicated to our security program and protecting this great nation we live in, our warfighters and their missions, our citizens here and abroad and our technological and economical edge. DCS' commitment to the highest levels of ethics, integrity, and excellence is of central importance in all that we do, which is why winning the James S. Cogswell Award for the eighth time is such an honor for our company.

There are many aspects that go into building and maintaining a successful security program. It's not something that happens overnight. It takes everyone working together to really make it work.

- **Strong management support** – Security must play a key role in the everyday functions of the company including many of the decisions made by senior management. The management team must lead by example and show their dedication to maintaining a successful security program.

- **Qualified and dedicated security team** – You need a team of enthusiastic security personnel who strive to support the employees with quality, reliable service. You need a team that the employees can trust, offers an open door approach, and is someone that employees can openly and confidentially confide in.

- **Dedicated employees** – Cleared and uncleared – who are dedicated to providing classified and sensitive information the highest protection.

- **Great working relationship with DSS** – The DSS representatives are there to assist you. They want you to succeed. Don't be afraid to turn to them for help. I have had many different DSS representatives over the years and they have all been wonderful to work with. They are very busy, so I try not to ask them something unless I have exhausted all other resources, but when I do, they are always very eager to help me.

- **Security awareness program** – Get the word out! Let your employees know that it is extremely important to protect classified information, self-report, report suspicious activity, remain vigilant, report foreign travel, etc. Here at DCS, we have a Security Awareness Committee whose job is to keep security out in front of our employees.

- **Security education** – Education is the most powerful weapon you can use. Security needs to be a constant reminder. At DCS, it is mandatory that all employees complete at least three security training briefings a year. The Annual Security Refresher and the Insider Threat Training are mandatory. I have been running this training program for over 20 years and I can proudly say that we have met this requirement with 100 percent completion each year. Remember to keep your training informative and interesting, and discuss new and upcoming policy changes before they happen.

- **Marketing** – You need to market great security to your employees. You are selling the importance of protecting classified and sensitive information. If you just have mundane procedures and rules, then the employees will see security as an inconvenience. But if you remind them that they are playing a vital role in protecting this great country we live in, and that we are all working together as a team to protect our soldiers, missions and even our jobs, they will

want to ensure they are doing everything they can to participate and follow procedures.

- **Always be prepared for change** – I have worked in this field for 32 years and one thing I learned is that you have to be willing to change. Procedures change, requirements change, databases change, etc. Keep in mind that change is a good thing – change can make us better. You need to be willing and able to change quickly when the requirements change.

- **Mentors** – Find a good mentor through local area security groups, NCMS, or even ask your DSS representative. When I first started in security, we didn't have mentors. I had to learn the hard way and felt I had nowhere to turn for help. I vowed never to let anyone else go through that which is why I mentor many facility security officers (FSOs) today. Once you are an experienced FSO, give back and be a mentor. It's such a rewarding experience.

- **Use free resources** – There are tons of great resources at your fingertips. Take advantage of the great information and training out there. Some of my favorites: The DSS website has tons of great information as well as upcoming policy changes, alerts, news, etc. Add that page to your favorites and check it daily. The FSO toolkit on the DSS website is another excellent resource. NCMS offers a great deal of shared experience on their site as well, and the NCMS website and their chapter websites are great resource tools. Center for Development of Security Excellence (CDSE) training, STEPP training, toolkits, shorts, and Personnel Security Management Office for Industry webinars are more helpful resources. Also, think about joining LinkedIn groups, such as the FSO group. There are so many useful resources out there that you shouldn't be afraid to research and find the ones that best suit your needs.

In summary, to have an effective security program that is Cogswell worthy, you must have a program that goes above the requirements of the National Industrial Security Program Operating Manual, is creative and adaptable to change and is fully supported by your senior management team. At DCS, we proudly accepted the James S. Cogswell Award with deep gratitude and appreciation for the team work it takes to be Cogswell worthy and we applaud with great respect the other companies that won this year and in the past.

The Georgia Tech Research Institute

by Harriet Sheffield
Facility Security Officer

Georgia Tech Research Institute, Warner Robins Field Office | Warner Robins, Ga.

The Georgia Tech Research Institute (GTRI) is the nonprofit, applied research and engineering arm of Georgia Tech (Georgia Institute of Technology). Each day, GTRI's science and engineering expertise is used to turn ideas into workable solutions for our customers. GTRI's strong bond with Georgia Tech, and its academic units, opens the door to the vast intellectual resources of one of America's leading research universities and provides unparalleled access to the world's leading problem solvers.

The GTRI Warner Robins office serves as an onsite liaison between GTRI and Robins Air Force Base (RAFB), and provides immediate engineering support to the RAFB customer in a secure environment. This environment exists because of the superior security program developed by the GTRI Warner Robins team. The success of our facility is a combination of three elements, partnership with the DSS, creating an in-depth self-inspection program, and making security training fun.

Partnership with DSS

The DSS is a support mechanism for our program and provides us with expert guidance and support. They supply training and information, and alert us to possible mistakes when necessary. This input ensures the best possible program. Our outlook on each one of our security vulnerability assessments (SVA) is to listen to the advice of our DSS representatives and to improve our program with their feedback and suggestions. Our representatives tell us exactly what they expect and how to obtain the results we want. The enhancements are a critical part of our security program because they always come back to help our facility and allow us to help others. If something works, I love to share it with other facility security officers (FSO) to use in their facilities. We don't view our relationships with other facilities as competition, but as a partnership with a common goal to protect our country and the people in it.

Self-Inspections

Conducting quarterly self-inspections helps the administrative end of our program. It also helps prepare for the DSS SVA. Quarterly inspections validate that our records are up-to-date and correct before the SVA, therefore reducing preparation time. We developed an internal check sheet that is implemented first, and then we use the DSS Self-Inspection Handbook. Using both ensures we do not miss anything and helps identify corrections that need to be made before the SVA. This extensive preparation guarantees that we are prepared, and that we respect the limited time and resources of the DSS SVA team.

Training

The FSO requires extensive training to apply an effective security education program, and to ensure our employees know how important they are to the program. An FSO cannot do this on his/her own. Once an employee is trained, we remind them often of the correct procedures to protect sensitive and classified information that positively impacts the warfighter. One of the most effective ways to instill teamwork and pride is to remind everyone to cross-check each other when going in a closed area, classified meeting or a discussion. This shows our employees how vital they are to the success of the program. We also try to make learning and remembering fun. Our monthly newsletter has a security question with prizes for the correct answer. A quarterly Insider Threat pamphlet was developed and is disseminated to each employee. Almost every employee-related event, such as cookouts or luncheons, includes security awareness where prizes are awarded for providing correct answers. If our engineers have fun, they remember it and want to do it instead of it being a chore.

At GTRI Warner Robins, we use dedication, hard work, partnerships, self-inspections, and training to ensure success.

Harris Corporation

by Kristin Covey
Security Manager/Facility Security Officer/CSSO

James Smith
Information Systems Security Manager, Senior Specialist

Electronic Systems/Harris Corporation | Columbia, Md.

Harris Corporation's Electronic Systems division at Columbia, MD, formerly known as EVI Technology, LLC, started off in 1983 as a small company serving several government customers by providing innovative engineering solutions for unique problems. Over the years, EVI has grown and been acquired by several leading companies in the defense industry. EVI is now a part of Harris Corporation, an internationally renowned 120-year old American technology company and defense contractor. We are a Fortune 500 company that serves diverse customers throughout the world. We are honored to receive our first James S. Cogswell award.

For over 17 years, I have been a part of our security program which has expanded to a four-person team supporting multiple customers. As our security function has evolved into the multi-faceted program we have today, one thing has been a key part of our success – the support from our DSS industrial security representative.

Our DSS representative has always been there to assist and encourage us. Our rep has provided factual guidance, motivation, and inspiration to take our program to the next level after each inspection. The DSS rep became an integral part of our team, and as this award attests, instrumental to our success.

> Our **DSS rep became an integral part of our team**, and as this award attests, instrumental to our success.

If I were asked how to create and grow an effective security program, I would say change how people define the concept of security. We don't see security as rules to follow dictated by a group of people who make sure the rules are obeyed. Rather, we see security as a collaboration among everyone in the company working together to provide the best possible solutions for our customers while protecting our nation's most critical information. The security team sets the tone for the security mindset; i.e., we guide, we inspire, we motivate, we educate, we congratulate, we encourage and we lead by example. We set the tone for how everyone at our facility sees and implements security, so a collaborative and inclusive mindset is essential.

When asked by peers, "How do you get better than a satisfactory rating?" My answer is, "Prepare for the inspection, not the inspector." Do what the National Industrial Security Program Operating Manual (NISPOM) instructs you to do; don't try to second-guess what you think the inspector might want to see. The NISPOM is straightforward and the Industrial Security Letters provide essential clarification.

In other words, strive for a successful program: Follow the NISPOM and do the work that needs to be done. Don't neglect the basics in order to chase enhancement points. Enhancements should come from improving the way you implement your security program, not from shallow changes that don't improve your program.

Finally, a successful program needs to be organized. Create a "security at your fingertips" binder that includes copies of every document or artifact that is essential to your security program. When performing day-to-day tasks, the binder should be the one-stop reference for all core activities. When undergoing an inspection, the binder should be the only place you should need to go to answer your inspector's questions.

At the end of every inspection, our DSS industrial security representative would always ask: "What do you intend to do now to make your program better?" After being honored with the James S. Cogswell Award, we now take inspiration from our representative and ask ourselves: "What do we intend to do to make our program better?" Thank you industrial security representative for inspiring us!

Integrity Applications Incorporated

by John Minzey
Regional Security Manager/Facility Security Officer

Integrated Applications Incorporated | Ann Arbor, Mich.

Integrity Applications Incorporated (IAI) is an engineering, software service and solutions company. IAI maintains a nationwide presence primarily supporting the Intelligence Community and other civil, defense and intelligence customers with a focus on government space, and intelligence, surveillance and reconnaissance systems activities. IAI's headquarters is in Chantilly, Va., and has offices in California, Hawaii, Massachusetts, Maryland, Michigan, New Mexico, Ohio, and Pennsylvania.

At IAI, excellence is a way of life. Our selection for the prestigious James S. Cogswell Award reflects our commitment to create, enhance and uphold sustained security excellence over time for IAI customers and employees. We are honored to receive this award.

As a retired law enforcement officer, I understood that successful crime prevention required citizens' participation. It required a partnership between the police department and the community that included education and neighborhood watch programs. When I began my career as a facility security officer (FSO) at IAI, I believed the same would hold true when implementing a successful security program. Employees would need to not only comply with security regulations, but would also require education and to proactive participation.

Staffing

While the FSO is responsible for overseeing security at a facility, competent security staff is essential for security programs to be successful. At IAI, we always look to hire personnel who possess the desire to be better. The entire IAI security staff continually strives to find new ways to improve security procedures and achieve superior ratings.

Management Support

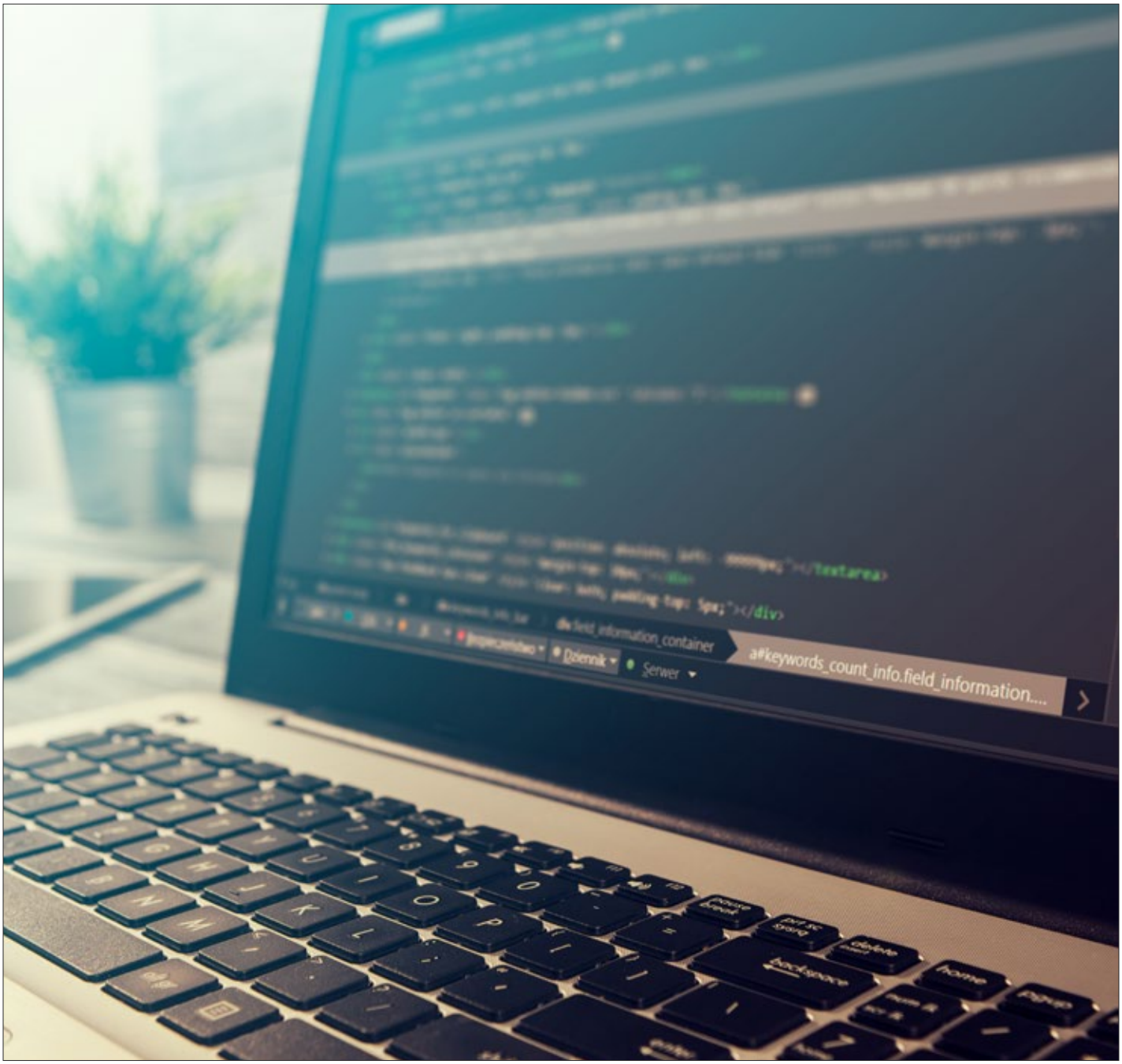
Our senior leadership has supported our security efforts and provided the tools for our team to be successful. IAI's goal is to produce high quality products and services above and beyond our customers' expectations and demands. This holds true for our security program as well. I have worked for other companies where leadership is satisfied with meeting the minimum security requirements. IAI's leadership realized the significance of a superior security program as a government contractor. Without the full support of our senior leadership, it would be difficult to implement the additional parts of our security program that go beyond the minimum National Industrial Security Program Operating Manual requirements.

Education & Awareness

Training and awareness briefings are ongoing activities. Limiting training to the minimum requirements can result in an average security program that will eventually fail to provide essential tools and knowledge that employees need to protect government, company, and personal assets. We believe that offering a variety of training options keeps employees interested. Enlisting government partners for briefings provides employees the opportunity to hear actual incidents that are happening in the world. We also solicit information from our employees on what they liked and disliked about training. There is a better chance they will absorb the information if they like it.

Government Partners

It is essential to have a good rapport with the DSS and we have been fortunate to have great support from our DSS industrial security representative and counterintelligence special agents. We have also built strong relationships with other government security agencies such as the Federal Bureau of Investigations and the Naval Criminal Investigative Service. These relationships have provided valuable resources which ensure we can implement security measures to protect our nation's classified information and the U.S. warfighter.



Human Habit

No matter what procedures are implemented, security software is installed, or physical protections put in place, the success of a security program will always hinge on human behavior. Our employees believe that security should be practiced 24/7. We offer our employees training on how to stay safe at home, when they travel, and in the course of their day-to-day activities. Like in their homes, we ask our employees to participate in a neighborhood watch at work by watching out for themselves, their neighbors, and reporting anything suspicious to security. Winning a James S. Cogswell Award is a neighborhood accomplishment.

JAVELIN Joint Venture

by Marissa Mikich
Facility Security Officer

Lockheed Martin Missiles and Fire Control
Raytheon/Lockheed Martin JAVELIN Joint Venture | Orlando, Fla.

It's been a good year for **JAVELIN Joint Venture** (JJV) – the facility was recently awarded the Aviation Weekly Excellence Award and the Performance-Based Logistics Award for Material Readiness by the Secretary of Defense. So to add the James S. Cogswell Outstanding Industrial Security Achievement Award to this list is more than an honor. Hearing DSS Director Dan Payne state that being one of the 36 companies out of 13,000 that won a Cogswell Award means you are "the best of the best" is so humbling and makes me even more proud of the work I do.

Being a small company has its advantages – as the only security representative, I know all that goes on from a security aspect and have built a rapport with the program team. However, being a small company also presents its challenges. Being able to prioritize responsibilities is a crucial element when being the only security representative for a company, while also wearing multiple hats.

I have been the facility security officer for JAVELIN Joint Venture for almost two years; however, I have worked in industrial security for almost 13 years and over the years have developed meaningful working relationships with DSS representatives. Our DSS representative has been an invaluable resource and mentor.

While the JAVELIN Joint Venture facility has received five consecutive "Superior" ratings; our goal is not to obtain the "Superior" rating or "Cogswell Award," it's about doing the right thing. The recognition is just proof that we always put security first and are protecting our warfighters. It is hard to pinpoint just one contributing factor for our success.

We could not have won the Cogswell, much less have a successful program, without a few key items and resources that allowed our security program to be successful:

- **Security education** – Continuous education is key to a successful program. On top of our standard annual security refresher training, I provide security education to the workforce via pamphlets and posters, audiovisual screens, counterintelligence briefings, monthly education emails, and annual security fairs. I also attend and participate in the Florida Industrial Security Working Group and local NCMS chapter meetings and readily share the information with the JJV workforce.

- **Lockheed Martin Security support** – We could not have a successful program without the assistance of our Corporate Audit Support Team. They help us track all assessments, to include self-assessments, via our Security Management and Reporting Tool, which provides an enterprise-wide approach to share all audit data allowing Lockheed Martin to identify assessment trends, areas of risk, and share best practices. We meet with our Audit Support representative before each and every self or DSS assessment to go over clearance and JPAS issues and concerns, adverse reports, training records, and enhancement packages.

- **Program support** – Most importantly, I have the support of the JAVELIN Joint Venture program team and senior management. The team understands the importance of security and recognizes what the ramifications would be without a security program. Security is kept in the loop from everything to customer visits to the fact that a classified CD was just created. It is clear that the entire program has pride in what they do and who they are working for!

Lockheed Martin Corporation - Missiles & Fire Control

by Ronald Walls
Facility Security Officer

Lockheed Martin Corporation – Missiles & Fire Control | Chelmsford, Mass.

As the facility security officer (FSO) for the Chelmsford Facility I was thrilled to accept the award on behalf of the senior staff and employees who made this possible!

Lockheed Martin Missiles & Fire Control
Chelmsford Operations is a design and manufacturing site that supports air and missile defense programs, and the 68,000 square-foot facility is located in Chelmsford, Mass.

We are honored to be recognized by the DSS, as we value our partnership with DSS and their recognition of our dedication in protecting our facilities and classified information systems.

> "...we value our partnership with DSS and their recognition of our dedication in protecting our facilities and classified information systems."

Chelmsford benefits from a corporate-wide integrated security team with a focus on communication and sharing security practices. The corporate and enterprise wide tools, subject matter experts, and management support are invaluable to the site FSOs who just need to tailor them to their facility.

The credit for the Cogswell Award belongs to a very dedicated security team and our security-conscious employees and their commitment to security practices. The security culture is evident with every employee in all of our activities. We stay engaged with our employees from on-boarding to retirement. Additionally, we believe our partnership with the DSS Andover Field Office could be used as the industry standard.

What factors contributed to our success?

- A team of security professionals available at a moment's notice. From an award winning Corporate Counterintelligence Program, dedicated Corporate and Enterprise Audit Support teams, to subject matter experts in every security discipline.
- Security education and awareness is the foundation of our program. One of our most successful methods involve tailoring questionnaires around specific security disciplines and use the results to create a targeted education program focusing on any weakness discovered.
- Employees! Employees! Employees! In my 30 plus years' experience in security I have never witnessed the level of support we receive at Chelmsford. It's an "all in" organization where all employees participate in every activity. They not only participate, they are engaged and readily support security efforts.
- Leadership and management support is required to be successful. The Chelmsford Security Team receives outstanding support from security and site leadership teams. From personally supporting the program to providing the necessary tools and manpower to get the job done.
- Our efforts are never solely based on receiving 'Superior Ratings' or winning the 'Cogswell Award.' We focus day-to-day on doing the right thing at the best of our ability and the rest will follow.

L3 Platform Integration

by Ronald Rhea and L3 Public Affairs

L3 Platform Integration | Waco, Texas

L3 Platform Integration is a leading aircraft systems integrator with more than 30 years of experience in maritime surveillance, advanced communications, avionics modernization and special-mission aircraft for military, commercial and Original Equipment Manufacturer customers.

There are more than 700 cleared employees on our team, so it is imperative that we maintain a strong and vibrant security program. I use our company's name, L3 Technologies, as an inspiration for the key components of this program, and we receive outstanding support from our corporate and business segment security teams.

Corporate Security has implemented a corporate assessment program that evaluates each L3 facility on a recurring basis – including uncleared facilities – to ensure they are meeting or exceeding national and internal security regulations, standards and policies. The assessment focus is not just on compliance, but also on how each L3 facility can operate more effectively to safeguard classified and sensitive unclassified information. Corporate Security also supports our facility through one of the strongest counterintelligence (CI) programs in cleared industry. L3 is a leader in cleared industry suspicious contact reports to DSS every year, and maintains outstanding relationships with the FBI, Department of Homeland Security and others in the law enforcement and intelligence communities.

L3 is one of 13 companies that participate in the DSS CI Partnership Program, which provides relevant, real-time threat information to be used by L3 facility security officers (FSOs) to provide CI briefings and critical threat awareness training to our employees. In 2016, L3 Corporate Security also developed and implemented our new Insider Threat Program. DSS has pointed to L3 as an industry leader in our implementation of this key initiative. At DSS's request, L3 participated in DSS-led tabletop insider threat exercises and briefed our program as a model to other cleared companies.

As always, a strong security program starts at the top, and our Chairman and Chief Executive Officer strongly support our security initiatives. To our CEO, security is a serious 'business discriminator' by which the corporation is measured in the marketplace. Through his leadership and the leadership of the business segment presidents, L3 has built a security program that is second to none in cleared industry. L3 has earned at least one James S. Cogswell Award each of the past 13 years, and 25 overall. We have also won the DSS Counterintelligence Award three times in the past five years.

This strong leadership, support and a corporate culture that reflects a strong need for a vibrant security program have been key factors in our success at L3 Platform Integration. In my job as FSO, I have a straightforward strategy in leading our security program: Leadership, levels, and learning. I come to work each day with the goal of successfully implementing these three Ls.

Leadership

As security professionals, we know that it can be challenging to quantify our value to an organization. Fortunately, the leadership at L3 understands the importance of security. The ultimate goal of our security program is to protect information that is critical to the safety and security of our employees, customers and ultimately, our nation. Our executives lead by example, setting the tone for security across our business in both their communication and their actions, and they provide the support and resources we need for the effective management of our security program.

Their leadership also enhances the business operation. Maintaining a comprehensive, award-winning security program is critical to our success as a business.

Levels

A successful security program requires engagement from all levels of the organization. Every department, including Legal, Compliance, Human Resources, Marketing and Operations, plays a role in the success of our program. A great example of this is our Empowered Official. She

is able to answer the tough export-related questions from DSS and is also skilled at working closely with our security professionals to ensure compliance.

It's one thing to get employees' attention when your leaders prioritize security. However, if you want employees to commit to being actively involved in a robust security program, you have to help them understand why security is important and how their actions can directly affect our customers and business. My team works closely with our Public Relations (PR) department to communicate to employees our security processes, as well as emphasize our employees' responsibility in protecting classified information.

We also work with the PR team to kick off a security refresher campaign ahead of our DSS audits to remind employees of their security responsibilities. However, it is key to note that our communications occur continually throughout the year to ensure security remains at the forefront of everyone's mind.

Learning

Continuous improvement is imperative to our program, so we are always learning. Our security program must continue to evolve, and I've worked hard to integrate comprehensive training into all elements of our business. If we want to continue our success and duplicate our superior ratings year after year, learning is key.

I have found it is extremely important to work closely with our DSS representative. Our mission is truly a partnership between government and industry, supporting national defense and the warfighter. Communication is vital to the learning process. During our last vulnerability assessment, our DSS representative explained the need to demonstrate specifically what we were doing to refine our program to be able to earn enhancements. Bullet justifications are simply not enough.

Winning awards says a lot about our commitment to security, but the most important thing is that our security program is better today than it was when DSS last visited. That's my goal: Continuous daily improvement to our security program.

It is indeed an honor to earn a Cogswell Award. I am humbled and extremely excited to have this experience and to share the accolades with the security team, as well as with all my L3 Platform Integration colleagues. It takes all of us working together to get this job done right.

Northrup Grumman Corporation

by Debra L. Martin, CPP
Security Manager/Facility Security Officer

Northrop Grumman Corporation - Marine Systems Sector | Sunnyvale, Calif.

Northrop Grumman Corporation is a leading global company providing systems, products and solutions to both government and commercial customers. With more than 60,000 employees in all 50 states and more than 25 countries, Northrop Grumman is recognized as being one of the best places in the world to work.

Northrop Grumman's Marine Systems business unit is an important part of the overall Northrop Grumman portfolio. Headquartered in Sunnyvale, Calif., Marine Systems is a supplier to the U.S. Navy for power generation/propulsion and launcher systems. Marine Systems has approximately 1,200 employees at the Sunnyvale location and roughly 200 at eight field site locations around the country.

There's a lot that goes into a successful security program and some may disagree with me on this, but it's my belief that three of the most critical components of a successful security program are a good self-inspection process, a robust SETA (security education, training and awareness) program, and a dedicated team of well-trained and experienced professionals.

Self-inspections

A good self-inspection program is critical to the success of any site's security program. The self-inspection checklist is a good starting point but the old thought process of conducting one self-inspection midway between DSS assessments simply isn't adequate, particularly for a large facility with lots of moving parts. What we've found works best for us is an ongoing/year-round process where we take the various sections of the self-inspection checklist and spread it out throughout the year with several areas that are reviewed multiple times during the year, e.g., we do a 100 percent classified inventory which is reviewed three-to-four times per year.

For us, the toughest part of the self-inspection process (besides fitting it all into the schedule) is documenting everything. When you find something that needs to be fixed, the tendency can be to simply fix it and move onto the next thing. Taking the time to stop and document what was found, what caused the issue as well as what actions were taken to fix it can help to identify patterns and potential problem areas that may need more long-term improvements to prevent a recurrence. We maintain a large binder of all our self-inspection records that we add to throughout the year; these records are made available to DSS during the annual security vulnerability assessment.

Security education, training and awareness

A good SETA program needs to be meaningful, and a bit of fun certainly goes a long way in getting our message out there. Being a part of a large corporation means that we have access to a wide variety of SETA materials including annual refresher briefings, newsletters, posters, etc. These are all great tools in helping us meet the requirements of the National Industrial Security Program Operating Manual, but more is needed.

At our location, our employee base varies from a large population of union touch-labor to highly educated technical professionals (engineers) and managers. What works for one group may not work for the other, so we need to tailor information to fit the needs of both groups. For example, we can gather a large group of engineers in a room and provide them with a briefing but gathering a group of shop workers means shutting down production, something that's not easily done. So when developing a new SETA tool, we always try to keep in mind who our audience is going to be and what is going to be the best way to present it.

We try to use a variety of different methods for getting the word out about security, starting with security banners at all the entrances. We do specialized briefings

(e.g., program-specific, job-specific and even holiday-themed) and quarterly newsletters. We have security slogans ("Got Security" and "Security StroNG") and a mascot, known as "Security Sam," site-specific posters (not just for our bulletin boards but also for places like the lunch rooms and restrooms), global emails, games and contests, and Security Awareness Month events including bringing in representatives from DSS, the FBI and Naval Criminal Investigative Service.

A good SETA program also includes ensuring the security staff is up-to-speed with the latest requirements, so we support memberships and participation in organizations such as NCMS and the American Society for Industrial Security. We also support courses through STEPP/Center for Development of Security Excellence, and certification programs such as the Certified Protection Professional (CPP), Security+ and others.

The team

Maintaining a high level of success can't be achieved without a strong multi-faceted team that goes well beyond the people in the security department or even the company itself.

Defense Security Service - Sites like ours cannot achieve the level of success needed for Superior ratings and Cogswell awards without having the help and support from a strong team of DSS representatives. Having a good working relationship and open communications with the lead industrial security representative and his/her team is critical...they help provide policy interpretation, assistance when needed to resolve issues, guidance, and are someone we can go to if we just want someone to bounce ideas off.

Management support – Having management support within your organization is important, not only from a standpoint of having adequate resources (budget, staffing, and equipment) but it also goes a long way to ensuring employee participation and engagement. We are fortunate to have a great management team that recognizes the importance of a good security program that doesn't just meet minimum requirements.

Employee engagement – Let's face it, without the buy-in and engagement of your employees, your security program won't even get off the starting blocks. Finding a way to get your message across to a widely varied employee base is challenging and certainly never dull.

And, finally, the security staff - The security staff is the core group that pulls the whole team together. As the Security Manager/FSO for Marine Systems, I have the privilege of overseeing a great team of people who are tasked with ensuring that Marine Systems maintains a security posture at the highest possible level to meet the ever-evolving needs of our customers.

Ultimately, there's a lot more that goes into a strong security program but with a good base of having teamwork supported by a good SETA and self-inspection framework, makes all the other aspects of a good security program work. The ultimate goal of any security team is the safety and security of our employees and contributing to the strength and success of our national security program; receiving Superior ratings and the highest honor of receiving the Cogswell award is great validation that your team is headed in the right direction!

DSS employees receive DoD and National Counterintelligence and Security Center award recognition

In August 2017, several DSS employees received award recognition for achievement in counterintelligence activities.

Kevin Flowers, San Francisco field office chief, was presented with the DoD Counterintelligence (CI) and Human Intelligence (HUMINT) for CI Functional Services-Individual award by Lt. Gen. Vincent Stewart, director of the Defense Intelligence Agency. Flowers received the award for his efforts while as a CI special agent (CISA) in the Colorado Springs Field Office.

Flowers received the award for providing sustained superior CI support and liaison to cleared industry, the Intelligence Community, and law enforcement partners, culminating in the identification and neutralization of 31 foreign targets, which included three arrests and seizure of monies. By prompting CI vigilance among cleared industry, he protected U.S. national security on the front lines of the fight against illicit technology transfers and foreign threats. He provided critical, actionable intelligence to the Colorado Springs CI Working Group, in order to counter the threat of unauthorized technology transfer. The over 700 reports collected from the defense industrial base were directly related to potential foreign collection attempts targeting DoD classified, export-controlled, and critical International Traffic in Arms Regulation (ITAR) technologies.

William Evanina, National Counterintelligence Executive, presented the following National Counterintelligence and Security Awards to DSS employees:

- **Industrial Security (Individual Category)** - Kevin Flowers, as a CISA in the Colorado Springs Field Office.

- **CI Investigations (Individual Category)** - Nick Luce, CISA, Phoenix Resident Office, Ariz.

- **Industrial Security (Team Category)** – New York Field Office, Industrial Security Field Operations, represented by:
    - Diane Craig, field office chief
    - Matthew Backus, industrial security representative
    - Janet Banzer, industrial security representative
    - Virgil Capollari, CISA
    - Maureen Hannigan, senior industrial security representative
    - Amy Juers, industrial security specialist
    - John Long, senior industrial security representative
    - Russ Reynolds, CISA
    - Laura Thoss, information systems security professional

- **Education and Training (Individual Category)** – Rebecca Morgan, Center for Development of Security Excellence

The NCSC Industrial Security Awards recognize notable activities that further the industrial security profession, function, or discipline through the application of innovative policies, practices and/or technology to protect classified information developed by or entrusted to U.S. industry.

Individual: Kevin Flowers

Flowers provided sustained superior CI support and liaison to cleared industry, the Intelligence Community, and law enforcement partners, collecting over 700 reports from the defense industrial base related to potential collection attempts targeting DoD classified, export-controlled, and critical technologies protected by the International Traffic in Arms Regulation. He referred 85 reports and generated 149 Intelligence Information reports which contributed directly to the identification and neutralization of 32 identified foreign n and domestic targets, leading to three arrests and seizure of large amounts of money. By promoting CI vigilance among cleared industry, he protected critical U.S. national security components, on the front lines of the fight against illicit technology transfer and foreign threats. Flowers worked hand-in-hand, providing critical, actionable intelligence to the Colorado Springs CI Working Group, in order to counter the threat of unauthorized technology transfer to foreign nations.

Team: New York Field Office

The New York Field Office displayed the greatest level of innovative practices in their pursuit to guard the National Industrial Security Program, protect classified information/technology through the identification of foreign intelligence entity threats, and communication of these threats to stakeholders. They executed a trailblazing non-traditional security vulnerability assessment that identified CI and security flaws at two facilities housing sensitive trusted foundry technology. The team implemented a risk-based approach to education and support to cleared industry and other government agencies, resulting in a 12 percent increase in suspicious contact reports and a 35 percent increase in agencies opening investigations and operations.

CI Investigations – Individual: Nick Luce

The CI Investigations Award is given for the application of investigative tradecraft and analysis that aided in the identification and neutralization of ongoing foreign intelligence entities' operations directed against U.S. national interests. It recognizes exemplary achievement related to participation in a formal investigation related to espionage, other intelligence activities, sabotage, assassinations, or international terrorism that has significant impact on the nation's security. This award recognizes those activities that further the CI investigations profession, function, or discipline.

Luce collected over 1,800 reports from cleared industry related to potential foreign collection attempts targeting DoD classified, export-controlled, and critical technologies protected by the ITAR. He referred over 300 reports and generated over 300 research, development, and acquisition intelligence information reports which contributed directly to the identification and neutralization of 48 identified foreign and domestic targets. By promoting CI vigilance among cleared industry, he protected this critical U.S. national security component, on the front lines of the fight against illicit transfer and foreign threats. Ultimately, the critical, actionable information he provided to the Phoenix and Tucson Counterintelligence Operations Groups directly impacted the threat of unauthorized technology transfer to foreign nations.

Education and Training - Individual: Rebecca Morgan

The Education and Training Award is given for the application of notable efforts to ensure that the Intelligence Community has effective learning programs strategically designed to assist CI and security professionals in developing and refining their substantive and tradecraft skills, competencies, and expertise to foster a cadre of future CI and security experts and leaders. This award recognizes the most exemplary achievements related to training or educating the CI/security community and furthers the education/training profession/function, or discipline.

Morgan distinguished herself serving as acting curriculum manager for the Counterintelligence and Insider Threat Awareness Curriculum. Morgan's team developed 15 new CI and Insider Threat training products during the year, which were received by 817,683 students, including 72,123 completions by cleared defense contractors meeting new training requirements directed by the policy change to the National Industrial Security Program Operating Manual.

DSS employees garner three awards at NCMS TRAINING SEMINAR

by Beth Alber
DSS Public Affairs

During this year's annual NCMS training seminar, three DSS employees were presented with Industrial Security Awards.

Robert Gerardi, Industrial Security Specialist, Melbourne Field Office, who was recognized for assisting with the formation of the Florida Industrial Security Working Group (FISWG). The FISWG is comprised of contractor and government security professionals dedicated to raising security awareness within the security community.

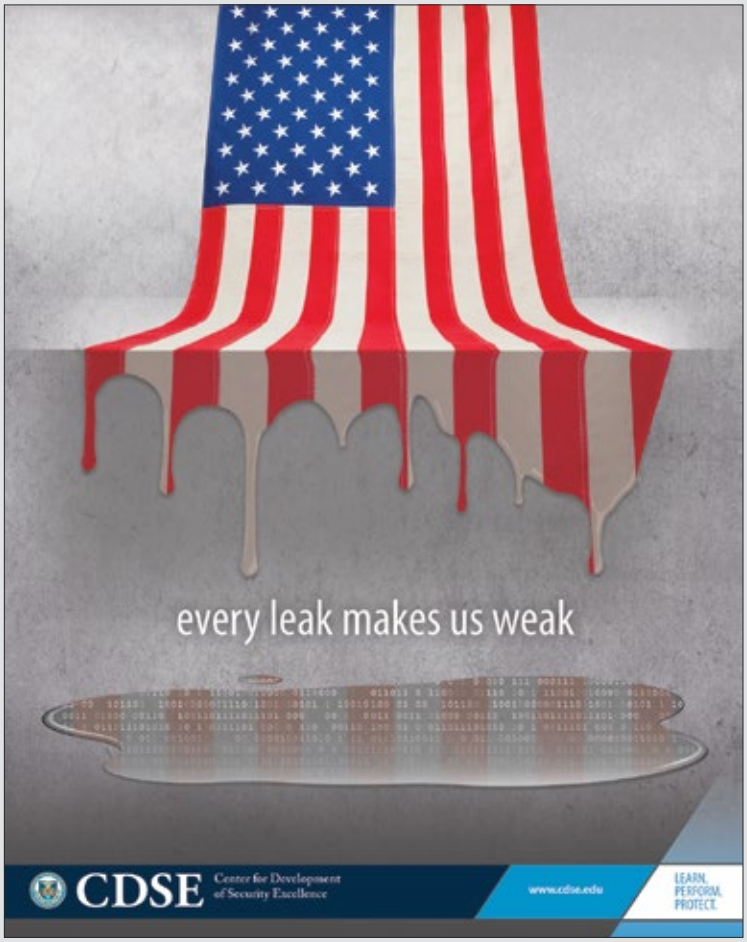
Joseph Parker, Counterintelligence (CI) Special Agent, Huntsville Field Office, was recognized for his support to the Huntsville cleared defense contractor community, providing security training on the insider threat requirements in Conforming Change 2 of the National Industrial Security Program Operating Manual, and for the establishment of a CI-focused working group for information systems security professionals.

Michelle L. Yoworski, CI Special Agent, Morrisville Resident Office, who received the award as one of the three founders of the RED DART-North Carolina team, which is comprised of counterintelligence personnel from various Federal agencies and the intelligence community, in an effort to combine resources, share intelligence, provide joint outreach to industry, and open joint investigations and operations.

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

- 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.

Robert Gerardi (second from left), industrial security specialist in the Melbourne Field Office, receives the NCMS Industrial Security Award along with Steve Abounader (second from right), Lockheed Martin Corporation. Dennis Arriaga, NCMS President (left), and Jane Dinkel, Lockheed Martin, stand with the winners. (NCMS photo)



CDSE captures first place in NCMS poster competition

The Center for Development of Security Excellence (CDSE) has supported the annual NCMS Conference for more than 10 years. Every year the conference hosts a poster competition where organizations are able to submit poster designs in various categories (professional design, contemporaneous, etc.). This year CDSE had the honor of taking home first place in both the Professional Design and the People's Choice Award. The People's Choice award in particular was a significant feat since CDSE competed against 94 other posters on which the 1,500 conference attendees voted.

The winning poster, "Every Leak Makes Us Weak," was a collaborative effort among CDSE employees, designed as a result of an internal contest.

Robert Gerardi

After observing a lack of formal education and training opportunities within the local security community, Gerardi partnered with Steve Abounader, Lockheed Martin Corporation, to create the FISWG. The working group provides a forum to broaden the knowledge of local security professionals and offers up-to-date security education and training to the security community by gathering subject matter experts from government agencies, professional organizations, and experienced security staff knowledgeable in various areas of national defense information.

"I was jointly nominated for this award with Steve for our work in providing security education to the community through our local FISWG," said Gerardi. "The FISWG has created a partnership with NCMS to hold security events that help educate, train and foster an environment of sharing within the security community."

The FISWG provides quarterly security training seminars for all levels of security professionals, and subject matter experts provide training on topics to include personnel security clearances, self-inspections, file management, suspicious contact reporting, Insider Threat, etc. Since 2008, FISWG has organized 25 training seminars providing more than 28,450 hours of instruction to the thousands of people who have attended these events.

"The FISWG puts on four training events a year for free to the local security community and gets between 160-180 attendees per event," Gerardi said. "We come up with the agenda for each meeting and call on SME's within the local community and across the country to speak on security relevant topics that are applicable to everyone."

The FISWG teamed with the local NCMS and created a strong relationship with NCMS Chapter Chair Dela Williams, University of Central Florida, to sponsor the events together to foster the sharing of information. The FISWG also has a website with relevant security information, and past briefing presentations so they can be referenced for those individuals who couldn't attend the training events.

Joseph Parker

Parker is actively engaged with local cleared defense contractors, and was instrumental in the establishment of the Huntsville Information Systems Security & Counterintelligence (ISSC) working group. It was designed for information systems security professionals managing classified networks with the goal of leveraging the counterintelligence and information security disciplines to mitigate external and internal threats to classified networks. Concurrently, the working group offers a great opportunity for management personnel and/or program managers to get a perspective on the threats that drive regulatory guidance and the complexity of managing these risks. He formed the CI-focused working group to explore threats to classified information systems from both the insider and advanced cyber threat perspectives, believing it would mutually benefit both cleared industry and the U.S. government.

Additionally, Parker provides security education and training presentations to the cleared companies and to the NCMS Mid-South Chapter, specifically on the Insider Threat requirements in Conforming Change 2 of the NISPOM. He was the impetus behind establishing the Rocket City Threat Awareness Conference, an annual all day classified conference held in coordination with the local FBI office, which had both industry and government attendees.

Michelle Yoworski

Yoworski is one of the three founders of RED DART-North Carolina, which is a unified, cross-agency team of counterintelligence professionals from various federal intelligence agencies dedicated to the protection of classified and sensitive technology research throughout a given area of responsibility. RED DART is a federal agency counterintelligence working group that operates regionally but is inter-connected with other RED DART teams throughout the country.

Once the inaugural team was created, others quickly followed. Today there are 15 RED DART teams assisting security professionals with information and assistance. RED DART-North Carolina assists each new RED DART team being formed so that they can efficiently and effectively provide valuable security assistance to the security professionals in their area.

RED DART-North Carolina also conducts outreach events, providing in-person training to several NCMS chapters, as well as at the national seminars, resulting in improved and enhanced performance in industrial security. Additionally, they provide monthly newsletters intended to educate readers on events and items of interest relating to technology protection and counterintelligence throughout the United States.

Michelle L. Yoworski (second from left), counterintelligence special agent, Morrisville Resident Office, receives the NCMS Industrial Security Award as one of the three founders of the RED DART-North Carolina team along with FBI special agent Lou Velasco (second from right). Not present to accept the award was Naval Criminal Investigative Service special agent Brent Underwood. Dennis Arriaga, NCMS President (left), and Jane Dinkel, Lockheed Martin, stand with the winners. (NCMS photo)

DSS Excellence in Counterintelligence

DSS Director Dan Payne presents the DSS Excellence in Counterintelligence Award to the 2017 winners – **TOP:** Honeywell International, Inc. **BOTTOM LEFT:** DRS Technologies, Inc. **BOTTOM RIGHT:** Lockheed Martin Corporation. DSS established the award to recognize cleared contractors who achieved extraordinary accomplishments in helping to thwart foreign directed theft of U.S. defense technology.

THE DSS CI STRATEGIC ENGAGEMENT DIVISION fosters collaboration, information sharing

by Bryan Galloway
Counterintelligence Directorate

The mission of the Strategic Engagement (SE) division is to develop, consolidate, execute, and expand industry and government CI partnership and collaboration efforts.

Chief among the division's functions is management and administration of the CI Partnership with Cleared Industry program. The program operates under a relatively simple concept of operation, collaboration between government and industry to continuously increase effective communication, information sharing, understanding, awareness, and resolutions to advance the CI directorate's mission of *identifying unlawful penetrators of cleared U.S. defense industry and articulating the threat for industry and U.S. government leadership.*

Strategically, the program increases U.S. government efforts to foster enhanced security and CI engagement against foreign intelligence entities (FIE), setting conditions for uncompromised delivery of classified technologies and services for the warfighter. At present, the partnership is comprised of CI and security experts from 13 companies in the National Industrial Security Program. Combined, these companies support a substantial number of DoD's major defense acquisition programs.

To build on the success of the program, DSS sought to expand the engagement, information sharing and collaboration by hosting quarterly secure video teleconferences with industry. A large increase in participation and positive feedback from industry attendees led DSS to hold the secure teleconferences on a monthly basis beginning in November 2016 and continuing monthly since. DSS partners with law enforcement and intelligence community agencies to prepare and deliver timely, actionable briefings, designed both to inform security programs and to establish requirements for relevant collections. These sessions have reached more than 2,000 industry security personnel.

In addition to partnering with industry, the division also

develops and maintains national level collaboration with other federal agencies whose missions complement DSS. The division manages liaison relationships, formal partnerships, and ad-hoc cooperation, focused on ensuring that information, chiefly provided by industry to DSS, contributes to enhancing national security and disrupting our adversary's efforts to steal sensitive information.

Director Payne recently told the DSS workforce, *"This agency is poised to revolutionize the industrial security oversight model. Where DSS has traditionally concentrated on schedule-driven NISPOM compliance, we will be moving to an intelligence-led, asset-focused, and threat-driven approach designed to help our industry partners better protect critical technologies and national security information."* The division is fostering collaboration and information sharing that enables faster, more efficient and effective protection of critical capabilities and technologies.

CDSE hosts concurrent live/virtual seminar

In June, the Center for Development of Security Excellence (CDSE) hosted a live, virtual session of the popular "Getting Started Seminar for New Facility Security Officers (FSOs)." This session is the first of its kind streamed live, while the in-person seminar took place at the Linthicum, Md., facility. It was a resounding success with 38 virtual attendees, as well as 33 in-person attendees.

The use of the Adobe Connect as a concurrent virtual classroom to the actual classroom allowed CDSE to offer this training to additional students who attended with little or no cost to their company. Virtual students participated from over 15 different states, including Arizona and Colorado. Not only were the virtual students able to attend the training, they had the opportunity to participate in every practical exercise, ask questions, and provide feedback through the use of an instructor/moderator who worked exclusively with them during the entire course.

Student feedback was very positive. Most students thought the addition of the virtual audience enhanced their overall training experience as it provided the opportunity to learn from an expanded network of security personnel.

This was the first time the boundaries of an instructor-led course were expanded to include a virtual audience. This course enabled CDSE to reach more students who would not have otherwise been able to attend, and also save travel and training funds at the same time.

INTRO TO CI COURSE: Members of the Introduction to Counterintelligence Course 02-17 take a group photo at the FBI National Academy, Quantico, Va. The one-week resident course introduces DoD and federal government counterintelligence principals and techniques to security professionals.

DSS employee is first student to earn all five CDSE Education Certificates

CDSE Acting Education Division Chief John (Scott) Hill (left) presents Curtis Cook, Huntsville Field Office, with the Certificate in Security Management.

by Julie Wehrle
Center for Development of Security Excellence

Curtis Cook, a DSS information systems security professional (ISSP) team lead in the Huntsville Field Office, Ala., is the first Center for Development of Security Excellence (CDSE) student to earn all five CDSE Education Certificates offered by the Education Program. In 2014, he was the first DSS student to earn an Education Certificate and the first CDSE student to earn the Certificate for Systems and Operations. Other certificates soon followed and he earned the last one, the Certificate in Security Management, in April 2017.

The CDSE Education Program offers a curriculum of advanced and graduate courses designed specifically to broaden DoD security specialists' knowledge and understanding of the security profession and prepare them for leadership positions and responsibilities. The virtual instructor-led courses are all tuition free.

Students can earn Education Certificates by successfully passing four CDSE Education courses in any of five concentrations. The virtual instructor-led courses are all tuition free. The five Education Certificates are:

Certificate in Risk Management - Provides students with the skills they need to develop and execute responses to a wide range of challenges. The courses provide an understanding of the major threats to the DoD, as well as the DoD cross-disciplinary security functions and fundamental concepts of research and statistics that support the missions of DoD commands and agencies.

Certificate in Security Leadership - Provides the skills needed to lead effectively in increasingly complex environments, as the courses facilitate an understanding of the cross-disciplinary DoD security functions, and effectively communicate challenging issues to decision makers.

Certificate in Security Management - Provides students with the skills they need to manage complex security issues while protecting an organization's resources and information. The courses help develop an understanding of security program evaluation and assessment procedures, financial and budgeting processes, as well as human resource recruiting, staffing and management.

Certificate in Security (Generalist) - Supplies the skills needed to succeed in a Security Generalist career path. The four courses facilitate an understanding of the bureaucratic politics and organizational approaches used to perform cross-disciplinary security functions within DoD, as well as security program evaluation and assessment procedures, and the legal requirements that define and limit the DoD security mission.

Certificate for Systems and Operations - Provides students with the skills needed to integrate information technologies, and DoD systems into increasingly complex security environments. The courses provide an understanding of the opportunities and risks of operative information systems to the cross-disciplinary DoD security functions.

Cook joined DSS in September 2010 in the Suisun City, Calif., Resident Office. In 2013, Cook transferred to the Hurlburt Field, Fla., Resident Office, and started his pursuit of the CDSE Education courses and certificates. "I was already taking CDSE classes and got into a rhythm of completing assignments. The certificate material was directly related to DoD, and it gave me a deeper understanding of our policies and procedures," he said.

"It's hard to find a program that matches the CDSE's since it's geared for the DoD security professional," Cook continued. "The courses do a deep dive into DoD regulations and national standards; and its great engaging students from DoD components or other federal agencies."

Cook, who transferred to Huntsville in 2016, believes the courses provide a sound security foundation and would benefit all elements of security professionals. "Supervisors or aspiring supervisors would benefit from the Certificate in Security Management," he said. "ISSPs and those in the information technology management job series would do well with the Certificate for Systems and Operations, and the Certificate in Security (Generalist) is a good certificate to obtain for a general look at what security administrators are doing for DoD."

One of the courses in the Risk Management Certificate entails an entire semester writing a research paper on either the intricacies of analytical risk management when considering adversaries and threats or effective techniques for communicating challenging issues to decision makers across the DoD. Cook added that all of the CDSE Education courses support "DSS in Transition," moving to an intelligence-led, asset-focused, and threat-driven approach to industrial security oversight.

The CDSE Education advanced and graduate courses are open to U.S. federal government civilian and U.S. military personnel only. Successful completion of the courses earns credit recommendations through the American Council on Education (ACE). This allows students who complete these and other CDSE higher-education courses to transfer credit towards a bachelor's or master's degree at participating universities. More information on the program is available from the CDSE website.

What advice does Cook give for those just starting the certificate coursework? "Every class is different, and some are harder than others. Start by taking a course you're comfortable with and don't give up mid-semester," he said. "Like real college life, sometimes life will get in the way. Just stick with it and manage your weekly assignments."

> "The **certificate material was directly related to DoD**, and it gave me a deeper understanding of our polices and procedures."

A Q&A with **Andrew Branigan**, Chief, Program Integration Office (PIO)

Editor's Note: *The following is the latest installment in a series of features on the DSS senior leadership team.*

As the PIO chief, Andrew Branigan ensures requirements are identified, programmed for and managed in a consistent and coordinated fashion through advanced planning, collaboration, requirements clarification and communication. He also acts as a liaison between support functions and operations; facilitates advanced planning through integrated project teams and working groups; and reviewing and analyzing business processes for improvements.

Prior to joining DSS in January 2013, he served as the deputy director of Innovation and Collaboration, Intelligence Systems Support Office (ISSO), Office of the Secretary of the Air Force. He began his federal service with the Department of Justice as a Deputy U.S. Marshal in 1985, and transitioned to Air Force federal service as one of the first Air Force Palace Acquire Security Police Interns. During his Palace Acquire internship, he was the first Air Force Security intern ever selected to represent the Air Force in a 4-month internship at the Office of the Under Secretary of Defense for Policy. During his 30 years of government service he has held a variety of positions with increasing responsibility, to include Contracting Officer's Representative, Information Security Specialist, Resource Protection Specialist, Program Security Officer, Chief Security Special Programs Office, Program Management, Intelligence Specialist, and Director, Business Process and Support.

Branigan earned a bachelor's degree from Indiana University of Pennsylvania in Criminology.

Q: Tell us about your background.

I was four years old when I came back from living in Africa, and I spent most of my early youth growing up on a subsistence farm in northeast Pennsylvania. After graduating from college, I started my federal career in the U.S. Marshal Service. I moved quickly to the Air Force federal service as one of the first interns in the Air Force Palace Acquire Security Police career field and spent over 26 years with the Air Force. During my Air Force time, I held a variety of positions with increasing responsibility from Information Security Specialist, to Director, Business Process and Support. I came to DSS a little over four years ago to stand up the Program Integration Office. I have had a fantastic career of over 30 years due to the quality and caliber of people I worked with and for. It's humbling to come to work every day with people who put mission before self.

Q: What lead you to this position?

I've always appreciated a challenge! DSS has an incredibly important mission and senior leadership realized DSS needed a focal point within the agency to coordinate a myriad of activities, de-conflict priorities and work with enabling elements to provide a consistent path to continual improvement.

Q: One of the reasons for originally standing up the office was Secret Internet Protocol Router Network (SIPR) to the field; to take a corporate look at an initiative, vice staying in stovepipes. What is that status of that effort and how did that lead to other initiatives?

It was a huge success. SIPR capability at all DSS facilities improved productivity, quality of life and provided secure communications throughout the enterprise. The new SIPR desktops are conservatively saving over $500,000 a year in downtime and have positioned us for the DSS in Transition way forward using classified methodologies.

It was also a blueprint to approaching future enterprise initiatives. It was a great learning opportunity and we still learn with every new project.

Q: How has the office changed since this original concept?

Our initial success led to putting additional structure into not just an integration office but a full enterprise program management office.

Q: What is the current mission/vision for the Program Integration Office?

Our mission is to use advanced planning, collaboration, requirements clarification, and communication to ensure requirements are identified, programmed for and managed in a consistent and coordinated fashion.

Q: The Services Requirements Review Board (SRRB) validates requirements and looks for cost savings by eliminating redundancies. The SRRB process is expected to identify opportunities for reductions and efficiencies. Are we on track to realize these efficiencies, and are you targeting specific areas during the review?

Yes, we are on target to realize these savings this year and across the Future Years Defense Program. We have been targeting support type services and subscription renewals in an attempt to consolidate areas where there are multiple separate contracts supporting individual mission areas. By consolidating these services or subscriptions, the agency can take advantage of quantity discounts and better use a standardized enterprise approach vice the stovepipe fashion. This ensures that options, renewals, and modifications have priority for acquisition purposes and also promotes increased visibility for capabilities associated with new services requirements.

Q: Do you encounter any challenges that you'd like to share?

One of the great things about DSS is it is a dynamic organization. We have to be flexible and responsive to shifting national priorities and uncertain budgets. The challenge is to find the most efficient way to attack requirements while also being good stewards for PIO customers, and increasing internal and external stakeholder satisfaction.

Q: What should DSS employees know about the office?

We are working for every member of DSS to develop and improve business processes and bring on the tools to better accomplish their missions.

Oklahoma City Remembrance

'We come here to remember those who were killed, those who survived and those changed forever'

by Denise Arel, *Office of the Chief Financial Officer and* **April Moore**, *Office of the Chief of Staff*

Editor's note: *The following is a first-hand account of two DSS employees who attended this year's Oklahoma City Remembrance Ceremony. The article reflects their thoughts and opinions.*

April 19, 2017, marked the 22nd anniversary of the bombing of the Alfred P. Murrah Federal Building in Oklahoma City. The Murrah building housed a day care center, credit union, snack bar, and 16 federal agencies, to include the Defense Investigative Service (the forerunner to the DSS). Each year on the anniversary of the bombing, downtown Oklahoma pauses for a memorial ceremony to honor the lives of the fallen and their families.

DSS Chief of Staff Troy Littles (center) stands with the daughters of Defense Investigative Service employee Norma "Jean" Johnson and Oklahoma Governor Mary Fallin (second from right).

Over the years, a number of DSS senior leaders have attended the annual memorial ceremony and this year DSS Chief of Staff Troy Littles represented the agency.

The outdoor memorial is administered by the Oklahoma City National Memorial Foundation, with National Park Service staff on hand to help interpret the memorial for visitors. For the first-time visitor, the experience is breathtaking. Each detail is a symbolic reminder of the tragic event. For example, the Field of Chairs are nine rows of empty chairs which represents each floor of the Murrah building and symbolizes where each person was located in the building at the time of the attack. The chairs are hand-crafted from glass, bronze, and stone with the names of the 168 victims etched in the glass base. The twin bronze monumental Gates of Time frame the moment of destruction at 9:02 a.m. The 9:01 East Gate symbolizes the city's innocence before the attack. The 9:03 West Gate symbolizes the moment when lives were changed forever and the hope that came from the horror. The gates border the Reflection Pool, whose shallow and calm surface offers its visitors a place of quiet retreat.

After giving time for family and friends to attach flowers, photos, and other mementos to the chairs, the ceremony began with a rich, harmonic bag pipe procession followed by introductory remarks from Michael Turpen, chairman of the Oklahoma City National Memorial Foundation. At 9:02 a.m., the crowd paused for 168 seconds of silence – one second for each life lost. Oklahoma Governor Mary Fallin then offered remarks. Senator (R-OK) James Lankford introduced guest speaker The Honorable Ben Carson, Secretary of Housing and Urban Development, who delivered a speech titled, "You are Not Forgotten." The event concluded with the reading of the names of the 168 people who died in the attack. Oneta Johnson, daughter of Norma "Jean" Johnson, read the names of the five DIS employees killed on the third floor of the Murrah Building – Robert G. Westberry, Larry L. Turner, Johnson, Peter L. DeMaster, and Harley Richard Cottingham.

Following the memorial ceremony, we visited the Field of Empty Chairs adorned with flowers and other items of remembrance where we received a warm welcome from the DeMaster, Johnson, and Turner family members who were in attendance. Each family shared memories of their loved ones. They also urged the DSS representatives to visit the Oklahoma National Memorial Museum that shares the memorial space and encompasses the land where the Murrah Building once stood, as well as the surrounding area devastated during the attack.

The chair for Peter L. DeMaster, Defense Investigative Service employee, in the Field of Empty Chairs.

Touring the museum was an emotional experience. Walking through the events of that day, we were able to hear the sound of the bomb, observe breathtaking displays of recovered possessions, and hear from survivors and the family members of those who lost loved ones. It added another layer of appreciation and honor to those who lost their lives and survived that horrific day.

As first time guests to the Oklahoma City Memorial Ceremony, we found the words that are inscribed outside each of the Gates of Time to be most fitting to describe our visit:

"We come here to remember those who were killed, those who survived and those changed forever. May all who leave here know the impact of violence. May this memorial offer comfort, strength, peace, hope and serenity."

Program provides agency with resources; **provides interns with experience**

College students often find themselves in a Catch-22 situation -- to get a job, you need experience. But to get experience, you need a job. Internship programs are a great way to obtain the necessary experience, and DSS conducts both paid and unpaid intern programs.

The Human Capital Management Office (HCMO) Paid Student Internship Program (PSIP) is a summer-long, full-time, temporary employment experience designed to attract high caliber college and graduate level students with an interest in federal government careers, provide real-life, relevant work opportunities, and network with professionals in a variety of fields.

Since fiscal year 2016, DSS has hired 36 interns, working in positions in the headquarters, Center for Development of Security Excellence (CDSE), and at 12 field offices, with two interns obtaining full-time positions at DSS. "As competition for top talent continues to intensify, DSS plans to use the PSIP as a recruitment and retention tool, providing future leaders with hands-on training, practical experience, and networking opportunities designed to help the agency successfully achieve its mission," said Laura Szadvari, HCMO Recruitment manager.

The PSIP aims to develop a pipeline of potential candidates for consideration in the industrial security, counterintelligence, and education services mission sets. During the internship, hiring managers monitor and assess students' work performance, familiarize the student with the agency mission, and provide interns with networking and training opportunities. Additionally, interns are often given hands-on experience in various functions within DSS.

"Our intern has completed many tasks that our industrial security representatives haven't had the time to accomplish," said Jeremy Lamps, senior industrial security specialist in the Huntsville Field Office. "During a Triage Outreach Program review, she identified some major issues at two facilities, and identified two other facilities no longer performing on classified contracts."

"As a CI intern, I get the chance for hands on experience," said Charity Ludwig, a Mercyhurst University senior studying Intelligence Studies and Criminal Justice, working in the Northern Region Counterintelligence Office. "I've been given the chance to write reports, and while I wasn't good in the beginning, the analysts were there to help."

"I am a big proponent of internship programs as I was once an intern," said Naimah Thompson, deputy chief of the Program Integration Office. "I learned a great deal from all my previous experiences as they helped set the foundation for my career. Internships allow students to gain work experience, develop hands on skills, make connections and strengthen their resume."

"This program is a worthwhile investment, as it exposes the college student to not only the DSS mission but also the intricacies of the contracting process and how integral it is in supporting the DSS mission," said Stephen Heath, deputy chief of the Office of Acquisitions. "It also provides the intern an understanding of how rewarding a career as a government civilian can be, and the impact one person can make in supporting the DSS and DoD mission."

The interns start the program between late-May to mid-June, depending on their preferences. HCMO conducts a New Intern Orientation to complete onboarding requirements, as well as provide a wealth of information on the agency. Additionally, each student is assigned a sponsor whose responsibility is to assist the student with meeting all objectives, maintaining punctuality and attendance, and ensuring compliance with agency and internship program policies.

Throughout the program, HCMO provides several opportunities for students to further their professional development by hosting a Director's Roundtable, where interns hold a group discussion with the DSS director, and Lunch and Learn sessions, where guest speakers cover a variety of topics.

Several DSS offices have hosted interns more than once, after realizing the benefits of the program.

"One of the biggest advantages for DSS is that we are not only exposing a new workforce to the life of a government employee, but DSS gains valuable inspiration

Interns participate in a Director's Roundtable, listening to DSS Director Dan Payne relate his experiences in the Central Intelligence Agency, and then asking questions about career opportunities and tips for networking.

from these interns," said William Howard, chief of the CDSE Multimedia Branch, who has hosted interns five times. "By going through the process of explaining why we accomplish certain tasks the way we do helps me to examine our internal processes."

"Prior to this summer, we have hosted three interns, and each of them enriched our experience as DSS employees by allowing us to share our mission, our values and our experience with someone interested in future government service," said Beth Whatley, Virginia Beach Field Office Chief. "One of our former interns is now working for the National Security Agency, and another is now a DSS industrial security representative – so our track record is very positive."

While getting experience is paramount to getting a job, many interns view their work with DSS as much more than a job, and would recommend the internship opportunity to others.

"I chose an internship with DSS because of the opportunities for growth, skillset and exposure that I knew would come with the experience," said Amanda Dupont, a Radford University junior studying accounting and finance, working in the Program Integration Office.

"The agency gives you a firsthand look into the federal government and you get to work closely with agents conducting hands on tasks," said Enrique Osborne, a Virginia State University senior studying criminal justice, working in the Capital Region.

"I would recommend a DSS internship to any student with a risk-based security interest," said Seth Markin, a George Washington University graduate student studying international affairs, working in the Enterprise Mission Management Cell.

"I would highly recommend a DSS internship to my fellow students," said Tracy Doubledee, a University of Phoenix senior studying criminal justice administration, assigned to the Huntsville Field Office. "The knowledge and experience gained by this opportunity is priceless. DSS truly wants to give you all the tools you need to succeed now and in the future."

The Paid Student Internship Program (PSIP) students are sourced throughout the fall recruitment season and asked to submit applications on USAJobs.gov during the open acceptance period in late October. The qualifications for the PSIP include being a U.S. citizen, enrollment in an accredited college or university pursuing a bachelor's or master's degree, minimum grade point average of 3.0, completion of at least 24 credit hours, and the ability to obtain and maintain a Secret clearance.

Agency hosts third **college student shadow day**

by Leila De'Vore
Human Capital Management Office

In early May, the DSS Human Capital Management Office (HCMO) hosted its third Student Shadow Day, in which 14 students from Daniel Morgan Graduate School, George Mason University, and the University of Mary Washington were paired with agency professionals to learn about the DSS mission and gain a "day in the life of" experience working in their chosen career fields.

The event kicked off with opening remarks from La Shawn Kelley, chief of HCMO, who welcomed the students and shared career advice gained from her years in federal service. Troy Littles, DSS Chief of Staff, introduced students to the DSS mission, and discussed how the agency's new tagline, "Partnering with Industry to Protect National Security," applies to the mission. Littles also provided an overview of the agency's core occupations and challenged students to use the day to solicit career-related guidance that would facilitate their entry into the intelligence community.

Students then toured the Russell-Knox Building and participated in an informal lunch session with representatives from the agency. Soon after, they met with their respective DSS employees, who they would shadow to discuss job-related goals and objectives, along with best practices for success in the workplace. Kelley wrapped up the event by sharing a few nuggets of wisdom, motivation, and encouragement for these burgeoning professionals.

Student feedback indicated that the event was an excellent opportunity to experience what it might be like to work within a federal government agency in general, and at DSS in particular.

"It was wonderful to have a point of contact with someone inside the department to ask questions and have 'inside knowledge'," one student said. Another declared, "I really appreciated the time and attention that the DSS men and women provided to inform us of what working at DSS is like. I gained so much knowledge." A third student said, "The actual shadow portion was by far the best, most interesting and useful." Another student stated, "I just want to say thank you so much for the career advice and insight into what the DSS does and how my skills can benefit the DSS mission."

TOP: Leila De'Vore, HCMO Recruitment Office, offers career advice to the students. **BOTTOM:** Briana Rudolph, George Mason University student, pitches her resume and experience during a Shadow Day exercise.

DSS professionals expressed that the experience was a great way to attract potential job candidates to the agency and develop a pipeline of future leaders. The Recruitment Office will continue to partner and build relationships with university career development offices in fiscal year 2018 in an effort to facilitate similar events in the future.

Director receives promotion from CIA

On July 5, DSS Director Daniel E. Payne was notified by the Central Intelligence Agency (CIA) that his personal rank had been elevated to Senior Intelligence Service (SIS)-5, which is the CIA equivalent of a four-star general.

Payne began his Federal career as a special agent for the Defense Investigative Service (predecessor to the DSS) in 1982. He joined the CIA in 1984 and spent most of his career in the field of counterintelligence. Over the past 35 years, Payne has worked in more than 20 countries and has been involved in numerous espionage investigations. He was the lead investigator in the Aldrich Ames investigation, playing a key role in Ames' identification, arrest, and subsequent conviction for espionage on behalf of Russia. Payne made several significant innovations to the methodology used by the CIA and other U.S. government agencies in conducting espionage investigations, which led to him being awarded the Donovan Award by the CIA's Directorate of Operations.

Payne has held several senior positions at the CIA, to include deputy chief of Counterespionage, deputy chief of Counterintelligence, deputy director of the Counterterrorism Center (responsible for the CI aspects of counterterrorism operations), a special assignment related to CIA's Enhanced Interrogation Program, assistant Inspector General for Investigations, and deputy chief of South Asia Division (responsible for CI operations). In his last position before his arrival at DSS, Payne served as the deputy director of the National Counterintelligence and Security Center.

Previously, Payne was the recipient of the National Intelligence Superior Service Medal, the Intelligence Community Seal Medallion, the National Intelligence Medal of Achievement, the Donovan Award, CIA's Intelligence Commendation Medal, and the George H.W. Bush Medal for Excellence in Counterterrorism.

DSS Director Dan Payne speaks at the annual NCMS conference.

Travels with the Director

TOP LEFT: DSS Director Dan Payne (far right) participates on an insider threat panel at the Professional Services Council Annual Conference in Williamsburg, Va. The Professional Services Council is the largest association for service contracts in the United States, and the bulk of DoD contracts under the National Industrial Security Program are service oriented. **TOP RIGHT:** In March, DSS Director Dan Payne (center) and Deputy Director James Kren (left) visited the Defence Security and Vetting Service (DS&VS) in Canberra, Australia, to share best practices and establish an open line of communication to foster greater information sharing. In June, officers from the DS&VS visited DSS to gain a greater understanding of the counterintelligence role in Industrial Security. **BOTTOM:** While in Tucson, Ariz., the director visited the Tucson Resident Office and spoke to employees about the future of DSS. He then visited the Raytheon Missile Systems facility, where DSS and Raytheon conducted a joint presentation on addressing risk and developing a tailored security program. During the visit, he was given a tour of the products manufactured at the facility (in the background of the photo).

PSMO-I initiative helps field navigate fluid personnel security environment

by Dedra Lee and Mark Hedges
Personnel Security Management Office for Industry

There are over 13,000 cleared facilities with over 900,000 cleared employees in the National Industrial Security Program. Finding information on one individual's clearance status or where in the process the individual's case is, can be daunting even for DSS employees. For companies whose facility clearance is dependent on a clearance for a senior management official, the wait can translate to delays and frustration. To provide better customer service and insight into the personnel security clearance process, the Personnel Security Management Office for Industry (PSMO-I) created and implemented a program that partners with field offices across the country. The Field Integration initiative provides additional data, personnel security subject matter expertise and overall support to the industrial security representatives as they navigate the fluid personnel security environment that exists today.

The Field Integration initiative leverages the expertise of personnel security specialists within PSMO-I by assigning a specialist to each field office to serve as a liaison and a conduit through which field personnel can get real time answers and assistance with addressing the intersection of personnel and facility clearances. The effort also combines real-time access to personnel security data, trends, and adverse information from PSMO-I with field intelligence, physical security and the agility to quickly reach vulnerable facilities via the industrial security representative. These pooled resources and extensive knowledge base make for a dynamic resource that facilitates enhanced risk analysis as it pertains to national security.

With this new initiative, the field offices now have a specific point of contact that assists with questions or concerns as it relates to personnel security. Most queries can be answered and resolved within the same day of the initial contact. In addition to having their own direct link to a PSMO-I subject matter expert, the field office can submit their individual culpability reports directly to their designated contact and also receive adverse information reporting on a quarterly basis to aid in the prioritization of facility vulnerabilities and risk assessments.

This initiative bridges the gap between the PSMO-I staff and field personnel who generally do not regularly cross paths, enhancing continuity of operations across the board. It offers the opportunity to learn more about both the personnel and facility clearance processes and the policies that regulate them. It also sheds light on the nuances that plague both sides with an opportunity to innovate and create new and better ways of mitigating risk.

Deputy director visits **TAMPA RESIDENT OFFICE**, tours cleared facility

by Jon Grogan, *Industrial Security Representative* and **Doug Hartwell**, Counterintelligence Special Agent *Tampa Resident Office*

During a recent visit to the Tampa, Fla., Resident Office, James Kren, DSS deputy director, discussed DSS in Transition, outlined the Risk-Based Analysis and Mitigation philosophy and listened to the concerns of DSS field personnel about the future of DSS.

Kren explained how DSS is working to be a full partner in the counterintelligence community and related some anecdotal accounts of how the agency is continuing to mitigate efforts to steal classified information and export controlled technologies in the hands of industry.

Kren also visited a local cleared facility under a foreign ownership, control or influence mitigation agreement. He toured the facility, saw a demonstration of the facility's products, engineering and manufacturing processes, and explained how DSS will integrate elements of DSS in Transition into a tailored, risk-based plan focusing on each cleared facility's assets, threats and vulnerabilities. During the facility tour, the facility security officer/export control officer related events concerning attempts by a person to gain access to restricted components manufactured by the company. The individual attempted to acquire an export restricted electrical component while providing falsified end-user data. The requestor, who was running a front company based out of an apartment, identified the end user as a different legitimate company, but he manipulated the contact information listing to appear as though it came from the company's e-mail, but with a small variation, so the e-mails would come to him. He also made several attempts to obtain the restricted components through foreign companies that had legitimate licenses but again the diligence on the part of the export control office paid off, and prevented the sale of the restricted items. The facility export control officer, working with DSS, coordinated with a federal agency investigating the issue, which ultimately led to a federal indictment.

Additionally, DSS CI analyzed different field reports and stitched together a pattern, which revealed the above individual was part of an illicit procurement network aggressively attempting to obtain export restricted commodities and information across the United States.

L to R: Charles Duchesne, DSS ISSP; Jon Grogan, DSS ISR; Scott Kempshall, VP TRAK Microwave; Doug Hartwell, DSS CISA; Scott Baxter, ISSM TRAK Microwave; Cindy Peeters, FSO Smiths Interconnect; Cheri Evangelist, ECO TRAK Microwave; John Perrine, AFSO Smiths Interconnect; James Kren, DSS Deputy Director; John Bennett, DSS Congressional Liaison; Ed Wheeler, DSS FOC; and Deb Del Bianco, VP TRAK Microwave.

Andover Field Office provides localized RMF training for industry

by Sean Donnelly
Andover Field Office Chief

On June 15, 2017, industrial security representatives, information systems security professionals, and leadership from the Northern Region and Andover Field Office held a Risk Management Framework (RMF) workshop at the Kostas Research Institute for Homeland Security, Burlington, Mass.

The event came about when several industry security professionals requested localized RMF training. Industrial Security Representative James Herbert worked with Information Systems Security Professional John Fratturelli who facilitated the presentation with the goal of providing an overview of the current RMF process, emphasizing that RMF continues to evolve and DSS is here to guide industry and assist them with the process.

The event attracted 76 facility security officers, information system security managers and information system security officers, representing 70 cleared facilities from Maine, Massachusetts, New Hampshire and Vermont.

The training utilized a "town hall", question and answer approach that elicited more than 55 questions from the audience. The day concluded with a panel of DSS subject matter experts, led by the Northern Region Authorizing Official Jeffrey Blood, who answered additional questions from the audience.

Feedback from Industry:

"

.....This presentation was **helpful to link the bridge to the similarities** between RMF and the C&A (certification and authorization) process

.....Explanation of the RAR (Risk Assessment Report) was excellent – it emphasized that **threat assessment is everyone's job**

.....Many aspects of the accreditation process under RMF **were clarified by the presentation and discussion**. This was very helpful

.....I **learned more** than I did from the online training

.....the "it depends" responses given as an answer is understandable and truly **shows how fluid RMF is at this time**

"