

DSS

ACCESS

VOLUME 1, ISSUE 4

OFFICIAL MAGAZINE OF THE DEFENSE SECURITY SERVICE



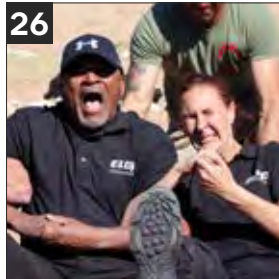
**NATURAL
DISASTERS**

TEST DSS FIELD OFFICES



WINTER 2012

VOLUME 1, ISSUE 4



SPOTLIGHT

Natural Disasters Test DSS Field Offices 4

INSIDE

Webinars Reach Wide Audience 8

Mergers, Acquisitions & Joint Ventures in Aerospace and Defense 11

RED DART Protects Classified 12

Partnership with Industry Exchange Program 14

Annual Training Touts Value of Cyber Preparedness 20

Northern Region Trains Supervisors 22

Facility Clearance Branch Embraces Change 23

ELDP Grows Future Leaders 26

Call Center Tour 35

WHO'S WHO IN THE NISP? 23

NEWS IN BRIEF 24

DOUBLE CHECK

Quality Assurance: Maximizing Agency Effectiveness 10

HELPFUL HINTS

ISFD and Safeguarding 15

DSS CASE STUDY

The Thumb Drive Smasher 16

THEY SERVE

DSS Reservists, Guardsmen Juggle Service and Duties 18

AROUND THE REGION

Enterprise Day Celebrates 40th Anniversary of DSS 30

Feds Feed Families Program 32

New Raytheon Facility Shows Benefit of Partnership 33

Colorado Springs Field Office Helps Wounded Warrior 34

DSS ACCESS

Published by the
Defense Security Service
Public Affairs Office

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

DSS Leadership

Director
Stanley L. Sims

Deputy Director
James J. Kren

Chief of Staff
Rebecca J. Allen

Chief, Public Affairs
Cindy McGovern

Editor
Elizabeth Alber

Graphics
Steph Struthers

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

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

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

FROM THE DIRECTOR

Welcome to the DSS ACCESS magazine. This marks our fourth and final issue of 2012. I knew the idea of a magazine for DSS was long overdue and that there were many stories from across the agency that were waiting to be told. We have captured much of our busy and challenging past year at DSS on these pages. I must say that the magazine has exceeded my expectations, and even I learn something new about the agency and its workforce with each issue.




The cover story of this issue looks at the DSS response to two natural disasters from this past summer: the Waldo Canyon fires in Colorado and Hurricane Isaac, which pounded the Gulf Coast. It may seem that all our emergency response plans and telework drills are just another bureaucratic check in a box for completion. But as these real-world events remind us, simply checking a box is not enough. In both of these cases, the local offices used their emergency response plans to respond quickly and appropriately to events as they developed. They evacuated, exercised telework options and kept in touch with the facilities in their areas of operation. They also had outstanding support from the regional offices, where even more DSS employees were standing by to help.

I am impressed with the level of dedication and commitment these employees exhibited during these very trying circumstances, and I am proud to be associated with them. We developed lessons learned from each event that we will use to refine our mission assurance planning. This was also a reminder to all 60 DSS locations that we were, and remain, at the mercy of Mother Nature, and it behooves all of us to prepare for and pay attention to our emergency response procedures.

I want to highlight another article as well, and that is the one on our Reservists and National Guardsmen. As anyone who has read my biography knows, I am a retired Army officer who continues to serve my country as part of the federal civilian service. I often remind DSS employees that federal civilian service is just that, service to the nation. I know DSS isn't unique in this regard, but I was impressed with the statistics on the number of retired and/or prior military service members who now work at DSS. Clearly I am not the only one who is still called to service. But our Reservists and members of the National Guard are answering two calls to service at once. They are called upon to sacrifice time with their families, juggle two careers, and deploy to troubled areas when needed. I applaud their unwavering dedication and thank them for their service.

The remaining articles in this issue highlight not only the work DSS employees are doing to develop leaders, improve processes and further the mission of the National Industrial Security Program, but also of the work they're doing in their local communities as caring and responsible citizens. Please take a few minutes to learn more about DSS.



SPOTLIGHT

NATURAL DISASTERS

TEST DSS FIELD OFFICES





The summer of 2012 will be remembered for many weather events: the extreme drought across much of the nation's mid-section, the hottest July on record and the Derecho that brought the Washington, D.C., area to its knees in early July. But two events tested DSS employees in very different ways in very different locations.

On June 23, 2012, the Waldo Canyon Fire broke out northwest of Colorado Springs and became the most destructive wildfire in Colorado history. The fire was declared officially contained about two and half weeks later on Tuesday, July 10. The fire forced the evacuation of more than 32,000 people, consumed 18,247 acres in the Pike National Forest and in Colorado Springs, destroyed 346 homes, left two people dead and is considered part of Colorado's worst wildfire season in a decade.

The Colorado Springs Field Office is located in the northwest section of Colorado Springs near the U.S. Air Force Academy. By June 26, the fire had jumped the fire line in west Colorado Springs, and was roughly five miles from the Field Office. In fact, the fire could be seen from the Field Office picture window.

While on travel to Salt Lake City, Utah, Michael Stell, Field Office Chief, coordinated with Larry Harrison, Senior Industrial Security Specialist, to execute the pre-evacuation phase of the office Continuity of Operations Plan (COOP). When Stell returned to the office on June 27, he discovered that the field office staff had executed the COOP without loss of any government equipment or injury.

The evacuation affected nine employees in the field office, and involved packing and loading approximately 300 facility folders and the two flags into eight government vehicles, and moving them to points north, east, and south of the fires to the homes of field office employees. "This team effort was the catalyst to ensuring a successful, measured response to the situation," Stell said.

Additionally, field office personnel were directed to telework until further notice. Group e-mails were sent to Facility Security Officers (FSOs) in the Colorado Springs area to determine the situation at their locations and ensure the protection of classified material. While several cleared facilities were evacuated, all material was properly protected and no cleared facility suffered any loss as a result of the Waldo Canyon Wildfire. While Erin Anderson, Field Office Administrative Support Assistant, was forced to evacuate her home, it was ultimately spared any damage and no other employees' homes or families were affected.

By June 29, the pre-evacuation phase was lifted, all items were returned to the Field Office and the telework option

was rescinded. The success of this effort was predicated on a Field Office COOP, which was a significant topic of discussion during a December 2011 Field Office meeting. The meeting resulted in the development of a limited plan that was never fully codified.

Also contributing to the office's success was Stell's participation in local workshops and courses sponsored by the Federal Emergency Management Agency (FEMA). In fact the office participated in the Mile High Tabletop Exercise in April 2012, which was designed to test an agency COOP at various levels. Stell, Anderson, Rich Owens, Industrial Security Specialist, and Joe Jackson, region IT support technician, all played a role in the exercise. The lessons learned from the Waldo Canyon Fire will help in developing a final documented COOP plan for the office.

Across the country, the Southern Region dealt with a different problem when Tropical Storm/Hurricane Isaac slammed into the Gulf Coast in late August. Isaac made landfall on Aug. 28, near the mouth of the Mississippi River, bringing high winds and prolonged rains. Hardest hit was Plaquemines Parish in Louisiana, which suffered extensive flooding. The storm also hit Gulfport, Miss., with 70 mph winds and dumped almost 11 inches of rain on the area.

Darrell Crawford and Regina Saunders, Industrial Security Specialists assigned to the Gulfport Resident Office, and Joe Campbell, assigned to Hurlburt Field Resident Office in Florida, were in Isaac's path and not only had to secure their homes and families from the storm, but the offices as well. Campbell had just completed the first week of a planned two-week trip in support of the Chantilly Field Office and returned home early to prepare for the storm. Crawford canceled an upcoming business trip to remain at Gulfport.

Kirk Paulsen, Chief of the Atlanta Field Office, began implementing the COOP on Aug. 26, when the offices and government vehicles were secured. Implementation prompted the team to send employees home to telework, if able; move government vehicles to a safer location; and ensure back-up power for the computer server was operational.

He also began periodic contact with the three employees for status updates. All three teleworked when possible, with Saunders and Crawford sheltering in place in their homes for two days with intermittent power, leaking roofs and flooded



WATER RESCUE: An Army Special Forces officer with the 2nd Battalion, 20th Special Forces Group (Airborne), Mississippi Army National Guard, helps a sheriff's deputy evacuate a local resident from a flooded area using a zodiac boat during Hurricane Isaac operations. – Photo courtesy of Army National Guard

roads. Saunders reported fluctuating power, flooding, downed power lines and debris in her neighborhood. Crawford reported seeing a tornado near his residence in Hurley, Miss., as well as severe flooding and strong winds.

“Throughout the storm, e-mails and phone calls were made to FSOs to determine the status of their homes and facilities,” Saunders said. “We offered assistance through NISPOM guidance concerning temporarily relocating offices, changes in mailing addresses, and safeguarding requirements during disasters. FSOs responded promptly, although few were able to get to their offices.”

During the storm, attempts to reach cleared facilities in the area were hampered by widespread flooding and debris in the roadways. Shipyards in Mobile, Ala., Pascagoula and Gulfport, Miss., and Avondale, La., all sustained damage but Isaac did not have any impact on their classified operations.

“Safety is always an issue when returning to these areas, as there are hidden structural weaknesses from water and wind,” Saunders said.

In spite of Isaac, Saunders was soon back in the office mopping up water, rebooting servers and laptops and closing out a Committee on Foreign Investment in the United States case. The office and government vehicles were secure with no damage.

In Florida, Campbell escaped damage to his home, but Hurlburt Field was closed for two days with flooded roads and damaged bridges. He was able to telework and check on the status of his cleared facilities, none of which sustained damage.

“The support we received from DSS was great,” Saunders said. “The DSS Headquarters leadership, the Southern Region Office, the Atlanta Field Office, and the Hurlburt Field Resident Office let us know quickly that they were standing ready to lend support. In echoing the sentiment of FSOs in this area, thanks for letting us know you were there.”

With summer giving way to fall and winter, chances are good that the weather will continue to be a challenge. As evidenced by the wildfires in Colorado and the hurricane that swept through the Gulf Coast, having an established plan is an important tool in being prepared.

Editor's Note: At the time this issue went to print, Superstorm Sandy had just hit the East Coast. DSS offices from Virginia Beach to Long Island were affected. Their story will be captured in a future issue.

PREVIOUS PAGE: The Colorado National Guard provided red-card certified aviators representing National Guard units from Colorado, Wyoming, Kansas and Nebraska to fight the fire by helicopter and hose. – Photo courtesy of Army National Guard

WEBINARS REACH WIDE AUDIENCE

The National Industrial Security Program (NISP) includes more than 13,000 cleared facilities and approximately one million cleared contractor employees. It also encompasses the government industrial security specialists working with the various departments and agencies participating in the NISP. Delivering security education to such a wide, diverse audience in an accessible, timely fashion is a challenge.

Today's fast-paced environment and limited budgets make traveling to the Center for Development of Security Excellence (CDSE) in Linthicum, Md., for formal classroom training a luxury rather than a necessity. Further adding to the challenge is an increasingly younger workforce used to less traditional learning environments. The result is a CDSE staff that is constantly looking for new technology solutions and new ways to distribute current information quickly and efficiently.

Brian Miller, Chief of Training, came up with one such solution for industry – webinars. And although CDSE plans on presenting webinars from each security discipline, the industrial security webinars, known as Learn@Lunch, were the first to deploy.

According to Christine Beaugard, Industrial Security Curriculum manager, the 30-minute sessions were a direct response to the need to provide training for facility security officers and government industrial security specialists with NISP training in a format that was accessible and available at anytime, anywhere. The goal is to host one Learn@Lunch (industry topic) on the third Thursday of each month.

"We found that for industry, any training lasting longer than 30 minutes had to be billed to a specific contract or customer," Beaugard said. "So our intent was to keep the training to 30 minutes or less and to make it even more appealing, provide it at lunchtime. Everyone takes a break for lunch." Each Learn@Lunch session is offered at 11:30 a.m., and again at 2:30 p.m. for those on the West Coast.



CDSE held three Learn@Lunch webinars in FY12: Adverse Information Reporting Requirements (July); Security Rating Matrix (August); and, Life Cycle of a Suspicious Contact Report (August). Each session saw increased participation with approximately 3,300 participants signed up and a 60 percent actual participation rate.

“We’re finding that not everyone who signs up actually participates,” said Beauregard. Currently, the webinar platform can support 1,000 participants at each session.

The webinars are hosted on Defense Connect Online, which provides DoD with worldwide web conferencing, virtual meetings, and chat services. As a result, CDSE is looking at better ways to track actual participation. Not only will this give CDSE a clearer idea of actual participation, it also provides students a better way to manage and track their webinar participation.

Tracking participation is just one of the challenges the CDSE team faces. Since the platform was already available, the team had to find a way to announce and promote the webinars.

“We also had to create the web pages, and then develop internal processes and procedures to implement the sessions,” explained Beauregard. “Our biggest challenge was that we had never presented webinars in this format before so it was a new process for everyone.”

The CDSE team continues to find support from across DSS. Heather Green, Chief of Quality Assurance in Field Operations, presented the Security Rating Matrix session, and Tom Badoud from the Counterintelligence Directorate presented Lifecycle of a Suspicious Contact Report. The webinar in October featured Keith Minard from Industrial Policy and Programs discussing a new Industrial Security Letter.

Webinar topics chosen have to be “chunked” down into manageable, 30-minute segments. “We

“TO MAKE IT EVEN MORE APPEALING, [WE] PROVIDE IT AT LUNCHTIME.

EVERYONE TAKES A BREAK FOR LUNCH.”

were looking for topics that would have broad application across the NISP, and would apply to both large and small facilities,” said Beauregard.

The CDSE industrial security staff routinely receives questions from NISP facilities. They looked at some of the most common questions, and developed webinars addressing those issues. Additionally, the webinar format is also an ideal way to promote and present new initiatives to a large audience with minimal effort.

The webinars are designed to be as interactive as the CDSE team can make them. Beauregard said they try to incorporate a “take-away” or handout for each webinar that the participant can download and print out. The presentation typically includes poll questions for participants to answer to gauge their knowledge. And the sessions also feature a live question and answer session where participants can enter a question, and the presenter will answer as time permits. All questions and answers are subsequently posted on the CDSE webinar website.

As previously mentioned, CDSE staff from other security disciplines, such as information security, physical security, etc., are developing similar sessions. The audience for these sessions is government security professionals. As a result, the sessions can be longer and offered during duty hours rather than at lunch. The first such session was offered in August and addressed information security. The team is also planning sessions focused on the internal DSS security workforce.

QUALITY ASSURANCE: MAXIMIZING AGENCY EFFECTIVENESS

By Heather Green
Industrial Security

DSS operates in a challenging environment with a nationally dispersed workforce, dynamic mission, and strained resources.

Now more than ever, it is critical that we maximize our effectiveness and consistency with oversight of classified information in the National Industrial Security Program (NISP). The Industrial Security Field Operations (ISFO) Quality Assurance Office (QAO) is poised to meet this challenge.

The QAO mission is “to build and maintain a culture of quality and consistency into daily activities, drive efficiency and process improvements at every level, and develop innovative products to better assist agency personnel in execution of the DSS mission.”

QAO accomplishes this mission through technical and subject matter expertise, application of process assessment and improvement practices, networking with government and industry stakeholders, coordinating policy and training development, to name a few.

The following QAO initiatives are designed to improve internal collaboration and provide field personnel with feedback and consistent processes that help them better accomplish their jobs.

PEER REVIEW

A peer-, field office chief- and region-level evaluation program has been developed to ensure a consistent application of oversight and policies. The evaluation program consists of peers reviewing the core mission work products of others and providing timely feedback on areas in need of improvement. This strengthens the ability to develop new tools and guidance to improve operations across the DSS enterprise.

The process has been a huge success thanks to the ISFO field personnel who participate as reviewers. Trend analysis of the results of the work product reviews is conducted to identify best practices and areas requiring additional training or policy clarification. In addition to providing invaluable data for high level change, by assessing their peers’ actions, reviewers can also enhance their own professional skillsets to deliver an immediate impact at the local level.

PRIORITIZATION MODEL

Declining resources and changes in mission sets require clear field priorities for ISFO actions to ensure DSS resources are focused where they are needed. The ISFO Action Prioritization Model has been revamped to ensure ISFO is “doing the right assessment at the right time.”

TRIAGE OUTREACH

The national Triage Outreach Program (TOP) will be fully implemented in November 2012. DSS recognizes regular communication with our industry partners is vital. The agency’s oversight role includes the accurate maintenance of core data pertaining to cleared facilities that is normally obtained, verified, and reviewed during assessment visits.

The TOP will assist in maintaining communication with industry partners between assessment cycles. This outreach initiative may include a phone call from a representative from DSS to confirm the accuracy of the data that we currently maintain pertaining to your company. Facilities will receive advanced notification from DSS prior to the call with further information.

QAO is excited to continue maximizing the efforts of the ISFO workforce in the coming years. Many current activities will continue and improve, to include: security assessment rating determinations, enhancing industry and government stakeholder partnership, prioritizing nationwide workload, personnel clearance process improvements, driving NISP vulnerability mitigation efforts, teaming with the Center for Development of Security Excellence (CDSE) to develop high-value products, and more. Future efforts will enhance mission areas and drive continued increases in DSS quality standards.

MERGERS, ACQUISITIONS & JOINT VENTURES IN THE AEROSPACE AND DEFENSE SECTOR

By Shana Dittamo

Industrial Policy and Programs

Despite an unpredictable economy and uncertainty in future defense budgets, mergers, acquisitions and joint ventures in the aerospace and defense sector (A&DS) are on the rise, both in dollar value and number of transactions.

According to a PricewaterhouseCooper press release, there were 341 A&DS merger and acquisition deals, valued at \$43.7 billion, in 2011 — making it a record year. Nearly a third of the value was generated from the largest such merger in history, the United Technologies acquisition of Goodrich Corporation, announced in September 2011 and completed in July 2012.

Mergers and acquisitions differ from joint ventures in two distinct ways: ownership transfer between companies, and nature and scope of the contract. A merger or acquisition involves the transfer of ownership either by forming a brand new merged company or by one company absorbing the other. A joint venture is created when two or more individuals or business entities form a contractual agreement for the purpose of executing a particular business activity. In contrast to a merger or acquisition, no ownership of either company changes hands in a joint venture. Also, the scope of a joint venture is limited to a specific purpose and generally has a defined end, while mergers and acquisitions are permanent changes to the corporate structure.

Significant value can be created for companies joined together by a merger or acquisition. Synergistic systems can enhance revenue and eliminate unnecessary costs. Economies of scale, or value that is created when production increases, can improve cost efficiency. Mergers and acquisitions can also increase market share, generate tax savings, allow geographical diversification and enhance competitive edge by gaining new technology from the acquired company.

When a National Industrial Security Program (NISP) company is involved in a merger or acquisition, DSS examines each company to ascertain the security risk, particularly as it relates to foreign ownership, control or influence (FOCI). A FOCI determination can be more challenging if the business

structure of the newly formed company is extremely complex and convoluted. Mergers often involve a change in the management structure, and the Industrial Security Representative should ensure the company updates its Key Management Personnel list and that the appropriate employees are cleared at the required level.

Like mergers and acquisition agreements, joint venture agreements can involve complex contractual relationships and require careful review of the parent structure for each member of the joint venture to ascertain the potential risk to national security. As a general rule, each joint venture member must be processed for a facility clearance.

However, when one or more — but not all — of the joint venture participants requires access to classified information, those entities not requiring access may be excluded by formal agreement. The agreement must clearly state that the uncleared contractor(s) will be effectively excluded from access to classified information; that safeguards are in place to preclude transfer of technology and intellectual property to the uncleared company; and the financial arrangement for distribution of profits and losses among the members.

The inherent value of joint ventures is typically created when companies are able to penetrate markets that would otherwise be difficult to reach. They are widely used by companies to reach foreign markets by partnering with domestic companies that are already in the desired market. For example, if a United States company is interested in marketing its product in Canada, it may be beneficial to partner with a Canadian company that is already familiar with the culture and the political and legal environment. Additionally, the foreign company may bring new technologies to the joint venture, while the domestic company already has a foothold with existing relationships.

Mergers, acquisitions and joint ventures can be beneficial endeavors for companies in the NISP, but because of their complexity, DSS must take extra care to ensure the process is properly vetted by reviewing contractual documents, the management structure (to include KMPs), the potential for technology and intellectual property transfer, and profit and loss sharing agreements.

RED DART

PROTECTS CLASSIFIED

PROGRAM STRENGTHENS EXISTING, ESTABLISHES NEW RELATIONSHIPS

By Matthew Guy
Counterintelligence

In early 2011, Stan Sims, DSS Director, laid out his goals for DSS. The first was to “identify and reduce vulnerabilities and threats to the defense industrial base” by developing innovative products and service-delivery models to increase our value to government and industry. He also wanted to strengthen existing partnerships and establish new ones with government, industry, and international stakeholders to increase awareness of DSS and improve information sharing, open communication, and transparency.

Michelle Brody, Field Counterintelligence Specialist (FCIS) in the Virginia Beach Field Office, turned those words into action through her participation as one of the founding members of the RED DART program. RED DART stands for Research and Development Defense Alliance of the Research Triangle. It is a unified, cross-agency team of counterintelligence professionals throughout North Carolina and South Carolina who are dedicated to the protection of classified and sensitive technology research.

RED DART became operational in October 2011, with inaugural participation by counterintelligence special agents from the Federal Bureau of Investigation, U.S. Air Force Office of Special Investigations, the Naval Criminal Investigative Service, and DSS. Due to the program’s success, participation has expanded to include the U.S. Army 902nd Military Intelligence Group, Homeland Security Investigations, Defense Criminal Investigative Service, U.S. Army Criminal Investigations Division, and Coast Guard Investigative Service. RED DART operates under a “shared leadership” principle, which allows each partner agency to own the program while being responsible and responsive to the other partner agencies.

“One of the most common questions we get is ‘Who owns this program,’” said Brent Underwood, NCIS Special Agent, Cary, N.C., resident agent office. “The answer is we all own it. The partners contribute as much or as little as they see fit, while staying responsive to the needs and requests of the other partners.”

Since its inception, RED DART has fueled joint production and operational opportunities within the constraints of Department of Defense and Department of Justice regulations and policies. The concept includes the use of joint collections, joint reporting, and joint operations. De-confliction of prospective operations and collections is accomplished nearly real-time under the RED DART program because a majority of the information is collected jointly.

“‘Collaboration and team work’ is not just a catchphrase with RED DART,” said Luis Velasco, FBI Special Agent in the Charlotte, N.C., field office. “Indeed, it has allowed us to collectively pool our knowledge, resources and skills. In an era where we are asked to do more with less, RED DART has provided the perfect platform for us to execute our respective missions.”

The backbone of the RED DART program is an aggressive and focused CI awareness and education briefing program aimed at cleared contractors in North and South Carolina. The briefing program focuses on bringing real-time, specific, and relevant CI information to those in industry so they can better protect themselves and their intellectual property.

“The days of the ‘canned’ CI awareness briefing are gone,” said Brody. “RED DART’s briefing success is based on the concept of providing targeted, relevant briefings to the customer.”

The program serves as a force multiplier for the partner agencies. In just a short time, RED DART partner agencies have seen firsthand the resources made available by pooling assets instead of trying to accomplish operational activities unilaterally. RED DART has resulted in:

- Increased reporting from cleared contractors
- Increased Intelligence Information Reports
- Increased operations and investigations
- Operational focus on cyber issues

Brody attributes RED DART to the opening of 10 law enforcement investigations based on her referrals. More than 50 joint Intelligence Information Reports have been published by RED DART participants.

“In the current economic atmosphere, it makes sense that Federal agencies with common missions act in a joint fashion,” said Underwood. “Keep in mind, this program was not mandated from the management level. This program was conceived and implemented at the field level because a group of special agents felt like there was a better way to do business.”

Because of the success of the RED DART program, the concept is spreading. It was the catalyst for the creation of the Virginia Technology Task Force in the Charlottesville-Roanoke-Norfolk, Va., area.

Brody and two of her RED DART partners briefed the program to Sims and field counterintelligence specialists during last year’s DSS Capital and Southern Region all hands



Manning the RED DART booth at the North Carolina Defense and Economic Development Trade Show in Fayetteville, N.C., on August 7, 2012, are (from left) Brent Underwood, Naval Criminal Intelligence Service; Michelle Brody, DSS; Lou Velasco, FBI; and William Raybourn, Army Criminal Investigation Command.

training workshop. “The program is potentially replicable, especially for locations with one-man CI shops,” she said. “The keys to success are providing up-to-date information to our customers and breaking down institutional barriers. This is not a DSS or USAF or FBI problem — it’s a U.S. Government problem.” Currently, she is working with other DSS CI regions to assist them with starting similar programs.

“The RED DART program is a perfect platform for me as the strategic partnership coordinator, but more importantly it has bound the Intelligence Community in ways I never thought possible,” said Velasco. “This success story is due in no small part to Michelle’s tenacity and enthusiasm for her job at DSS.”

The concept of RED DART is directly in line with the objectives set forth in the Office of the National Counterintelligence Executive’s (ONCIX) 2012 Counterintelligence Strategy.

In the strategy document, ONCIX outlined three enabling objectives for CI entities:

- Engage partners to expand understanding and awareness of intelligence threats;
- Ensure responsible and secure information sharing and collaboration, and;
- Make efficient and effective use of resources.

PARTNERSHIP WITH INDUSTRY

EXCHANGE PROGRAM

By Darnell Carlisle
NISP Team Action Officer

The Partnership with Industry (PWI) Exchange Program was launched in 2009 to provide an opportunity for cleared industry and DSS industrial security professionals to “walk a mile” in each other’s shoes.

The goal of the program is for participants to gain a deeper understanding of their counterparts’ roles in industrial security, and to develop a better understanding and appreciation for the challenges and obstacles faced by government and industry security professionals.

The first “pilot” PWI exchange took place between Lockheed Martin Corporation and DSS in November 2009. Since then, the program has grown in popularity and size to include 16 industry partners. DSS has conducted exchanges on a quarterly basis, totaling 18 exchanges involving over 78 Industrial Security Professionals from Industry and DSS.

Participating industry professionals spend three to four days at a DSS site, normally a field or regional office. They work closely with DSS employees to gain a deeper understanding of how DSS operates within the scope of its mission, upcoming initiatives, and the challenges faced by DSS in its oversight of the National Industrial Security Program.

DSS personnel participating in the program gain exposure to issues faced by industry and witness first-hand how

security is integrated into a facility’s day-to-day mission, how resources are allocated, and how industry security professionals balance internal business requirements with requirements from DSS and its government customers.

In order to accommodate the increasing interest, DSS is planning to host 13 exchanges per region in fiscal year 2013, for a maximum of 36 exchanges. Additionally, DSS will offer the option of a “one way” exchange for small, non-complex facilities, where DSS will simply host an industry professional. This will allow facility security officers of small facilities to also benefit from the program.

Feedback on the PWI program has been consistently positive, with participants stating they never knew how much work goes into developing and integrating security into a company’s culture.

Industry participants have commented on how they were not aware of the size and scope of an industrial security representative’s workload. Participants from both sides have indicated that they learned a lot and were taking new ideas and new perspectives back to their work places.

This program and the combined efforts of DSS and industry work to form a partnership to protect classified material, information, and technologies while maintaining a competitive edge for our warfighters.



BENEFITS OF THE PROGRAM:

Industry: Provides an opportunity for industry employees to understand the perspective, mission, and roles of government employees charged with industrial security oversight.

DSS: Provides an opportunity to gain an understanding and exposure to contractor business operations and a variety of information systems. This exposure will assist the DSS industrial security representative and information system security professionals in understanding how industry operates from an Industry perspective.

HOW TO JOIN THE PROGRAM:

For questions or comments regarding the PWI program, please contact DSS Industrial Security Field Operations (ISFO) at PWI@dss.mil.

HELPFUL HINTS

ISFD AND SAFEGUARDING

By James Perham

Industrial Policy and Programs

DSS issues facility clearances (FCLs) on behalf of the Secretary of Defense as the Executive Agent of the National Industrial Security Program. In addition to issuing FCLs, DSS issues safeguarding approval at the level required for a facility to retain classified information in performance of a contract when DSS is the cognizant security office (CSO) for the contract. Both the FCL and approved safeguarding level are recorded in the Industrial Security Facilities Database (ISFD), an unclassified database managed by DSS.

A classified contract that contains or supports sensitive compartmented information (SCI) or carved-out Special Access Program (SAP) information requires the facility to hold an FCL at the classification level (Top Secret/Secret/Confidential) equal to or higher than what is required for contract performance. In this case, DSS still issues the FCL.

However, DSS does not issue safeguarding approval for SCI or carved-out SAP contracts because DSS is not the CSO for those types of contracts. The appropriate CSO issues safeguarding approval by accrediting a SCI or SAP facility. This safeguarding is not captured in the ISFD; it is captured in databases managed by the appropriate CSO (usually not at the unclassified level).

This can cause confusion when government organizations or prime contractors attempt to determine the level of classified information a facility has been approved to safeguard by an authorized CSO. If ISFD is the only source used to determine safeguarding level of a facility, it will not indicate safeguarding approved by other CSOs.

For example, a facility can possess a Top Secret FCL (issued by DSS), which is recorded in ISFD. The facility is performing on a Top Secret carved-out SAP contract (DSS is not the CSO) and has been issued Top Secret SAP safeguarding approval by the SAP CSO. That safeguarding determination is recorded in the carved-out SAP CSO's industrial security database, not ISFD.

The facility is also performing on a Secret level classified contract (DSS is the CSO) and has been issued Secret safeguarding by DSS, which is captured in ISFD. ISFD would indicate a facility with a Top Secret FCL with Secret safeguarding. The SAP CSO database would indicate a Top Secret FCL with Top Secret SAP safeguarding.

All CSOs and industrial partners should take an active role in resolving miscommunications concerning safeguarding.

THE THUMB DRIVE SMASHER

In May 2011, a cleared contractor employee assigned to a forward-deployed location received a classified document from the government customer. Using an unclassified scanner, he scanned the document to an unclassified thumb drive, then uploaded the document to an unclassified laptop computer.

The employee subsequently destroyed the thumb drive by smashing it with a hammer, after being told by the on-site facility security officer (FSO) this was not an authorized means of destruction and not to destroy the thumb drive in that manner.

The company entered an incident report in the Joint Personnel Adjudication System (JPAS) in June 2011, and the employee was permitted to remain in place, with the understanding that any disciplinary action would be taken when he returned to the United States in January 2012.

DETAILS

The government customer at the deployed location deemed this incident to be a security infraction and not a serious security violation.

A security infraction is a failure to comply with requirements which cannot reasonably be expected to, and does not result in the loss, suspected compromise, or compromise of classified information. A security incident indicates knowing and willful negligence for security regulations, and that results in, or could be expected to result in the loss or compromise of classified information.

- *A security violation resulting in the possible loss or compromise of classified information was not the focus of this incident.*
- *The government customer stated the employee's presence was essential and, to avoid adversely*

affecting the mission, requested any suspension not be served until the employee returned to the United States.

- *The employee served a five-day suspension in January 2012 after returning to the United States. The suspension was for the unauthorized method used to destroy the thumb drive and for disregarding employer instructions regarding the destruction of the thumb drive. The employee also received a letter of reprimand, refresher security training, and the facility suspended his access to classified information.*
- *Based on information received by DSS, the government customer and the cleared company did not address the potential loss or compromise issue.*
- *Due to the length of time between the incident and the notification, it is unknown if clean-up actions were taken.*

Following notification by the government customer, after they conducted an administrative inquiry, the Defense Industrial Security Clearance Office entered a loss of jurisdiction on the contractor employee's JPAS record and is processing him for interim suspension of his personnel security clearance. The Office of Personnel Management will conduct a reimbursable suitability investigation.

LESSON LEARNED

Had this security violation been reported immediately, the cognizant security agency could have assisted with procedures for sanitizing the affected information technology systems.

Since the facility entered an incident report in JPAS a month after the incident, DSS could have acted sooner



and prior to receipt of the administrative inquiry (six months later). This may have facilitated getting answers to the many unanswered questions this situation presents:

- *Why did the employee scan a classified document onto an unclassified system?*
- *Who determined the employee should not undergo any disciplinary action until he returned from deployment?*
- *Why did the government customer consider this situation to be a security incident rather than a security violation?*
- *Why did the disciplinary action center on the method the employee used to destroy the thumb drive with no apparent concern for the data spill?*
- *Was the data spill properly cleaned up?*

THE EMPLOYEE DESTROYED THE THUMB DRIVE BY SMASHING IT WITH A HAMMER AFTER BEING TOLD BY THE ON-SITE FACILITY SECURITY OFFICER THIS WAS NOT AN AUTHORIZED MEANS OF DESTRUCTION.

>> THEY SERVE

DSS RESERVISTS, GUARDSMEN JUGGLE SERVICE AND DUTIES

By Beth Alber
Public Affairs Office

The choice to serve in the military wasn't always an option. Mandatory service, or conscription, has been enforced several times, usually during war, but the United States discontinued the draft in 1973, moving to an all-volunteer military force.

As any military veteran will tell you, serving often involves sacrifice. Whether it is being on duty 24/7; the challenging missions that can't be discussed at home; or deploying away from family — the sacrifices are there. Yet, they serve. Approximately 60 percent of the DSS work force has served in the military, whether for a few years or for more than 20. These people proudly wear the title "veteran."

But there's a dedicated group of DSS employees who still serve; they juggle the responsibilities of their DSS duties and carve out time to fulfill their service in the National Guard or Reserve. They have deployed to support contingencies from South America to Southwest Asia, and have been a part of missions that had far-reaching effects.

Jim Chituras, industrial security specialist in the San Antonio Field Office, has deployed twice to Afghanistan, most recently from July 2011 to May 2012. As a colonel in the U.S. Army Reserve, Chituras served as the plans chief at Kandahar Airfield, where he was involved in the development and coordination of the immediate and mid-range plan for re-sizing the logistical support footprint and redeployment/redistribution of United States equipment to meet the 2014 force drawdown initiative for Afghanistan.

Jake Palmer, field counterintelligence specialist in the St. Louis Field Office, has deployed throughout Central and South America, most recently to Colombia in 2007. As a chief warrant officer 2 in the U.S. Army National Guard, Palmer helped track the location

FROM TOP: Sharon Dondlinger plays with local girls while deployed as an while deployed to Joint Base Balad, Iraq, in 2011. Jim Chituras sends home on an outbrief from a recent network security audit while deployed as an



of some captive government contractors, and gathered information that led to the capture of a drug cartel boss.

Sharon Dondlinger, Chief of the Alexandria Field Office, was deployed to Iraq in 2005, where she assisted the U.S. Marshal Service in providing security support during the trial of Saddam Hussein and assisted with security for the first free elections and the seating of the Iraqi parliament. Dondlinger, a major in the U.S. Air Force Reserve, was assigned to the 732nd Expeditionary Security Forces Squadron and served as the operations officer for the Law and Order Detachment in the International Zone. She assisted with the training of local Iraqi police and conducted numerous good order and discipline inspections of U.S. facilities.

Although military service takes employees away from their office, many are able to transfer their military experience to their jobs and duties at DSS. Quite often, mandatory military training directly relates to their DSS roles and expands their capabilities.

Conrad Bovell, chief of computer network defense in the Office of the Chief Information Officer (OCIO), deployed to Iraq from June 2010 to May 2011 in support of the U.S. Central Command. As a chief warrant officer 2 in the U.S. Army Reserve, Bovell served as a member of the Regional Computer Emergency Response Team Southwest Asia, Computer Defense Assistance Program Team, where he conducted network security audits at many forward operating bases throughout the country.

"Prior to my deployment, I worked on the operations side of OCIO. Working in an information assurance role while in Iraq, I got to see a depth and breadth of security issues the likes of which are rare for the majority of information assurance professionals," Bovell said. "I gained 10 years' worth of experience while deployed, and that experience has served me well as the Chief of CND, where a calm head, technical savvy and operational know-how come into play."

Max Shier, an information systems security professional (ISSP) in the Colorado Springs Field Office, was a security policeman when he transitioned into the U.S. Air Force Reserve, after serving 10 years on active duty. Recently, the technical sergeant cross-trained into a new career field, computer security, which directly relates to his duties as an ISSP.

"My recent training has more directly contributed to my duties with DSS," Shier said. "Specifically, it has helped me

with the new SIPRNet mission, and in conducting training for industry information systems security managers to comply with the more stringent requirements levied by CYBERCOM (U.S. Cyber Command) and DISA (Defense Information Systems Agency)."

While the work is rewarding, juggling DSS duties while fulfilling military responsibilities can be challenging. Serving in the National Guard or Reserve requires a commitment of one weekend a month, two weeks per year, and depending on the job, possibly a deployment. However, most DSS employees have found a way to make it work and are proud to serve.

When serving as an intelligence officer at RAF Molesworth, United Kingdom, James Moran, an industrial security representative in the Detroit Field Office, "effectively prioritizes requirements, offers solutions, and aggressively tackles all projects through completion." With 13 years of service, the lieutenant in the U.S. Navy Reserve and a Special Forces intelligence officer who was wounded in action, notes the key to his success is "a positive attitude and diehard persistence in juggling civilian, military and family obligations."

Palmer describes it as a "constant battle. Fortunately my unit allows me to drill locally to fulfill my requirements," he said. "And the military requirement to remain physically fit is easier now that we (DSS employees) are allowed some admin time to work out. That has saved me time and improved my quality of life."

Juggling DSS duties, Reserve duties and family "has been particularly tough this year," Dondlinger said, noting her Reserve unit is readying for a major inspection and her field office is short staffed. "But I serve because of the airmen. I know that when I take them downrange, that I will do everything possible to ensure their safety while they protect national interests. I do it for the airmen to my right and to my left."

Shier, who deployed to Joint Base Balad in Iraq in 2011, said it is a challenge to juggle his duties, specifically over the past couple of years, after he was activated and deployed to Iraq.

"Both workplaces have been receptive to accommodating each other and I have had no issues," Shier said, noting that the majority of his DSS office co-workers are military veterans. "Ultimately though, I consider it an honor to serve in both capacities.

ANNUAL TRAINING TOUTS VALUE OF CYBER PREPAREDNESS

By Selena Hutchinson

Office of the Designated Approving Authority, Field Operations

Cyber security and cyber preparedness were front and center in the annual training held for information systems security professionals (ISSPs) from July 30 through Aug. 3, 2012 at Quantico, Va. DSS senior leaders shared their ideas with the ISSPs, and attendees also benefited from technical presentations provided by nationally recognized academic and corporate information security leaders.

In his opening remarks, Stan Sims, DSS Director, quoted Army General Keith Alexander, Commander, U.S. Cyber Command who said, "The United States is not adequately prepared for a serious cyber-attack as the country is a 'three' on a scale of one to 10 when it comes to preparedness..." adding, "...defending the nation from a cyber-attack is complicated as it's

not just a question of preparing the Department of Defense or federal networks, but private industry as well." Alexander's remarks were delivered at the Aspen Institute's annual security forum in Aspen, Colo.

DSS plays an important role in countering these threats and maybe the most important partner in this effort due to our access and oversight of cleared industry. Sims added that technical training, such as this course, is the key to closing the gap.

In order to have a fighting chance against cyber-attacks, industry needs to know quickly when technology is threatened and respond just as quickly to attacks. Both industry and DSS require a qualified workforce to facilitate these notifications to industry, Sims said. He added that one of the things that keeps him up at night is the concern that ISSPs are leaving DSS for positions in private industry. Sims emphasized that he understands what the agency is asking of the ISSPs

Q&A: Stan Sims, DSS Director, left, answers a question from Tim Weaver, Western Region Designated Approving Authority.



in terms of workload and technical knowledge, but he encouraged them to stay with DSS and highlighted initiatives that explore retention incentives.

In closing, Sims noted that ISSPs are being pulled in many directions and because of this, "I have made the hiring of ISSPs one of the top priorities for the agency. We need you out front, advising industry on how to develop and maintain a resilient cyber environment, and promoting cyber security knowledge and training."

Richard Lawhorn, Director, Industrial Security Facility Operations (ISFO), followed and stated that ISFO's biggest challenge is balancing new, emerging threats such as cyber notifications on unclassified systems, insider threat, Command Cyber Readiness Inspections (CCRI) and expansion of the Defense Industrial Base, without negatively impacting our mission of ensuring the protection of classified information. "We are receiving great feedback on what we currently do from our government partners AND our industry partners," Lawhorn said. "This confirms that we are doing a good job overseeing the protection of classified information in the hands of industry. We are not perfect, but we are much improved," he said.

Lawhorn directly addressed the new cyber notification process and said, "We appreciate your patience and willingness to step up as we work our way through this. We recognize that you're being pulled in many directions and we are developing cyber response strategy on the fly. Our goal is to notify, ensure companies have a plan to fix, and provide assistance as we can." While there are still details to be worked out, Lawhorn emphasized that the notifications were a high priority.

The SANS Institute provided technical presentations from two leading cyber security experts. Marcus Sachs presented "Deadliest Hack: Eye of the Storm." This "straight from the battlefield" presentation provided case studies that describe in detail the most recent computer security incidents that his team has responded to. The anonymous in-depth case studies covered the recent complex hacks against commercial and financial organizations.

The talk showed how the intruders are gaining access, what they are doing, and resulted in a discussion of the malware used in the attacks.

His second presentation "What if I Were Evil," discussed what would happen if a "good guy" penetration tester woke up and decided to be evil. What are the targets and tactics he would use to break into your organization? What defenses would work in keeping him out or prevent the malware attacker from doing great harm? This presentation looked at the cutting-edge attacks used to bypass traditional defense technologies deployed in most organizations today. The talk demonstrated how anyone can create a piece of undetectable malware in 10 minutes with the same degree of difficulty as ordering a book online.

The highlight of the training was on practical, efficient UNIX auditing (with scripts). James Tarala, a senior instructor with the SANS Institute, provided a practical, step-by-step approach to auditing UNIX operating systems. Not only did students receive a better understanding of the audit process for these technical controls, but they walked out of the presentation with access to a few audit script ideas to assist them in their certification and accreditation efforts.

Other training sessions included a return presentation by Marty Lindner, who teaches internet security at the Carnegie Mellon University Heinz School, and a panel of industry information security experts. The industry panel used various pictures of DoD-related technical projects as a spring board to discuss certification and accreditation issues from their vantage point. The panel asked the ISSPs, "what do you see when you look at these pictures?" The ensuing discussion proved educational to both industry and government representatives.

This year for the first time, the training featured a regional breakout session where items of discussion included the need for consistent implementation of guidance, preparations for a successful CCRI, and training/individual development plans. Randy Riley, the Designated Approving Authority, intends to make these sessions a permanent item on the annual meeting agenda.

NORTHERN REGION TRAINS SUPERVISORS



GROUP PHOTO OP: Participants in the Northern Region supervisors' off-site pose by the Minute Man statue in Minute Man National Park, Concord, Mass. **A PIECE OF HISTORY:** Old North Bridge in Concord.

The Northern Region held a supervisors' off-site in Andover, Mass., Aug. 14 to 16. This training event provided an opportunity for the leadership team to discuss operational and managerial challenges, share best practices, and enhance team building.

The Human Capital Management and Equal Employment Opportunity Offices (EEO) supported the event and provided presentations on the hiring process, employee relations, Defense Civilian Intelligence Personnel System, and EEO responsibilities.

The team travelled to Concord, Mass., to explore a number of battle sites of the April 19, 1775, Battle of Lexington and Concord. They also discussed the roles and actions of various leaders when the American militia began the long war for independence.

The visit modeled the Staff Rides conducted by the Army to train soldiers to understand higher level decision-making, military tactics and leadership as well provide a historical view of training.

The Staff Ride originated in the mid 19th century with the German general and theorist Helmuth von Moltke the Elder, who saw it as a way to train general staff officers on key military and strategic concepts. Since the Army's first staff ride to Civil War battlefield of Chickamauga in 1906, the concept has been adopted by other government activities, notably the U.S. Forest Service, as well as private companies.

The leadership team walked in the footsteps (and hoof prints) of Paul Revere, William Dawes, and John Parker. They crossed the North Bridge in Concord where militia commander Colonel Barrett finally stopped the British advance through Concord and began pushing the Regulars back toward Boston. They walked along the Bay Road between Concord and Lexington where a bloody running battle was fought by local militia against retreating British Regulars.

The training helped the leadership team come away from this off-site better equipped to lead their offices, and with a much better understanding and appreciation of one of the most important days in our nation's history.

WHO'S WHO
IN THE NISP?

GISWG?

By Keith Minard

Industrial Policy and Programs

Deciphering the acronyms associated with the National Industrial Security Program (NISP) can be a challenge. To help understand the acronyms, as well as the various working groups associated with the NISP, this is the first in a series of articles on “who’s who in the NISP.”

In this edition, we introduce the Government Industrial Security Working Group or GISWG. The GISWG is a government working group comprised of representatives from the Department of Defense and 24 other Federal departments that meets to discuss updates and issues in policy implementation as it relates to industrial security and is chaired by DSS.

During FY12 the GISWG met four times to address and discuss key issues to include the use of the Army’s Enterprise 254 Contract System for preparing the DD Form 254, Certification and Accreditation of Information Systems overview, DSS’s role in conducting Command Cyber Readiness Inspections for contractors with access to Secure Internet Protocol or SIPRNET, and a discussion of best practices to streamline National Interest Determinations.

One of the major accomplishments of the group was the proposal for a joint effort between the Army and DSS to build an automated DD Form 254 database. The partnership includes reviewing the Army’s Contractor Automated Verification System (CAVS), which currently supports the Army’s Sensitive Compartmented Information contracts as a solution for the management of DD Form 254s for all classified contracts.

This joint effort will create an enterprise database to meet the needs of DSS, Government Contracting Activities, and Facility Security Officers to manage and track classified contracts more effectively and efficiently. The FY13 plan for the system’s development includes leveraging the existing system and its capabilities, gathering information for development of requirements, identifying system interfaces, and budgeting and funding the contract for development.

FACILITY CLEARANCE BRANCH EMBRACES CHANGE

By Sarah Beauregard

Facility Clearance Branch, Field Operations

The relocation of the DSS Facility Clearance Branch (FCB) from Columbus, Ohio, to DSS Headquarters in Quantico, Va., as part of the Base Realignment and Closure, resulted in a tremendous turnover of staff and the loss of a wealth of knowledge and experience.

However, as Martin Luther King proclaimed, “The ultimate measure of a man is not where he stands in moments of comfort but where he stands at times of challenge and controversy.” The FCB took advantage of the opportunity to create more efficient processes, enhance the collection of metrics, and strengthen its relationships with industry and government contracting activities (GCAs).

As part of this process, the branch analyzed the metrics pertaining to new facility clearance (FCL) sponsorships, specifically the percentage of sponsorships rejected, as well as the most common reasons for rejections. Analysis showed a lack of understanding of the information and materials FCB requires to initiate a new facility clearance. In an effort to add transparency to the FCL process and enhance communication between DSS and the GCAs, the branch created a pamphlet highlighting various aspects of the sponsorship process.

The pamphlet covers who can sponsor a facility for an FCL; what needs to be submitted for a complete sponsorship package; the most common reasons packages are rejected; and most importantly, how to contact FCB. In addition, FCB offers its support through teleconferences and/or briefings.

Since the August release of the pamphlet, the branch has been overwhelmed with positive feedback. The pamphlet not only provides guidance, but provides an avenue of communication between GCAs and DSS, through which DSS can share requirements and guidance. The pamphlet will be available on the DSS website, as well as the Resources and Job Aids webpage of the Center for Development of Security Excellence.

30 YEARS OF SERVICE

RICHARD RETIRES FROM MILITARY

Dana G. Richard, DSS Counterintelligence Directorate, retired from military service on July 1, 2012, after serving 30 years on active duty and in the Air Force Reserve.

Richard, who retired as a colonel, graduated from the U.S. Air Force Academy in June 1982, with a Bachelor of Science degree in International Affairs, specializing in National Security Policy.

After completing technical training as an Air Intelligence Officer, he was assigned to the 388th Tactical Fighter Wing, Hill Air Force Base, Utah, and later to the Headquarters Tactical Air Command (predecessor to Air Combat Command) Intelligence Staff at the height of the Cold War.

During this time he was awarded special experience identifiers for major command level readiness and operational evasion and escape and was one of the Air Force's first electronic combat intelligence officers.

In 1989, Richard resigned from the regular Air Force and accepted a Reserve commission. As a Reservist, he served with six combatant commands, with his last assignment as the Individual Mobilization Augmentee (IMA) to the Headquarters Air Force/Intelligence, Surveillance and Reconnaissance (ISR), Chief of ISR Forces and the senior HAF/A2 IMA.

Richard's military training includes Air Command and Staff College, the Joint Military Intelligence College and Air War College program.

He was mobilized for Operation Desert Storm, serving with Central Air Forces deployed, and Operation Noble Eagle, serving with the U.S. Space Command and U.S. Northern Command Counterintelligence staff offices, and served multiple volunteer active duty tours supporting active duty activities and operations.



NEWS IN BRIEF

DSS TEAM RECOGNIZED FOR SUPPORT TO

The Recruitment Team of the DSS Human Capital Manager received the 2012 National Intelligence Professional Awards ceremony for their contribution to the Intelligence Community Wounded Warrior program, a recognition within the intelligence community as a leader in providing professional experiences, marketable skill-sets, and sound security credentials to military veterans and interns with employment opportunities.

The working group, in which DSS participates, received the award, which is presented to a group of human capital professionals for their contribution to the highest caliber team effort, exceptional human capital management of a major program, and demonstration of a significant achievement in the mission of the human capital intelligence community.

The award specifically recognized the working group for its leadership, recruitment, placement, and support of the Wounded Warrior programs. Each award symbolizes collaboration in addressing human capital issues.

CDSE CYBERSECURITY AWARENESS COURSE WINS INTERNATIONAL RECOGNITION



The Cybersecurity Awareness course (CI 130.16) is the latest Center for Development of Security Excellence (CDSE) course to be recognized by the international training media community. The course received Bronze Omni Awards in the categories of Government and Education products. The Omni Inter-media Award recognizes outstanding television, video, film, internet, interactive, audio and animation productions.

CDSE developed the course in response to the relentless and pervasive cyber threats to our nation's networks and secrets. The 30-minute e-learning training provides a basic awareness and countermeasures for both Department of Defense and industry to help counter the cyber threat.

The training discusses the cyber threats and methods used to collect information from systems used by the government or defense contractors, the ability to recognize the cyber-attacks as collection attempts, viable countermeasures, and requirements to report these suspicious cyber intrusions to the appropriate security office.

The course was launched in October 2011 and has seen over 1,500 course completions in its first six months. The Cybersecurity Awareness course is available through the CDSE training site: <http://www.dss.mil/seta/enrol/stepp.html> (requires STEPP registration); or directly at <http://cdsetrain.dtic.mil/cybersecurity/> (no STEPP requirement).

F

WOUNDED WARRIORS

ment Office was recognized for its
ior Program Working Group at the
or Human Capital. DSS has gained
n providing meaningful internship
tials that support Wounded Warrior

Human Capital Outstanding Team
sionals whose contributions exhibit
support to the advancement of a
ment and/or the significance of the

ts superior execution in outreach,
ch team member received a lapel pin
s across the intelligence community.

"OPERATION EMPLOYMENT" CAREER FAIR

DSS participated in its first overseas recruitment effort at Ramstein Air Base, Germany, in July 2012. Antoe Allen, DSS Recruitment Manager; Tracy Brown, Office of the Designated Approving Authority; and Kirk Paulsen, Atlanta Field Office Chief, joined other Federal agencies at the "Operation Employment" career fair, jointly sponsored by the DoD Hiring Heroes Program and the Ramstein Airman and Family Readiness Center. This event attracted 208 transitioning service members, their dependents, wounded warriors and other veterans living overseas who will eventually relocate stateside.

The DSS Recruitment Team focused their efforts on showcasing DSS as an employer of choice by sharing information on the DSS mission, vision, and career opportunities--especially the opportunities available to Information System Security Professionals.

"I was very moved by the stories and circumstances that many of the attendees shared," said Paulsen. "They are true patriots in service of our great country, and I only wish everyone in DSS and other DoD agencies could experience first-hand what we did."

The DSS team was invited to attend a similar event slated for November in Kaiserslautern, Germany.

ELDP GROWS



FUTURE LEADERS

DSS GRADUATES TWO

In June 2012, two DSS employees graduated from the Department of Defense Executive Leadership Development Program (ELDP) with a better understanding of the roles and mission of the entire Department.

Ashley Bransome, Chief of Creative Services, Center for Development of Security Excellence, and Henry Yeh, Information Systems Security Professional in the Sunnyvale Field Office, were the first DSS employees to graduate from ELDP. They spent 10 intensive months in the program that develops future defense leaders. In total, 60 emerging leaders participated in this session, including civilians from all services, defense agencies and field activities, as well as active duty military personnel.

ELDP gives participants exposure to other DoD agencies to ensure future leaders have the tools and knowledge to lead in the dynamic DoD environment. The program includes monthly deployments to military facilities, combatant commands, forward-deployed locations, and other government organizations to provide an overview of the Department and help them better understand the challenges and

cultures of each of the services. Participants conduct research, write reports, and complete assignments, in addition to working their full-time jobs.

During monthly deployments, the ELDP participants experienced the military from a service member's perspective, participating in rigorous physical activities and often sharing the same meal. Through intense, hands-on field experience, participants dealt first-hand with the challenges others face in carrying out the mission of the Department.

The first step in the program was a two-week core curriculum course in October 2011. The class was divided into six teams, and participants quickly learned that personal goals were secondary to those of the team.

"They pushed us to our limits; there were a lot of tears, a lot of arguments, but also a lot of laughter," Bransome said. "Core allowed us to lay the foundation and develop the trust necessary to successfully work together as a team for the next 10 months of deployments and team exercises."

FEEL THE BURN: Ashley Bransome (right), along with other Executive Leadership Development Program participants, is tased as part of Exercise African Lion 2012, in Agadir, Morocco.

The deployments read like a travelogue and took the team around the world to experience different environments and cultures first hand. The first deployment for the team was to U.S. Forces-Korea, where the ELDP toured the Korean Demilitarized Zone.

“As we stood at the DMZ, we experienced the tension between the divided Koreas,” Yeh said. “After visiting South Korea, I saw how well our warfighters are trained and are prepared to fight anytime. From this perspective, the importance of how I help protect the secrets that give these soldiers an edge over their adversary seems obvious.”

In the U.S. Pacific Command, they visited USS Chung-Hoon, an Arleigh Burke-Class Aegis Destroyer that had just returned from a six-month deployment, and participated in a ceremony honoring the 70th anniversary of the attack on Pearl Harbor at the USS Arizona Memorial.

In San Diego, Calif., they took part in Basic Underwater Demolition/SEAL (BUD/S) training; diving in and out of the Pacific Ocean, doing push-ups and flutter kicks, and carrying the training log as a team. The importance of building effective teams was emphasized when the group navigated the Leader Reaction Course (LRC). Their ability to keep a cool head under pressure was thoroughly tested at the Aviation Survival Training Center, where they donned flight suits and egressed from a simulated aircraft under water in the training pool.

Yeh led a team of civilians and active duty officers through the LRC. “It was challenging because the desire to beat the best score made people eager,” Yeh said. “After explaining the goal, the team came together despite its differences. We worked together and completed several obstacles, beating all the other teams.”

The ELDP participated in exercise African Lion 2012, in Agadir, Morocco, during their deployment to the U.S. Africa Command area of operations. During hands-on training, several team members — including Bransome — volunteered to be shocked with a Taser gun by the 24th Marine Expeditionary Unit. In return,

the ELDP acted as rioters that had to be contained by Marine and Moroccan Armed Forces during a riot control exercise.

While at AFRICOM, Bransome was asked about her experience in ELDP and quoted in an article for the command website.

“I think the one-on-one time that we’ve been able to spend with the actual services has been amazing. Just to be able to sit and have lunch with them and talk. That’s really changed my views on a lot of things,” said Bransome, who added that she now sees the DoD budget cuts from a completely different perspective after witnessing first-hand how the cuts are affecting service members.

During their time with the Texas National Guard, the ELDP were strapped into a HUMVEE in preparation for a 360-degree vehicle roll over, and took part in Science, Technology, Engineering, Math program at the Texas sponsored STARBASE: a hands-on journey for fifth graders.

The participants of ELDP were taught about the Department, not just in a classroom, but by getting wet, sandy, and muddy. For those who never served in the military, ELDP took them out of their cubicles to the water, mud, red clay, sand, and steel decks so that they could make the connection between what they do and how it supports the warfighter.

“Throughout, we embraced the five tenants of ELDP: know yourself, express yourself, build teams, manage organizations and learn more about the DoD,” Bransome said.

“I learned that being a leader isn’t easy,” Yeh said. “I took the training to become a better leader and am committed to having the courage and compassion to do the right thing for this agency and the Department of Defense.”

Marc Brandness, Industrial Security Instructor for the Defense Security Service Academy, is enrolled in the current ELDP and recently departed for the core curriculum course.

“FROM THIS PERSPECTIVE, THE IMPORTANCE OF HOW I HELP PROTECT THE SECRETS THAT GIVE THESE SOLDIERS AN EDGE OVER THEIR ADVERSARY SEEMS OBVIOUS.”



GAINING PERSPECTIVE:

Henry Yeh rappels off a 72-foot jump tower at Fort Benning, Ga.

INSET: Yeh navigates the obstacle course at Kaneohe Marine Corps Base, Hawaii.





Enterprise Day
celebrates
40th anniversary
of DSS



To mark the 40th anniversary of the Defense Security Service, Stan Sims, DSS Director, declared Sept. 14 as “Enterprise Day.” The day was set aside to mark 40 years of service to the nation and to bring employees together for a day of rest and fun.

For the National Capital Region, it was a picnic at Castle Park on Fort Belvoir, complete with cakes, remarks by the director and posters highlighting agency milestones.

All DSS locations were encouraged to mark the occasion in some manner and almost all did with similar picnics or local get-togethers. The Virginia Beach Field Office took a different approach as employees went to lunch and then some went zip-lining.

FEDS FEED FAMILIES PROGRAM

DSS raised more than 2,904 pounds for the “Feds Feed Families” food drive, which was held June 1 through Aug. 31, 2012. This total exceeds the agency goal of two pounds per employee, and surpasses last year’s efforts.

“Feds Feed Families” is a voluntary effort undertaken by Federal employees to bring non-perishable food items to their offices for distribution to local food banks. The DSS team collected donations throughout the Washington, D.C. area, as well as at regional and field offices across the country.

Overseeing the National Capital Region campaign were Matthew Kroelinger (right) and Mario Medina, from the Office of the Chief Information Officer.

2,904

POUNDS OF FOOD COLLECTED
BY DSS FOR “FEDS FEED FAMILIES”





FAR LEFT: Stan Sims, DSS Director, listens to a safety briefing before touring the new Raytheon Redstone Missile Integration Facility on Redstone Arsenal, Huntsville, Ala.

LEFT: Angel Cresp (left), Plant Manager at Raytheon Redstone, explains how the new facility increases the ordnance integration capability to Director Sims.

NEW RAYTHEON FACILITY SHOWS BENEFIT OF PARTNERSHIP

In early August, Stan Sims, DSS Director, along with other members of the DSS leadership team toured the new Raytheon Redstone Missile Integration Facility (RRMIF) on Redstone Arsenal, Huntsville, Ala. The facility was built to handle predicted SM-3 and SM-6 missile production rates which will provide Raytheon Missile Systems (RMS) with three times the current ordnance integration capability.

The partnership between DSS and this new facility started during the design phase, prior to Raytheon breaking ground on the new facility. In October 2010, the Huntsville Field Office hosted a meeting to discuss early planning of facility security requirements, information system security requirements, and overall security best practices.

Since that initial meeting, DSS and Raytheon have been aligned in a partnership to ensure superior security measures were built into the facility. Mark Schoenig, Huntsville Field Office Chief, and the Industrial Security Representative assigned to the facility have visited the RRMIF on a continuous basis throughout the build phase. The Huntsville Field Office has also participated in key planning meetings with Raytheon personnel involved in the build, Red Stone Arsenal garrison security staff, Directorate of Public Works, and RSA Visitor Control.

Schoenig and Sara Ballard, Senior Industrial Security Representative, attended the groundbreaking ceremony held June 27, 2011, along with local, state, and military dignitaries from across Alabama. Completion of the facility

was projected for September 2012, with the ribbon cutting scheduled for Nov. 26. The facility will be approximately 70,000 square feet on approximately 200 acres, with additional area allocated should expansion be necessary.

The August facility tour was provided by various Raytheon team members. Randy Stevenson, Director of Raytheon's Weapon Integration Centers, conducted the first part of tour, which included the production floor, the control rooms, the test cells, and support areas.

Stevenson said, "We are building this facility based on approximately 10 years of research in advanced technologies and automation. The RRMIF will be different from all other missile factories with its use of automatic guided vehicles and robotics."

As the tour progressed, Plant Manager Angel Cresp described how each missile moves throughout the factory with the use of automatic guided vehicles that transport the missile down a concrete corridor into a test cell that uses a comprehensive, multi-layered system of protection from any potential explosion.

At the end of the tour, Sims expressed his appreciation for the tour and for the partnership between DSS and Raytheon from the facility's inception. Sims then presented Jim Collier with a certificate and a DSS coin thanking him for his 27 years of service as a facility security officer at Raytheon Warfighter Protection Center. Collier retired in August.

COLORADO SPRINGS FIELD OFFICE HELPS WOUNDED WARRIOR

Members of the Colorado Springs Field Office, alongside local Office of Personnel Management personnel, completed a volunteer project supporting a Wounded Warrior in Rocky Ford, Colo.

The team spent several long, hot days during March, April and June of 2012, converting a garage into living quarters for a disabled veteran who suffers from Post-Traumatic Stress Disorder.

The project involved removing the garage door, raising the floor, and enclosing the room by constructing a new outer wall and installing a window. In the end, the garage was transformed into a habitable room for sleeping. Materials to complete the renovation were donated by the community and local businesses.

The efforts of the Field Office got their beginning through the Colorado Federal Executive Board's Southern Colorado Council in which Field Office Chief Michael Stell is an active member. The Colorado Springs Field Office is proud to help members of the community. This project is a testament to their dedication to giving back, as well as outstanding teamwork.



NAILED IT: Volunteers from the Colorado Springs Field Office and local Office of Personnel Management put down new raised flooring while converting a garage into living quarters for a disabled veteran.



Call Center Tour

DSS senior leadership recently toured the DoD Security Services Call Center located in Lorton, Va. The Call Center is the DoD focal point for assisting customers with various industrial/personnel security-related systems/applications and inquiries regarding personnel or facility clearances.

The Call Center receives an average of 30,000 plus queries per month. It consistently maintains a call abandonment rate of less than 2% and a caller wait time (to reach an agent) of well under one minute.

DoD Security Services Center
10430 Furnace Road
Suite 101
Lorton, VA 22079



DEFENSE SECURITY SERVICE