DSS ACCESS

Volume 4, Issue 1 Official Magazine of the Defense Security Service

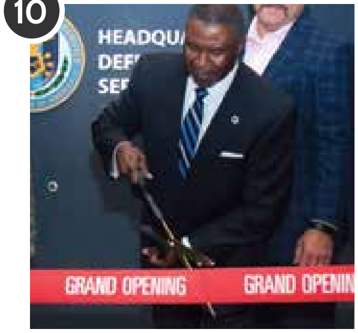
Pilot program seeks to streamline facility clearance process

Director Holds Annual Townhall | CDSE News | Classified Data Spills

SPRING 2015

Volume 4, Issue 1

10



22

26

SPOTLIGHT

INSIDE

CROSSING BORDERS

ASK THE LEADERSHIP

CASE STUDY

AROUND THE REGIONS

DSS ACCESS

Published by the
Defense Security
Service
Public Affairs Office

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

DSS Leadership

Director
Stanley L. Sims

Deputy Director
James J. Kren

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

Happy New Year! I know this is belated, but this is our first publication of 2015, so please indulge me. It has become my tradition while at DSS to host a town hall meeting for all DSS employees in early January to look back at the previous year and look ahead to the New Year. I find these sessions valuable to highlight accomplishments that were either forgotten, not well known or even some that may not have seemed significant at the time. But upon reflection, I find that an event or milestone has great significance and a tremendous effect on the agency.

I also try to chart the course for the agency for the year ahead, read the horizon and prepare the workforce for the challenges ahead. This year was no different, but in preparing for this town hall, I found myself returning more and more to the first such meeting we had shortly after my arrival at DSS. And in so doing, I was able to reflect on how much has changed in the past four years and how much remains the same.

DSS is a very different agency than it was in 2011; we have fundamentally changed how we approach our oversight mission by partnering with industry when we "inspected" them. We developed new processes and procedures to mitigate Foreign Ownership, Control or Influence. We initiated Information Technology Systems that will automate antiquated, manual processes. We outfitted our field offices to work securely in today's changing security environment. We launched a new education program and made certification for the security workforce commonplace.

While we did these things, and many, many others, we remained committed to the three priorities I established when I arrived:

People first, mission always

Partnership with industry

Tell the DSS story

We have other priorities, of course, but I realized when I came here that we needed a theme and I picked these because I believed they were central to DSS. They have not changed in four years and they will not change this year either. If you take care of your people, they will take care of the mission. Partnership with industry is the very essence of what we do. And only we can tell the DSS story; no one else understands our mission and our role better than we do. These priorities guide us and remain constant. I continue to believe that if we remain committed to them, DSS will continue to improve.

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

Pilot program seeks to streamline facility clearance process

Due to inconsistencies in the current facility clearance (FCL) process timetable, and in an effort to build in more accountability and streamline the FCL process, the DSS Facility Clearance Branch (FCB) recently conducted a pilot program using a modified FCL process that identified strict deadlines for each phase of the process.

by Beth Alber
Office of Public and Legislative Affairs

The pilot program, initially rolled out in March 2014 and expanded in July 2014 to include 10 DSS field offices, was designed to increase transparency among stakeholders and improve communication. The participating field offices were: Alexandria 3; Colorado Springs; Hanover 1 and 2; Irving; Melbourne; New York; Philadelphia; Phoenix; and Virginia Beach.

The National Industrial Security Program Operating Manual describes a facility clearance as "an administrative determination that a facility is eligible for access to classified information or award of a classified contract." The first step in clearing a company is for them to be sponsored for a facility clearance by either a government contracting activity (GCA) or other cleared company.

Once FCB receives and accepts the sponsorship letter, the communication starts flowing. The FCB provides the company facility security officer with the "FCL Orientation Handbook," which provides a roadmap to guide the company through the FCL process.

Concurrently, FCB notifies the sponsoring GCA/cleared company, as well as the industrial security representative that the sponsorship has been accepted and the FCL process is underway. This increased transparency in communication enhances the partnership with industry and the GCA, as it provides the necessary information to all involved parties before the FCL process begins.

Strict Deadlines

As outlined in the handbook, the company has strict deadlines it must meet to complete the FCL process. The first deadline placed on industry is to provide DSS with a complete package for the e-FCL online database within 20 days of receiving the FCL Orientation Handbook.

The second deadline is to provide personnel security clearance applications using the Electronic Questionnaire for Investigations Processing (e-QIP) website for its key management personnel within 45 days of receiving the FCL Orientation Handbook.

And finally, the third deadline is for the company to submit fingerprints within 14 days of submitting the e-QIP. If the company fails to meet any of the required deadlines, the process is discontinued and FCB notifies the sponsoring GCA/cleared company of the discontinuation and the reason for it.

"With the implementation of the new FCL process, there is increased communication and guidance resulting in increased comprehension and compliance," said Terri Panzel, FCB staff specialist. "The new FCL process is that handshake between us and our partners in industry. It is DSS extending a hand to our partners in industry and being greeted with the grasp."

Complex Structures

Some facility clearances are extremely complex based on the corporate structure of the company. One structure that has historically caused delays in processing is the excluded entity process. If a facility is a subsidiary of another corporation, then that "parent" corporation (and any other "grandparent" facilities) can be excluded from access to any classified information that will be made available at the cleared facility.

As part of the modified FCL process, a restructured excluded entity process was also rolled out to address inefficiencies in processing and a lack of compliance by excluded parents.

Previously, the DSS industrial security representatives would have the time-consuming job of visiting and interviewing each excluded "parent" to gather the information and determine whether foreign ownership, control or influence was present.

Under the new process, FCB is requiring any multi-tiered excluded entity legal structure to consolidate all required documentation to the highest cleared entity. Now the onus is on the company to provide the documentation on the business structure and include it in the highest cleared entity's e-FCL package, which will contain all required excluded parent information.

By the Numbers

Since implementation of the pilot program, the FCB has steered 341 facilities through the modified process, with some of the facilities having one or multiple excluded entities attached to them. Of the 341 facilities, 85 percent met the first deadline of providing an eFCL package in the time required.

Of the 341 companies, 91 percent met the second deadline and submitted e-QIP for key management personnel on time. All companies complied with the requirement to submit fingerprints within 14 days of submitting the e-QIP, which aligns with OPM standards.

With 10 of the 26 field offices involved in the pilot program, the processing time has decreased for the overall FCL process. Since July 2014, the FCL processing time has been cut by 23 percent using the modified process.

"The pilot program has been well received by the industrial security representatives (ISRs) and contributed greatly to streamlining the FCL process," said Joseph T. Cashin, Field Office Chief, Philadelphia Field Office. "Once all necessary documentation has been submitted in e-FCL, the orientation meeting has proved to be invaluable in allowing the ISR (Industrial Security Representative) adequate time to truly provide the facilities with advice and assistance directly related to their performance on classified contracts."

Based on the positive results obtained from the 341 pilot facilities going through the modified process, DSS plans to roll out full scale implementation of this program in April 2015.

Until that time, FCB is communicating with industry and DSS field offices to increase awareness of the modified process by offering educational webinars.

Director holds annual town hall meeting

Looks back at 2014, ahead to 2015

In keeping with an annual tradition established in January 2011, Stan Sims, DSS Director, held his annual "state of DSS" or town hall meeting for agency employees on Jan. 7, 2015.

And in keeping with a new tradition started in 2014, the agency leveraged its video-teleconference capability to connect all of the 50 remote field locations to one of the two sessions.

Sims noted that his first town hall was held exactly four years ago, shortly after he arrived at DSS. "At that meeting, I introduced myself to you," he said. "I talked about my philosophy and what I hoped to achieve together as an agency. Fast forward to 2015 and our conversation is going to be a little different. We know each other now and what to expect from each other. We know the good, the bad and the ugly about each other and this conversation will be different."

Sims also cited the changes within DSS since 2011. "We changed ourselves over the last four years, and I believe we changed for the better," Sims said. "We saw the changing security environment and we changed to meet that environment. Good organizations do that, they change themselves when change is needed; they see when they need to do things differently."

"Today we are central to both DoD and national security; we're at the epicenter of national security. We are more respected within the Department. We are more professional in how we engage with our customers and stakeholders," Sims continued. "We are more productive and we are good at what we do. We make a difference; collectively the work we do makes a difference and it is recognized." While much has changed at DSS, Sims said his three top priorities remain the same as they were in 2011:

People first, mission always | Partnership with industry | Tell the DSS story

> *We changed ourselves over the last four years, and I believe we changed for the better.*

In addressing "people first," Sims introduced the senior leadership team, many of whom were in place in 2011, as well as those who have joined DSS since then. He also noted the vacancies in a number of key senior leadership positions and said he planned to have the vacancies filled by the end of February.

He urged the workforce to embrace the leadership changes. "Don't be afraid of change or new leadership. New people bring in new ideas and fresh eyes," he said. "So embrace these changes and relish the thought of new ideas."

Sims noted that his tenure at DSS would likely end in 2015 but wanted to ensure the agency was on a strong path for the future. "The tenures at the director level are decided by seniors and it's dependent on a lot of things," said Sims. "I want to preserve continuity of operations and continuity of purpose. But it's not the individual, it's not me; the folks who make DSS what it is, it's you, all of you. Leadership does matter, but I know those things that will endure in DSS won't endure because of Stan Sims, they'll endure because of you. That's what you need to concentrate on."

Sims said multiple employees had asked him what he wanted his legacy at DSS to be. In response, he said two things stand out. The first is the culture change in partnering with industry and how DSS conducts its oversight mission. "We fundamentally changed how we deal with our partners and that is due in large part to the field workforce," said Sims. "You did a phenomenal job. I gave you a vision and you executed it."

Sims said the second was ensuring DSS was a respected, key player in national security. "We have changed our status in DoD and ultimately on the national security scene," he said. "So, when, if, I leave at the end of 2015, I want to have irreversible momentum; changes that will endure and live beyond my tenure, changes that must not matter whether I'm here or not."

Sims then addressed internal initiatives for the workforce such as the Director Award Program, the newly created Leadership Advisory Board and mentoring. In particular, Sims cited the need to identify emerging leaders within DSS and then educate, train, and develop them. His goal is to "produce caring, credible, accountable DSS leaders capable of motivating their employees and teams to be successful at achieving results that address the challenges of the national security environment."

"We need good leaders doing the right thing," explained Sims. "I want you [supervisors and managers] to identify your leadership pipeline. Who are you training to take your job? Who will come behind you? You should know who will do your job if you leave. You can tell your employees they are future leaders. You need to develop them and let them know how important they are."

Sims emphasized that everything he said about people was about mission. "Who executes the mission? People. If you're doing a good job, the mission will get better. Take care of the people; they will take care of the mission," he said.

Telling the DSS story is important because Sims said he found a lot of people in the community didn't know what DSS did or why what the agency does matters. "Now, there is a much greater understanding outside of DSS as to why we matter," he said.

In spite of progress, Sims acknowledged a continuing gap between the headquarters and field personnel. "I understand how it works," he said, "and it's something we always have to work on. We have to be better integrated internally. We have to tell the DSS story, but we also have to tell the same DSS story."

Sims closed by briefly discussing the agency's new insider threat program, and the DITMAC, the DoD Insider Threat Management Analysis Center. While Sims said he didn't know what the DITMAC would ultimately look like, standing up the new function would be the agency's biggest challenge for 2015.

"In closing, we have done a lot of things very well," said Sims, "and we will continue to do well. We are not slowing down this next year."

Multinational working group provides a forum

to discuss international industrial security issues

by Jason Heit
DSS International Division
Industrial Policy & Programs

In September 2014, I attended the 29th Annual Multinational Industrial Security Working Group (MISWG) Plenary, hosted by the Romanian Government in Bucharest, Romania. The MISWG Plenary was attended by 59 foreign delegates from 33 different countries, and also representing the United States was Mark Smith, International Security Programs, Office of the Under Secretary of Defense for Policy (OUSD(P)).

The DSS International Division attends the MISWG Plenary as its primary mission is to oversee and administer agency-level guidelines and international responsibilities regarding cleared U.S. industry's involvement with foreign governments, foreign contractors and NATO on behalf of the OUSD(P).

The MISWG was created in 1986 as an informal body to develop common security practices and procedures for the protection of classified information shared under non-NATO Multinational Defense Programs and international industrial security matters. It is comprised of NATO member nations (except Iceland), as well as Australia, Austria, Finland, Israel, Sweden and Switzerland.

The MISWG provides a forum to discuss ways to adapt security practices to continuing changes in the overall security environment, defense industry trends and international industrial security.

"Through the years, the MISWG's success owes much to the ad-hoc nature of its proceedings," said Smith, a long-time MISWG participant. "Many MISWG delegates have noted that by knowing their counterparts on a personal basis and by meeting them face-to-face, many problems that might otherwise have been impediments to cooperation have been solved, either in session or during other opportunities for engagement in the annual sessions.

"Removed from the confines of a more formal setting, the delegates are free to craft innovative ways to apply national law and policy, and address concerns raised by industry and government security representatives alike," Smith continued. "This is best witnessed in the smaller working-level sub-groups used to analyze and prepare recommendations on a particular issue. One only has to look at the increasing membership of the MISWG through the years as a measure of its success and utility."

Although 33 nations comprise the MISWG, other non-MISWG countries have asked to use MISWG procedures in their cooperative arms programs. As a result, 25 MISWG-published documents are now posted on the Internet for public use.

Informal Forum: The MISWG Plenary was attended by 59 foreign delegates from 33 different countries.

Most of the MISWG documents provide procedural guidance for implementing security requirements in international programs, while other MISWG documents are used in preparing the content of international agreements and contracts involving access to classified information.

For the Department of Defense, the documents may provide a baseline for negotiations on security provisions in these programs, and DSS may approve the use of these documents in individual classified commercial programs.

However, the U.S. Designated Security Authority must approve the coordination of all documents when they are required by an international agreement, such as when the documents are incorporated in a Program Security Instruction for international programs.

MISWG documents, practices and procedures are not legally binding. They do not constitute international agreements and are not intended to contradict or violate national laws, rules and regulations. Whenever practical, participating countries should apply MISWG documents in whole, or in part, to standardize security-related practices and procedures amongst participants in classified bilateral and multinational cooperative defense programs.

As the MISWG has no permanent structure, hosting of the Plenary each year is completed by a different MISWG-member nation. As agreed on in Romania, the host countries for upcoming MISWG Plenaries are Israel (2015), Sweden (2016) and Belgium (2017).

NSE SECURITY SERVICE
ES OF AMERICA
HEADQUA
DEF
SE
GRAND OPENING
GRAND OPENING
GRAND OP

With ribbon-cutting ceremony, DSS moves into new addition

by Dahlia Thomas
Office of Public and Legislative Affairs

The Defense Security Service officially opened its new headquarters at the Russell-Knox Building (RKB) in Quantico, Va., during a ribbon cutting ceremony on Nov. 13, 2014. The ceremony marked the completion of the military construction project and the opening of a permanent home for DSS.

The 40,000 square foot addition and 300-space garage will accommodate a larger DSS work force and allows the agency to consolidate its headquarters support elements in one place. Construction began on Aug. 1, 2013, with a ground breaking ceremony. After 14 months of disruptions, parking inconvenience and constant alarm testing, the project was completed on time and, at $32 million, under budget.

This significant milestone for DSS was 42 years in the making. From its inception as the Defense Investigative Service (forerunner to DSS), the agency was originally located in a leased facility at the Forrestal Building location. It then moved to Buzzard's Point in Southwest Washington, D.C., and later to Braddock Place in Alexandria, Va., where it remained until September 2011. As a part of the 2005 Base Realignment and Closure Commission recommendations, the agency was moved to the Russell-Knox Building where it was co-located with the Defense Investigative Agencies: Defense Intelligence Agency, Air Force Office of Special Investigations, Army Criminal Investigation Command and Naval Criminal Investigative Service.

"In each of those leased spaces, we shared the building with commercial tenants, which limited our ability to interact and didn't foster an inclusive work environment," explained DSS Director Stan Sims.

"Our move to Quantico was a great step forward, but the space was not adequate to accommodate the DSS workforce and we still had various support elements in leased space," he continued. "That's why this addition is so important. For the first time in its history, DSS has a headquarters in a government building with all elements collocated. For the first time, we have a headquarters that is truly ours."

A somber and memorable moment during the ceremony came as Sims recognized the display on the wall outside the command suite which honors the five DSS employees killed in the bombing of the Alfred P. Murrah Federal Building, Oklahoma City, Okla., on April 19, 1995: Special Agent in Charge Robert G. Westberry, Special Agents Harley Richard Cottingham, Peter L. Demaster, and Larry L. Turner, and Executive Secretary Norma "Jean" Johnson.

"It's fitting that we have this display at our new headquarters to honor their sacrifice, their families and to ensure DSS (we) never forgets," said Sims.

During the ceremony, Sims thanked the DSS project team, led by the Logistics Management Division and representatives from across the agency, for their commitment to the project. The team also included Fentress Architects and Hensel Phelps for their design and construction expertise. "I realize this addition was a small project to the design and construction teams, but hugely important to DSS," said Sims.

Sims also thanked the Naval Facilities Engineering Command team for their hard work in keeping the project on track and completing it on time and RKB fellow tenants and DSS employees for their patience in enduring the many inconveniences resulting from the construction.

In the photo, Stan Sims (center), DSS Director, cuts the ribbon at the ceremony. Looking on are from left: Navy Cmdr. Carl Kirar, Naval Facilities Washington; Marine Corps Col. David Maxwell, Commander, Marine Corps Base Quantico; Sims; William T. Thumm, Hensel Phelps Construction Co.; and Brian Chaffee, Fentress Architects. *(Photo by Hollie Rawl, DSS)*

A Q&A with Regina Johnson

Director, Southern Region

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

Regina Johnson, Director, Southern Region, assumed her current position in May 2012. As the regional director, Johnson is responsible for the industrial security oversight of approximately 3,200 National Industrial Security Program (NISP) facilities dispersed across a 14-state area, Puerto Rico, and the U.S. Virgin Islands. The region includes six field offices located in Irving and San Antonio, Texas, Huntsville, Ala., Atlanta, Ga., Virginia Beach, Va., and Melbourne, Fla.

Johnson began her federal career with the Internal Revenue Service and then moved to the Department of the Navy before joining the Office of Personnel Management as an investigator. In 1986, Johnson went to work for the Defense Investigative Service, now DSS, as a Special Agent conducting personnel security investigations.

In June 1989, Johnson was selected as an Industrial Security Specialist for DSS in the Houston Resident Office where she worked until 2008, when she was selected as the Field Office Chief for the Irving Field Office. The Irving Field Office covers all of North Texas, the states of Arkansas, Kansas and Oklahoma.

Tell us about the Southern Region, what makes it different from the other three regions?

The Southern Region covers 14 states, the Virgin Islands and Puerto Rico. We have six field offices and approximately 3,200 cleared facilities. The region is unique in several aspects; first, in geographic area. The region stretches from Texas to Kansas and east across the lower continental United States to Virginia Beach, Va., then south through Florida.

Due to the expansive territory, our employees travel extensively. This poses challenges at times, as some of our facilities and Resident Offices are in remote locations.

We've tried to address this by having the Field Office Chief and Region staff visit each Resident Office on a recurring basis. On those visits, the Field Office Chief will participate in local industrial security events, for example, NCMS meetings or JSACS/ISACS [Joint or Industrial Security Advisory Committees], to develop and maintain the partnership with the security community in those areas.

Another unique aspect is the variety of facilities in the region. We serve a full spectrum of contractors, from large shipbuilding facilities in Virginia and the Gulf Coast, to small parts facilities in Arkansas and Kansas, as well as a large number of facilities under Foreign Ownership, Control or Influence (FOCI).

In Alabama, the Huntsville Field Office has experienced a tremendous increase in workload due to the high concentration of facilities and Government Contracting Activities, some of which moved there under Base Realignment and Closure. The Huntsville Office has the largest number of complex facilities under the NISP, and we've had to supplement the office with TDY support to accommodate their needs.

We also have a large number of Indian Nation cleared facilities. They are all located in Oklahoma, and while they are treated like any other cleared facility under the NISP, they have unique organizational structures, as they are considered sovereign nations.

What are the unique challenges in the region?

Our most unique challenge is the number of Arms, Ammunition and Explosives (AA&E) facilities in the region. The Southern Region has the second greatest number of AA&E facilities in DSS, and most are located in remote parts of the southwest, away from large urban populations. Most of the AA&E facilities in the region are uncleared, while several others have both NISP and AA&E programs, thus posing a challenge for both contractor and DSS security professionals.

AA&E inspections primarily focus on physical security aspects of a facility such as storage structures, locks, key control, intrusion detection, and guards; however, there's quite a bit of confusion throughout industry since contractors also have to deal with security requirements levied by the Bureau of Alcohol, Tobacco and Firearms. Needless to say, working with these facilities takes quite a bit of patience and collaboration to be successful.

Because many of the AA&E facilities in the region actually produce deadly AA&E items, safety of our field personnel is always a top priority. We made a concerted effort at the end of fiscal year 2014 to ensure all Industrial Security Representatives inspecting AA&E facilities were authorized to purchase appropriate safety clothing, such as non-conducting, steel toed boots. We also ensure these personnel understand our traditional 'suit and tie' attire may not be appropriate, or safe, when visiting an AA&E facility since they may be working in and around dirty, dusty bunkers, and in areas where entry may be restricted if a certain percentage of the individual's clothing composition is not cotton. Safety first!

The Southern Region's AA&E coordinator is Senior Action Officer Brian Murphy, and he has been working with Field Operations Headquarters over the past year to not only enhance the AA&E program and knowledge base in our region, but nationwide as well.

The size of the region is also a challenge. Because we are so dispersed, we've developed new ways to interact with one another. For instance, we have field offices that conduct training together. This allows the offices to partner and share more information. As a result, they become a more cohesive group.

As I stated earlier, the Huntsville Office has experienced tremendous growth in workload with a small number of additional personnel. We conducted a team assessment of a large AA facility in the Huntsville area where all the team members were from outside the office. Not only did it help the office, it was also a great experience for the team and provided an opportunity for them to have a good dialogue.

What changes have you seen in DSS and in the region since you've been the regional director?

I progressed to the Regional Director position through a traditional path. I started as an investigator, back when DSS still had personnel security investigations as part of its mission. After several years of conducting background investigations, I became an Industrial Security Representative and moved to Houston.

My next position with DSS was the Field Office Chief of the Irving Field Office. For me, that background and experience has been invaluable. When I was an Industrial Security Representative, I was also the Counterintelligence representative, and I was approving some IT systems — a real mix of duties.

I have a broad base of experience and as a result, I have a good understanding of the roles and duties of each specialty. The difference now is that we have true Counterintelligence and Information Systems Security Professionals. That's been a significant shift since I joined DSS.

I think the Southern Region has been very effective in integrating Counterintelligence into Industrial Security because of my experience and because we have personnel in key positions who also come from an investigative background. We understand the intent behind the integration and what we're trying to achieve.

Another change I've seen, and this is not unique to the Southern Region, but we are putting a greater emphasis on developing future leaders to grow into positions that we expect to come available in the next few years. A large percentage of our workforce will be eligible to retire in the next five to 10 years, and we have been thinking about how we capture and transfer that knowledge. We also have to ensure we have employees positioned to step into those leadership positions when necessary.

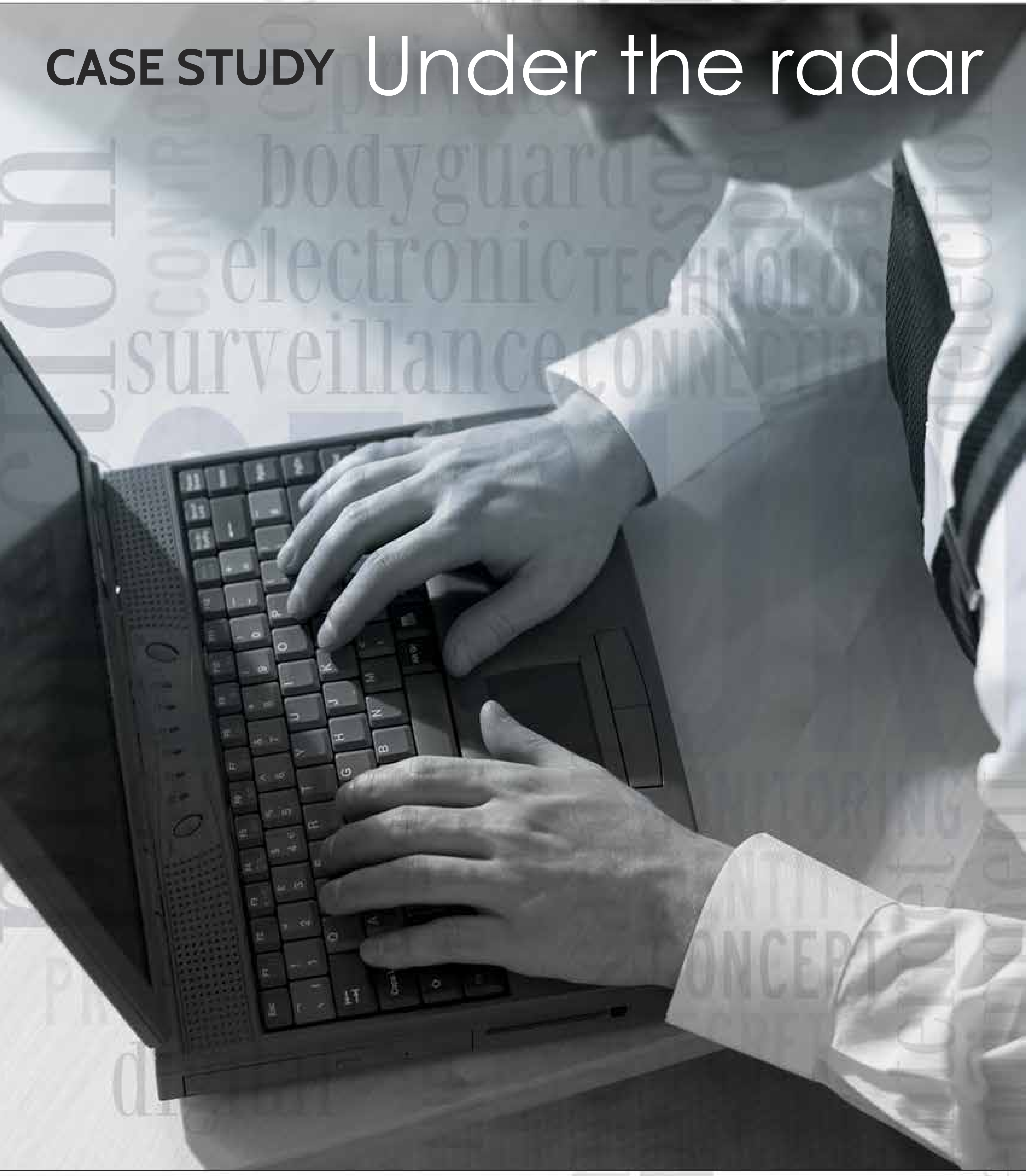
Just like the Western Region, you have had your share of natural disasters. How does that affect your operation?

Yes, we have our share of disasters, tornados — Oklahoma is tornado alley — as well as hurricanes and most recently earthquakes. Those tornado and hurricane seasons keep us very busy.

Every employee needs to have the tools available to them to deal with these situations. We've identified areas in our offices for safety, and when we have employees traveling, we ensure they understand current conditions, what to do, where to go, etc.

The Southern Region is also one of the alternate locations for DSS Headquarters continuity of operations. Therefore, we have to ensure our emergency operations plan includes that aspect in addition to local weather considerations. Everything that is currently done at headquarters has to be able to be done here, and we are also working closely with the International Division in Industrial Policy and Programs to ensure we can continue the international transfer of classified materials.

CASE STUDY Under the radar



In January 2013, a cleared employee received a reduction-in-force notice from his employer — a cleared contractor. Four days later, the contractor's security department detected that the employee sent several files from his work email account to his personal email account. Two of the emailed files contained information marked "For Official Use Only" and "Company Proprietary."

On his last day of work in March 2013, the employee met with his manager, a representative from the contractor's Human Resources (HR) department and members of the contractor's security department. During the meeting, the employee admitted to sending the files from his work email to his personal email account.

The employee then agreed to provide his personal computer to company security for a forensic review. He also agreed to provide the security department with all copies of company information that he had emailed to any personal email account, downloaded to external storage devices, printed in hard copy form, or otherwise taken from the contractor.

The employee agreed to delete or destroy any information from his personal computing resources or personal accounts in a manner that could be verified by the contractor's security department. At that time, the company entered nothing into the Joint Personnel Adjudication System (JPAS) concerning this incident.

During a follow-up meeting in April 2013, members of the contractor's HR and security departments met with the now-former employee and reviewed email messages in the employee's personal email account.

The security department recovered copies of 41 email messages that the employee had sent to his personal email account. This included information not previously known to have been transmitted out of the company.

In May 2013, subject matter experts reviewed all of the information recovered from the employee and determined that at least some of the information was sensitive. The reviewers described several of the files and email messages as being potentially useful to the company's competitors or foreign adversaries, and that one email contained unmarked classified information.

The incident was first reported to DSS in May 2013 when the company submitted a final administrative inquiry. DSS then sent an individual culpability report to the Department of Defense Central Adjudications Facility. However, the incident report was not reflected in the employee's JPAS record until June 2013.

Eighteen days after the incident report was entered, a loss of jurisdiction was entered on the employee's clearance eligibility (company separation with an unresolved incident report). In July 2013, a detailed report outlining potential espionage indicators was provided to another government agency and DSS.

The incident came to light again in May 2014 during a team security vulnerability assessment at the cleared facility. At this time, a suspicious contact report was written and elevated to DSS Headquarters.

Lessons Learned

There were several counterintelligence indicators present during this event. The employee involved in the incident was a dual citizen and demonstrated insider threat behavior by emailing company files to himself within just a few days of receiving a layoff notice.

The facility waited four months to report the matter to DSS and another government agency. When the employee left in March 2013, there was no incident report entered in JPAS. As a result, the employee could have been able to begin employment with another cleared contractor and be immediately placed back into access to classified information.

When the matter was elevated to DSS Headquarters in June 2014, all prior actions were validated. The employee's JPAS and personnel security records were updated, communication was initiated with other government agencies, and the case was shared with Industrial Security Field Operations, Quality Assurance and Counterintelligence leadership.

NISPOM Requirements

Paragraph 1-304 of the National Industrial Security Program Operating Manual addresses culpability reports, stating that "contractors shall establish and enforce policies that provide for appropriate administrative actions taken against employees who violate requirements of this Manual.

"They shall establish and apply a graduated scale of disciplinary actions in the event of employee violations or negligence. A statement of administrative actions taken against an employee shall be included in a report to the cognizant security agency when individual responsibility for a security violation can be determined and one or more of the following factors are evident:

- The violation involved a deliberate disregard for security requirements
- The violation involved gross negligence in the handling of classified material.
- The violation involved was not deliberate in nature but involves a pattern of negligence or carelessness."

Classified data spills

A costly error for employees and organizations

by Beth Alber
Office of Public and Legislative Affairs

In recent years, the media has covered several high visibility instances of sensitive government information being released to the public. Because of the potential damage that unauthorized disclosure can have to the United States and its interests, as evidenced by the actions of the Wikileaks organization and former government contractor Edward Snowden, the U.S. government implemented several security measures to minimize the potential for classified data spills.

Soon after Wikileaks made public videos and documents related to the wars in Iraq and Afghanistan in 2010, the president signed an executive order that directed structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks.

DoD, along with other government agencies, utilized new security technology to restrict use of removable media in an effort to prevent classified spills.

What is a classified spill?

Classified data spills occur when classified data is introduced either onto an unclassified information system or to an information system with a lower level of classification outside of approved procedures.

Early spill identification, notification, and a thorough understanding of where the spilled data occurred, as well as where the data might have been sent, are essential to avoid widespread contamination of back up servers, tape systems, and off-site storage locations.

Types of Spills

There are several types of data spills, including web-based, Personally Identifiable Information (PII), or Classified.

A "web-based" spill is any data found on any website available to the general public that is classified at any level higher than the classification of the system it is viewed on. Web-based spills apply to the viewing of classified data through a web browser. However, they have the potential to contaminate the local computer through temporary internet files and the browser cache.

The 2010 Wikileaks incident, as well as the 2013 Edward Snowden incident were largely web-based spills, and DoD employees and contractors were warned not to view the classified information available on the public sites using government-furnished equipment.

In addition, clearance holders are advised not to seek out and view known classified information that has not been officially cleared for public release using their personal computers, as doing so violates agreements made upon granting their individual security clearance.

Other types of data spills are identified based on the level of information or technology involved in the spill. A PII spill is any unauthorized disclosure of PII, either intentional or unintentional, or any authorized disclosure that is not disclosed utilizing the approved safeguards, such as encryption or secure transfer protocols.

PII is defined as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual.

A lost laptop containing social security numbers is an example of a PII data spill, as are posting PII on public-facing websites, sending data via e-mail or attachments to unauthorized recipients, and providing hard copies of data to individuals without a need to know.

Classified data spills are likely to occur during the improper handling/disclosure of data classified at the Confidential, Secret or Top Secret level. This includes, but is not limited to data that is emailed, transferred, copied, scanned, or created on any system not approved for processing or storage at the appropriate classification level or higher.

It is also important to note that a data spill can occur due to aggregation of multiple source inputs. For example, the processing of three related "Confidential" documents on the same machine can cause the overall classification level of the information to rise to a "Secret" designation due to relation and proximity. This would in turn cause a data spill on the machine if that machine was not accredited to handle classified at the "Secret" level.

Actions in Case of a Spill

What should you do if a data spill occurs?

During a spill event, a speedy and coordinated response among security, information assurance and other technical personnel is vital. In addition, end users must be trained in proper response activities to a data spill in order to avoid inadvertent propagation of the spill to other machines, users or facilities.

This training should include both procedural and communications instruction that end users should initiate when they believe a spill has occurred involving their system.

Significant unauthorized or inadvertent release of classified information on unclassified information systems can occur quickly, so prompt recognition and action by both end-users and technical staff can help minimize the exposure of sensitive or classified data to unauthorized parties.

The cost of cleanup actions for a data spill will increase exponentially as the number of workstations, mobile devices and servers touched by the classified data increases due to propagation.

When a potential classified data spill is discovered, users should immediately alert the security manager in accordance with published organizational procedures so that he/she can quickly implement technical isolation of contaminated workstations, servers, and back up systems to avoid spreading the contamination, prolonged loss of systems availability and/or possible destruction of contaminated assets, and to minimize exposure of classified information to individuals or organizations lacking the proper clearance and need to know.

Additionally, a classified information spillage is a security violation that requires investigation to determine whether the spill was willful, negligent, or inadvertent.

Spills and unauthorized disclosures of classified information are categorized into three categories:

Willful — An incident is willful if the person purposely disregards DoD security or information safeguarding policies or requirements (e.g., intentionally bypassing a known security control). An individual who knowingly and intentionally leaks classified information may face serious consequences, to include possible criminal prosecution.

Negligent — An incident is negligent if the person acted unreasonably in causing the spillage or unauthorized disclosure (e.g., a careless lack of attention to detail, or reckless disregard for proper procedures).

Inadvertent — An incident is inadvertent if the person did not know, and had no reasonable basis to know, that the security violation or unauthorized disclosure was occurring (e.g., the person reasonably relied on improper markings).

As a part of the investigation, dangerous security practices are identified, culpability may be assigned, and necessary actions are taken to preclude a recurrence of the spill or unauthorized disclosures.

Classified data spills cost the government and the defense industrial base millions of dollars each year, both in system sanitization/replacement as well as productivity lost for end users involved in the spill and subsequent cleanup.

However, the cost to national security from an unauthorized disclosure could be higher. Adherence to regulations and organizational procedures will help minimize these costs and strengthen the security posture of government agencies and contractor facilities.

Data Spill Scenario: “Beware the Scanner”

by Jonathan Cofer
Office of the Designated Approving Authority
Industrial Security Field Operations

An analyst works in an "Open Storage SECRET" work area and deals with classified information regularly. Occasionally, he is tasked to review TOP SECRET documents, which he does in the Sensitive Compartmented Information Facility (SCIF) area as he should.

One day, after reviewing the TOP SECRET document for his assignment, he fails to notice that a single page of the document fell out of the folder during his review, and after securing the folder he gathers his things and exits the SCIF. The single page from the TOP SECRET document is now shuffled among the other papers in his stack, which he places on his desk when he arrives back to his cubicle.

Already a violation has occurred, but it will soon get far, far worse, and very quickly at that. A few days later, a colleague asks our analyst to scan and email him a few unclassified documents they had been working on together.

So our analyst grabs the document pages out of the stack on his desk and proceeds to scan and email the requested documents to his colleague. Unfortunately the analyst didn’t examine each page he was about to scan prior to sending, and our misplaced TOP SECRET document was in that very stack.

Now a "data spill" has started. Let’s track the progress of the spill over the next few hours:

1. The TOP SECRET document was scanned via multifunction machine and emailed to his colleague.
2. The colleague then saved a copy of the scan to his desktop and network drive and, without thoroughly examining the scan, he forwards the email to the team’s group mailbox for distribution.
3. One of the other team members notices, after forwarding the scan to his supervisor for comments, that the document on page 9 of the scan is marked "TOP SECRET", and alerts his supervisor, who then notifies security.

As there is no approved method for sanitizing media that has touched "TOP SECRET" other than destruction, this small mistake will result in a very costly cleanup. By following the path the data took through the network, we can determine that at the very least we will have to physically remove, destroy and replace:

- The hard drive of the multifunction machine (they do have hard drives, and they are quite expensive!).
- The desktop/laptop hard drive of every user who received and opened the email.
- The affected hard drives of any email or file server on which the file resided, even temporarily.
- Any back up tapes, discs or drives exposed to the file.
- The BlackBerry smartphones of any user who received/opened the file on their mobile device.

If we say for the sake of argument that 20 people (and their associated machines/devices) were involved in this spill, we could be looking at destroying and replacing well over $35,000 worth of hardware. This doesn’t even take into account the lost productivity of the users involved, especially if they didn’t properly back up their other data.

Add in the man-hours required to hunt down and sanitize (destroy) any traces of the file by information technology/information assurance, and this momentary act of carelessness may approach the six-figure mark in cleanup costs. If our analyst had simply checked each page of the document he was about to scan prior to transmitting, he would have noticed the misplaced classified document, and the security violation would not have progressed into a major data spill.

Counterintelligence Certificate Curriculum Now Available

As part of the commitment to provide the best Counterintelligence awareness training, CDSE developed the CI Awareness Certificate Curriculum.

The curriculum addresses CI awareness and reporting, insider threat awareness, the integration of CI into security programs, CI concerns in personnel security and foreign travel, research and technology protection, and threats to cleared defense contractors under the National Industrial Security Program.

The curriculum is composed of eight eLearning courses, three short courses, and a comprehensive final exam. CDSE's eLearning courses are interactive, computer-based training sessions.

The short courses help security professionals bolster their knowledge of a critical topic or quickly access information needed to complete a specific task. Three of the courses included in this curriculum received multiple Omni Awards and/or Horizon Interactive Awards.

This program is designed for DoD military, civilian, and contractor security professionals (facility security officers) and practitioners responsible for developing and maintaining a security program for their unit or facility. The certificate demonstrates that an individual has successfully attained the competencies within this curriculum.

After students successfully complete all the learning activities through the Security Training, Education, and Professionalization Portal (STEPP), they can register for the final exam.

This comprehensive exam includes a battery of 50 questions from a pool of 100, with a minimum score of 75 percent required to pass. Exam questions emphasize the learning objectives from the collective CI Awareness Curriculum. After they complete the program, students are awarded a unique certificate.

For more information and to view the courses in the curriculum, visit the CDSE website.

Special Program Security Certification Newest in Series

The Center for Development of Security Excellence (CDSE) partnered with the Department of Defense Special Access Program (SAP) Council to renew efforts to develop a specialty certification program tailored to the SAP community's needs.

The result is that the fourth and newest DoD specialty security certification underwent pilot testing in June 2014, and in February 2015, the production version was released via commercial testing.

Fifty-four individuals representing the Army; Navy; Air Force, Defense Advanced Research Projects Agency; Missile Defense Agency; Defense Contract Management Agency; Defense Threat Reduction Agency; Defense Security Service; and Acquisition Technology and Logistics were identified to participate in this pilot.

Participants were required to have already been conferred with the Security Fundamentals Professional Certification (SFPC). The pilot was extremely successful with 33 percent of participants achieving a passing score.

Developed under the Security Professional Education Development (SPēD) Program, the Special Program Security Certification (SPSC) assesses candidates' understanding and application to create and maintain a secure environment to successfully develop and execute a SAP.

Competencies such as information security, classification management, personnel security, SAP fundamentals, physical security, program security, vulnerability assessment, and management and information assurance are assessed.

The target audience for the SPSC includes DoD and other U.S. government personnel (civilian and military), and contractors who are performing duties within the DoD SAP environment, and have already been conferred the SFPC.

The SPSC is the fourth specialty certification fielded under SPēD, the others being the Adjudicator Professional, Industrial Security Oversight, and Physical Security Certifications.

The SPSC is designed to meet national accreditation standards from the National Commission for Certifying Agencies, further validating the assessment as legally defensible for high-stakes certification.

More information on the SPSC can be found on the SPēD website at www.cdse.edu/certification/.

GIVING BACK

DSS serves the community

Field Offices across the nation lend a helping hand

WOUNDED
WARRIOR
HOMES
Helping Those Who Protect Our Freedom
www.WoundedWarriorHomes.org

Defense Security Service employees, in small groups and through individual efforts, are making a difference in the quality of their communities and in the lives of their friends, neighbors, and those in need. Through acts of kindness and commitments of time and energy, DSS employees are showing that ordinary people can make a difference in communities across the country.

Western Region Efforts

In November, nine DSS employees representing the Western Region Headquarters and San Diego and Los Angeles field offices participated in a volunteer project to enhance the lives of wounded service members. The project took place on the property belonging to Wounded Warrior Homes, a San Diego-based 501(c)3 charitable non-profit organization that provides transitional housing to single post-9/11 combat veterans with traumatic brain injury (TBI) and post-traumatic stress.

The team, which included a total of 30 volunteers from different organizations/companies in the area, helped prepare a section of the property where a pre-fabricated home will be located. The team moved concrete blocks for a retaining wall, dismantled an existing wooden deck as well as the concrete pathway leading from the house to the deck, and cleared and removed all concrete, branches, pavers, rocks, and dirt to proper disposal/storage areas.

A smaller team returned in mid-January to work on the new home that was placed on the portion of the property that was cleared/prepped during the volunteer day in November.

"We always talk at work about supporting the warfighter," said Regional Director Karl Hellman, "so volunteer days like these are special because we get a chance to really make a difference in the lives of some of our warfighters. Volunteering to help on a project like this is a natural extension of what we do every day."

Hellmann added that there are many former military members now working as federal employees in the Western Region, and they understand what it's like to transition back to civilian life. He noted that the Tacoma and Colorado Springs offices have volunteered for Wounded Warrior projects in their areas as well. "To get a chance to talk with these veterans and be a small part of helping is truly gratifying," said Hellmann.

While onsite, the team gathered into a formation to participate in a ceremony where Western Region Counterintelligence Chief Tom Montero, who spearheaded both efforts, and Deputy CI Chief Jeff Boick presented a U.S. flag to a wounded warrior who had suffered TBI in Iraq.

Capital Region Productions

On the East Coast, the Capital Region and Field Operations Headquarters teamed with a local cleared company to participate in a Habitat for Humanity project in Alexandria, Va. The team sanded walls, painted closets, installed doors and even did some landscaping work during their project.

Matt Roche, Field Operations Headquarters Chief and former Alexandria Field Office Chief, said, "This is the third year Capital Region has done a Habitat for Humanity project with our security professional counterparts from industry. Working and sweating side by side cements

Pitching In: (From left), Matt Roche, Headquarters Industrial Security Field Operations, paints a closet during the Habitat for Humanity event; Heather Green, Capital Region Director, puts the finishing touches on a paint job during that event; Mike Shydlinski (right), DSS Counterintelligence directorate, assists with tying flies as part of Project Healing Waters Fly Fishing.

the partnership, demonstrating that shared perspective of service to nation inside and outside of our day-to-day responsibilities."

"It was a pleasure participating in the Habitat for Humanity event," said Regional Director Heather Green. "Taking time out to give back to the community is critical. I found it to be very productive and rewarding to know that my time spent was directly helping a family in need. I look forward to participating in future events."

Sean Hofmann, Industrial Security Representative from Alexandria, said, "I volunteered for the project because I enjoyed my time serving others while I was in the Marine Corps and wanted to continue. It is a great feeling to be part of a massive cleanup effort or a home-building project that will benefit others. Now that I'm a father, I feel even more compelled to show my children why this is so important."

Other Ways to Contribute

"I see Habitat for Humanity as an organization that produces a real service for people in need of homes, but I would encourage someone interested in volunteer service to do some research and find an organization that they are passionate about," Hofmann continued.

Those other organizations include counseling and mentoring young people, supporting activities to end the cycle of homelessness, clothing and food drives, book sales, raffles, winter coat drives, disaster relief work, cooking for the needy, drives to collect school supplies, and holiday gift drives.

Selena Hutchinson, Office of the Designated Approving Authority in Field Operations, said, "I have been active in volunteerism all my life, and I will always serve the community in which I live." Hutchinson serves on the Board of Directors for Community Lodgings, a local charity that prevents homelessness in Alexandria by offering a hand up, not a handout. She also cooks and serves meals for S.O.M.E. (So Others Might Eat) with her chapel.

A Program for Every Skill

Mike Shydlinski, Counterintelligence Directorate, said he chose the charity, Project Healing Waters Fly Fishing, because, "I have seen and recognized the benefits associated with fly tying and fly fishing in the rehabilitation of our nation's veterans suffering from physical and psychological trauma incurred while defending our nation.

"The benefit I receive is knowing that through fly fishing, I am able to make someone forget about their troubles for a few hours and in doing so, helping our wounded warriors recover and find their way back," he continued.

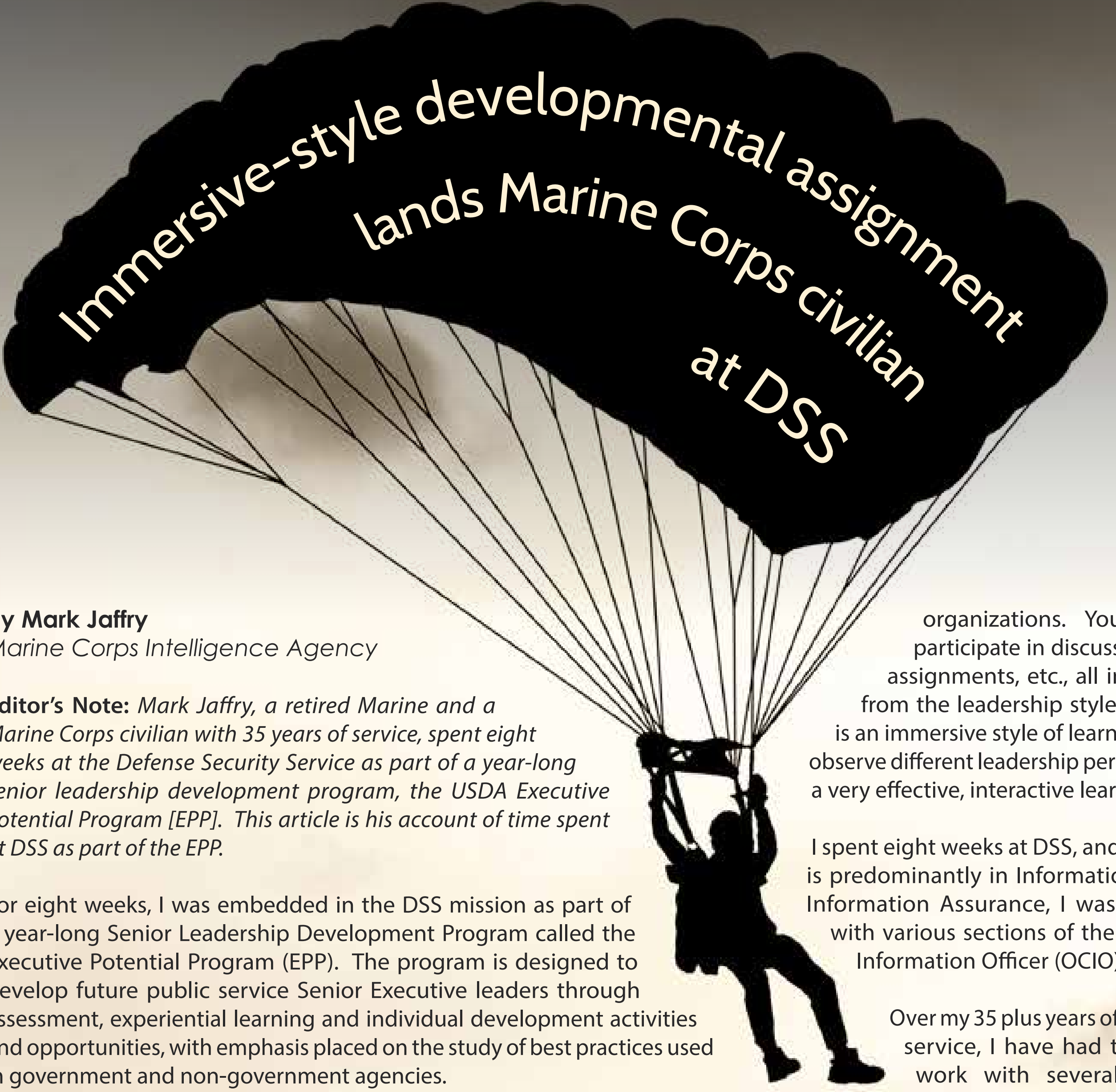
First introduced at the Walter Reed Army Medical Center to disabled active duty personnel, Project Healing Waters Fly Fishing aids in the physical and emotional recovery of wounded or injured military personnel through the art of fly fishing. The program, open to all disabled active duty and military veterans, is now expanding to offer its services to military hospitals and Veteran's Administration medical centers across the nation.

As a member of the Trout Unlimited and the Potomac-Patuxent Chapter of Trout Unlimited (PPTU), Shydlinski volunteers his time and experience as a fly fishing angler and guide to support the program. PPTU members meet with military members in the Warrior Transition Unit at Fort George G. Meade weekly, tying flies and building fly rods and testing their handiwork at the local pond. The program has reached more than 300 service men and women.

Through a variety of volunteer efforts and commitment of time and energy, DSS employees can and will continue to make a difference in communities across the country.

Hard Work: (At left, from top) DSS employees and family members pause for a photo while doing construction work at the Wounded Warrior Home; DSS CI Special Agent Jasan Thomason (right), from the Cypress Field Office, spreads gravel at the Wounded Warrior Home; DSS CI Special Agent Al Rodriguez, from the Cypress Field Office, sets a fence post at the Wounded Warrior Home.

Immersive-style developmental assignment lands Marine Corps civilian at DSS



by Mark Jaffry
Marine Corps Intelligence Agency

Editor's Note: *Mark Jaffry, a retired Marine and a Marine Corps civilian with 35 years of service, spent eight weeks at the Defense Security Service as part of a year-long senior leadership development program, the USDA Executive Potential Program [EPP]. This article is his account of time spent at DSS as part of the EPP.*

For eight weeks, I was embedded in the DSS mission as part of a year-long Senior Leadership Development Program called the Executive Potential Program (EPP). The program is designed to develop future public service Senior Executive leaders through assessment, experiential learning and individual development activities and opportunities, with emphasis placed on the study of best practices used in government and non-government agencies.

Participation in the EPP enhances leadership qualities, and the core curriculum is centered around the Office of Personnel Management's Executive Core Qualifications with emphasis on "Leading Change" and better preparing us to be agents of change within our own organizations.

During the program, I'm required to attend several learning seminars, obtain a senior executive-level mentor to help guide me through the program and answer any questions that arise, and conduct at least five one-on-one interviews with senior executives.

Another part of the program, and a major learning experience for me, was the requirement to complete two eight-week developmental assignments outside of my organization. I approached DSS senior leadership to consider allowing me to perform one of my two eight-week assignments here, as this organization's reputation is well-known and well-established within the Department of Defense.

During the EPP developmental assignments, you are integrated into the work center assigned, allowing you to observe specific leaders in action, in their own organizations. You attend meetings, participate in discussions, perform work assignments, etc., all in an effort to learn from the leadership style being observed; it is an immersive style of learning. The intent is to observe different leadership perspectives and styles; a very effective, interactive learning environment!

I spent eight weeks at DSS, and as my background is predominantly in Information Technology and Information Assurance, I was assigned to work with various sections of the Office of the Chief Information Officer (OCIO).

Over my 35 plus years of federal and military service, I have had the opportunity to work with several high-performing senior leaders and teams in other Department of Defense organizations, agencies and services, so I can say without hesitation that DSS is truly fortunate to have such an extremely large number of high-performing leaders.

In such a high-performing group as the DSS OCIO, I hesitate to call out specific individuals; however, I will describe the two leaders I worked with. I was first assigned to the Certification and Engineering team in the OCIO, led by Barbara Jackson. Considering the scope of its responsibilities, this small team's abilities and capabilities are truly noteworthy.

As her team was in the process of transitioning from one certification process to another, I had a front row seat to watch how, as a team, they developed and matured their understanding of this new certification process; first working through development of new process work flows, then outlining and describing new

A Winning Line-up: Senior Leadership Development Program participant Mark Jaffry (center), Marine Corps Intelligence Agency, stands with DSS Office of the Chief Information Officer employees that he worked with during his developmental assignment with DSS. The DSS OCIO employees are (from left) James Allen, Paul Murph, Jaffry, Conrad Bovell, and Barbara Jackson.

roles and responsibilities, and finally coordinating the creation of new templates to facilitate repeatable actions.

Over the course of the two weeks, I was able to participate in several team meetings and observed firsthand how Jackson interacted, both personally and professionally, with each member of her team. Despite a high workload that would challenge anyone's time management skills, Jackson capably led her team through several diverse projects, each with its own challenges, priorities, deliverables, and of course both internal and external dependencies.

My second assignment was with the Computer Network Defense team, led by Conrad Bovell. What Bovell and this team have been able to accomplish in such a short period of time is also worthy of recognition. Along with a small team of highly intelligent, technically proficient information assurance professionals, Bovell runs the Computer Network Defense Security Operations Center.

This high-performing team of information assurance professionals is responsible for watching over DSS networks, from the respective network boundaries to the desktop. This team manages each desktop computer, ensuring it is patched, updated, and upgraded as necessary to mitigate application and operating system vulnerabilities. In addition, they monitor network traffic looking for malicious code trying to come into the organization via email and the internet, and they also keep a watchful eye to ensure folks aren't doing things they shouldn't be doing or going places they shouldn't be going. This is a daunting task considering the size of the organization and the sheer volume of data that transits the DSS unclassified and classified networks on a daily basis. Fortunately, they have a tool kit full of applications that assist with parsing through it all.

Bovell and his team accomplish the seemingly impossible every day, keeping a vigilant eye out for trouble on the network as their tools scan the millions upon millions of data packets flowing into and out of the organizational firewalls, looking to stop hackers before they get inside and cause real damage.

As I look back on my time at DSS, I appreciate that DSS supported this Leadership Development Program and took the risk of allowing me to learn from this exceptional group of senior leaders. Without exception, they are all incredibly talented leaders, each one an inspiring example of the outstanding leadership resident within OCIO and DSS. This has truly been an invaluable experience for me, and I look forward to taking onboard, as well as passing along, all of the things I have learned here.

HIGHER LEARNING

First DSS Employee Earns CDSE Certificate

Curtis E. Cook (below, left), an Information Systems Security Professional with the Hurlburt Field (Fla.) Resident Office, receives the Center for Development of Security Excellence (CDSE) Education Certificate for Systems and Operations from DSS Director Stan Sims at a ceremony in January 2015.

Cook was the first DSS employee to earn one of five certificates offered by the Education Program, and the first CDSE student to earn that specific certificate.

Students can earn certificates by successfully completing four CDSE graduate courses.

Cook earned his certificate by completing the following courses: Security as an Integral Part of DoD Programs, The Future of Security Systems and Information Assurance, Security in the DoD Acquisition Process, and Cybersecurity and Oversight of Information System Security.

Each course is equivalent to a three semester-hour graduate course.

Sarah Laylo (right), Alexandria 3 Field Office Chief, presents U.S. Marine Corps Gunnery Sgt. Gary W. Triplett with a Certificate of Flag Presentation, for a flag flown over the U.S. Marine Corps War Memorial, during a retirement ceremony.

Retirement Ceremony Held for Triplett

In October 2014, employees of the Alexandria 2 Field Office and Headquarters Industrial Security Field Operations coordinated a retirement ceremony for U.S. Marine Corps Gunnery Sgt. Gary W. Triplett.

The presiding officer for the ceremony, held on Marine Corps Base Quantico, Va., was retired Air Force Maj. Sharon Dondlinger, Alexandria 2 Field Office Chief.

Triplett served in the Marine Corps for 18 years as a Marine scout sniper, working his way up to sniper/team leader, often occupying billets slated for higher ranking Marines. He served on numerous deployments, and was medically retired due to injuries sustained while deployed for Operation Enduring Freedom and Operation Iraqi Freedom.

His last assignment was at The Basic School on Quantico, where he served as the chief instructor for the Marine Gunner Course. In late 2012, Triplett worked at DSS as an Operation Warfighter intern.

His dedication to duty and technical prowess resulted in his being competitively selected for a civilian industrial security specialist position at the Alexandria 2 Field Office, after he was officially medically retired.

Attending the ceremony were members of Triplett's family, friends, and past and present colleagues.

DSS Welcomes Newest FISL 2 Graduates with Badges and Credentials

The most recent graduates of the Fundamentals of Industrial Security Level 2 (FISL 2) were honored at a ceremony at the DSS headquarters in mid-January. The 13 graduates represented all four DSS regions as well as Field Operations Headquarters and received their badges and credentials identifying them as Industrial Security Representatives.

Stan Sims, DSS Director said in his remarks, "This ceremony is a public acknowledgement of the effort involved and it says you have honed your skills and tradecraft."

Sims said that acknowledgement also brings responsibility and a requirement for each graduate to, "do your duty; to help ensure industry can safeguard our nation's technology. It also means we have 13 more Industrial Security Representatives charged with protecting national security."

Sims noted that three of the graduates were from Field Operations Headquarters. He said this will further the integration between the Headquarters and the field by ensuring a better understanding of the respective missions.

Sims told the graduates that few outside the security community may know what DSS does, but he emphasized, "Each American relies on us every day to do our mission in a fashion that serves national security. I charge each of you with that responsibility and to be inspired to continue our legacy."

The Fundamentals of Industrial Security Level 1 is the first in a series of Industrial Security Representative training and courseware. The purpose of the program is to develop productive employees as soon as possible. FISL 1 provides fundamental knowledge of National Industrial Security Program requirements and internal DSS processes and procedures. FISL 2 is conducted in a classroom setting and verifies the student's knowledge and understanding of the overall fundamentals of the NISP requirements and core responsibilities involved with the DSS Industrial Security mission.

Honoring the Legacy: To honor the legacy of Dr. Martin Luther King Jr., DSS hosted an event that combined poetry, music and a passionate recitation of King's "I Have a Dream Speech" on Jan. 14, 2015, at the Russell-Knox Building.

READY, SET, GO

Insider Threat Program Moves Threat Awareness into the Present

On Oct. 7, 2011, President Barack Obama signed Executive Order (EO) 13587, "Structural Reforms to Improve Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information."

EO 13587 directs the heads of agencies that operate or access classified computer networks (such as the Defense Security Service) to have responsibility for appropriately sharing and safeguarding classified information.

In November 2012, the White House issued National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs. These standards provide those departments and agencies with the minimum elements necessary to establish their own effective insider threat programs.

These elements include the designation of a senior insider threat official(s); capability to gather, integrate, and centrally analyze and respond to key threat-related information; monitor employee use of classified networks; provide the workforce with insider threat awareness training; and protect the civil liberties and privacy of all personnel.

These policies do not apply directly to cleared industry. Implementation of the National Insider Threat Policy for cleared industry will be outlined in Conforming Change 2 of DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM).

When issued, it is expected that the conforming change will outline insider threat requirements for cleared industry operating under the National Industrial Security Program. Once issued, cleared industry will have six months to implement the program. These minimum standards are expected to include:

Establish and Maintain Insider Threat Program

Designate Insider Threat Senior Official. This individual must be cleared in connection with a facility clearance with responsibility for establishing and executing an insider threat program. The official may be the facility security officer (FSO), but must also be a senior official. In any event, the FSO will be an integral member of the contractor's Insider Threat program.

Gather, Integrate, and Report. Each facility will be responsible for reporting relevant and available information indicative of a potential or actual insider threat when the information constitutes adverse information and suspicious contacts.

Develop Insider Threat Training. Contractors may develop their own training based on the minimum standards or use the training available through the DSS Center for Development of Security Excellence (CDSE) under Counterintelligence at: http://www.cdse.edu/catalog/counterintelligence.html:

There are currently two insider threat training courses available: Establishing an Insider Threat Program for Your Organization; and, Insider Threat Awareness.

Although these courses are not required, contractors may include the training in their security programs now. Contractors will also have to establish and maintain a record of all cleared employees who have completed the initial and annual training.

Insider threat is not a new concept for either the government or industry.

Insider threat is not a new concept for either the government or industry. The basic requirements of the NISPOM currently include insider threat standards. The NISPOM requires educating employees on what to report to their Facility Security Officer, DSS, and the FBI, which has contributed to finding insider threats for years.

The reporting requirements for adverse information, suspected espionage, sabotage, and terrorism, loss, compromise or suspected compromise, individual culpability and security violations have not changed. These reporting requirements have the potential to identify individuals who need assistance with additional security training or support and detecting the insider threat and risk to national security.

The difference now is that the Insider Threat Program will assist in recognizing potential or actual insider threat. It will also continue the DSS partnership with industry to protect the United States, its economy, secrets, and technologies and ultimately protect those we send into harm's way by deploying uncompromised tactics, techniques, plans, strategies, and systems for the warfighter.

As the conforming changes in the NISPOM move forward, there will be guidelines and assistance from DSS, along with guidance for developing and implementing these programs. In order for Insider Threat programs to work and to minimize the threat from insiders we need to get ready, get set, and go.

Capital Region Develops Peer Recognition Program

by Heather Green
Director, Capital Region

Sometimes in our busy work environment, employees' hard work and daily achievements are not recognized as often as they should be. Employees are our number one asset and the leadership of the Capital Region (CR) takes pride in acknowledging those dedicated to the mission.

In an effort to establish a meaningful, responsive program, the CR has implemented a regional recognition program that enables employees and supervisors to recognize one another for their achievements and contributions toward achieving the region's mission and objectives. The recognition program is comprised of the CR Star Recognition and the Peer Kudos Recognition.

The Star Recognition is presented quarterly and allows supervisors to nominate employees that have demonstrated success in any of the CR established objectives.

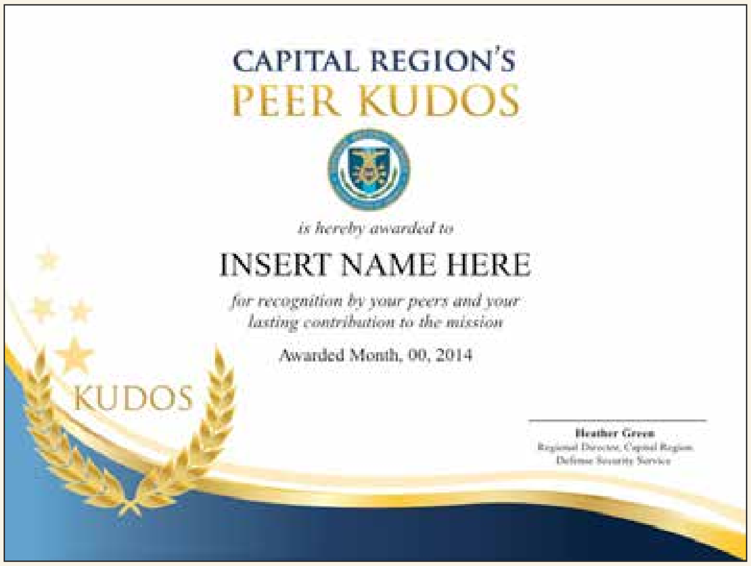
These objectives include: Teamwork and Coordination, Communication, Quality, Managing Priorities, Innovative Thinking and Building Morale. Each quarter a supervisor nominates an employee and provides a description of the impact the individual has made on contributing to the mission.

The Peer Kudos recognition enables employees to nominate their peers, an individual or a team, for recognition of a job well done. The nomination can be for anything that is viewed as going above and beyond an employee's regular job description.

The submissions are completely anonymous and announced throughout the quarter. Certificates are presented to the recipients at every quarterly town hall.

In the last year, over 50 peer kudos have been processed; recipients include CR employees as well as employees from other DSS directorates and other field offices who provide TDY support to the Capital Region.

The region's leadership team is fortunate to have an outstanding, dedicated workforce and will continue to find innovative ways to recognize those that go above and beyond the call of duty. We take pride in the accomplishments of our employees and will continue to shine a light on their successes!



CAPITAL REGION'S
PEER KUDOS

is hereby awarded to

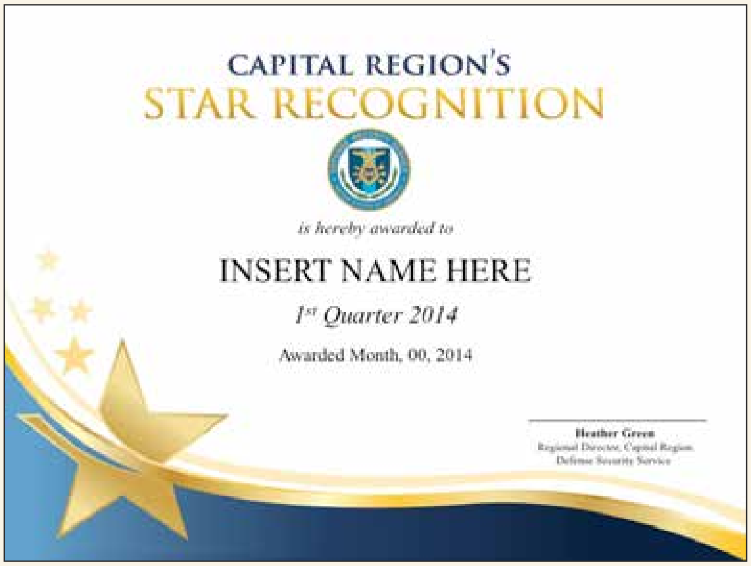
INSERT NAME HERE

for recognition by your peers and your lasting contribution to the mission

Awarded Month, 00, 2014

KUDOS

Heather Green
Regional Director, Capital Region
Defense Security Service



CAPITAL REGION'S
STAR RECOGNITION

is hereby awarded to

INSERT NAME HERE

1^{st} Quarter 2014

Awarded Month, 00, 2014

Heather Green
Regional Director, Capital Region
Defense Security Service

NCR's regional recognition program enables employees and supervisors to recognize one another for their achievements.

FY14 | DSS by the Numbers

Personnel Security Management Office for Industry (PSMO-I)

940,000	National Industrial Security Program (NISP) contractors with clearance eligibility
880,000	NISP contractors with access to classified information
220,000	Requests for Investigation for security clearances processed
80,000	Interim security clearance determinations made
7,000	Adverse information reports triaged
6,000	Overdue periodic investigations (down from 51,000 beginning of the year)
125	Interim Clearance suspensions

Security Professional Education Development Program (SPēD)

2,100	Conferrals of Security Fundamentals Professional Certification (SFPC)
571	Conferrals of Security Asset Protection Professional Certification (SAPPC)
264	Conferrals of Security Program Integration Professional Certification (SPIPC)
597	Conferrals of Adjudicator Certification
340	Conferrals of Physical Security Certification
157	Conferrals of Industrial Security Certification

Center for Development of Security Excellence (CDSE)

172	Education Course Completions
14,203	Personnel registered for webinars
37,265	PDUs [Professional Development Unit] Earned
64,146	Visits to Security Shorts
181,135	Visits to Toolkits
485,249	Course Completions

Counterintelligence

34,213	Reports of suspicious contact from Industry
6,778	Referrals to Law Enforcement/ Intelligence Community
989	Investigations/operations opened due to DSS referrals
4,315	Intelligence information reports
3,291	Personnel attending seven Counterintelligence Webinars

Office of the Designated Approving Authority

26	NISP Command Cyber Readiness Inspections containing 30 circuit reviews
3,967	System security plans accepted and reviewed

Common Deficiencies in System Security Plans (SSP):

1. SSP incomplete or missing attachments
2. SSP not tailored to the system
3. Inaccurate or incomplete configuration diagram or system description
4. Sections in general procedures contradict protection profile
5. Missing certifications from the Information Systems Security Manager

3,308	Completed validation visits

Common Vulnerabilities found during System Validations:

1. Security relevant objects not protected
2. Auditing. Improper automated audit trail creation, protection, analysis, and/or record retention
3. SSP does not reflect how the system is configured
4. Inadequate configuration management
5. Improper session controls. Failure to have proper user activity/inactivity, logon, and system attempts enabled

Foreign Ownership, Control or Influence (FOCI)

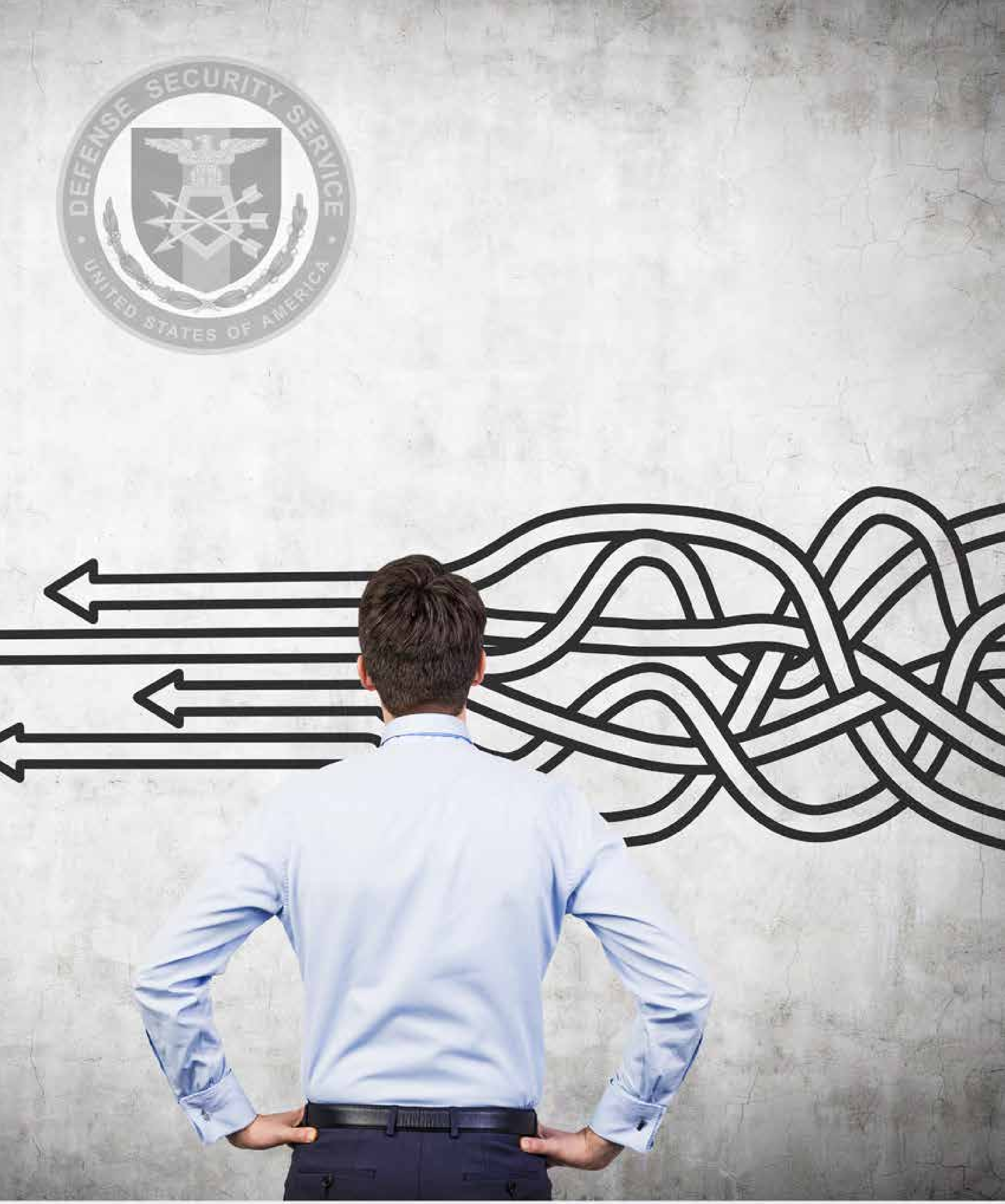
674	FOCI facilities
268	Mitigation agreements in place
53	FOCI agreements emplaced

Industrial Security Field Operations

6,783	Security Vulnerability Assessments conducted
10,856	Security Vulnerabilities identified
10,013	Non Acute/Critical Vulnerabilities identified
843	Acute/Critical Vulnerabilities identified
1,137	Facility Security Clearances issued

International

2,870	Request for Visits
12,500	Travelers/Visitors
946	NATO Visit Requests
2,213	NATO Travelers/Visitors
213	Transportation Plans
134	Hand Carry Plans



Defense Security Service