

# DSS ACCESS

VOLUME 2, ISSUE 1

OFFICIAL MAGAZINE OF THE DEFENSE SECURITY SERVICE



**CDSE ACHIEVES**  
**NATIONAL**  
**RECOGNITION**



# SPRING 2013

VOLUME 2, ISSUE 1



## SPOTLIGHT

CDSE Achieves National Recognition ..... 4

## INSIDE

DISCO Moves to DoD CAF ..... 6

Superstorm Sandy Pounds Northeast Offices ..... 14

Chief Financial Officer: What is Their Role? ..... 18

FOCI Operations Division Creates New Tool ..... 20

The Importance of Protecting Critical Program Information: *A Historical Perspective* ..... 22

Regional IT Project Managers Connect the Field to a New Level of IT Support ..... 26

DSS Office of Innovation: Design Forum Kicks Off New Initiative ..... 28

DSS Moves Out with Defense Agencies Initiative ..... 30

## DIRECTOR'S TOWN HALL

A Look Back at 2012 Successes, A Look Ahead to 2013 Challenges ..... 8

## ASK THE LEADERSHIP

A Q&A with the Director, Industrial Security Field Operations ..... 10

## DSS CASE STUDY

Bad Burn Run ..... 24

## AT ATTENTION!

DSS Offers CISSP Boot Camp ..... 28

## CDSE NEWS

..... 12

## WHO'S WHO IN THE NISP?

..... 31

## AROUND THE REGION

Facilitating Partnership Through Effective Communication ..... 32

Virginia Beach Field Office Opens its Doors to Industry ..... 34

Helping Habitat for Humanity ..... 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

**W**elcome to the first ACCESS of 2013. December 2012 marked not just the end of the calendar year, but the completion of my second year as Director of the Defense Security Service. Both milestones provided an opportunity to host two town hall meetings here at headquarters. My goal was to provide employees with a look back at 2012 and what the agency has achieved, as well as look over the horizon into 2013.



In preparing for the town hall meetings, I used the first issues of the ACCESS as a resource. Not only am I extremely proud of the magazine itself, I was struck by the depth and diversity of the articles. Every region and every mission area was included at some point. That shows me an agency at work on the same goals and committed to the success of DSS and our mission.

It also showed me that based on the achievements DSS had in 2012, we have set a very high bar for 2013! As I said at our town halls, we cannot afford to rest on our laurels. Regardless of the final outcome of the ongoing budget discussions and fiscal uncertainty, DSS must continually seek ways to improve our processes and procedures and achieve efficiencies where we can.

I believe our new Office of Innovation will play a critical role this year. We need to constantly look at better ways of accomplishing our mission, whether it is ultimately an IT solution or a different process. High-performing organizations (and I consider DSS a high-performing organization!) are always looking ahead, and we owe it to our employees, industry and government stakeholders, and ultimately the taxpayer to do the same.

In these pages you will find not only the latest news from DSS but also just how we are striving to be a better organization. The recent national accreditation of the Security Fundamentals Professional Certification (SFPC), our cover story, is the best example I can think of to show that commitment. Professionalization of the security workforce had been discussed for at least 20 years. But starting in 2008, a team at DSS embraced the idea and refused to be denied any longer. Just three years later, in April 2011, we awarded our first SFPC certifications. Now, we are awarding the second level of certification, with the third level projected to be fielded this year. And the result of the commitment to these efforts has been the first certification in the Department of Defense to achieve national level accreditation.

Regardless of the political environment and budgetary challenges, the DSS mission will always be relevant. I'm as excited to be at DSS as I was two years ago, and I look forward to a productive 2013!!



# CDSE ACHIEVES NATIONAL RECOGNITION

On Dec. 18, 2012, the DoD Security Fundamentals Professional Certification (SFPC) became the first DoD professional certification to receive national level accreditation. This event recognizes the significance of the SFPC and the rigor of its execution.

SFPC is the first of four certifications under the Security Professional Education Development Program (SPeD). The SPeD Certification Program is based on functions performed and requirements developed under DoD Instruction 3305.13, DoD Security Training.

Accreditation by the National Commission for Certifying Agencies (NCCA) places SFPC certification on par with others in the financial, legal, and healthcare professions such the American Association of Critical-Care Nurses and National Association of Social Workers.

Certification provides several immediate and long term benefits to commanders, directors, and the Defense Security Enterprise. Certification provides a portable credential across DoD and the Intelligence Community, promotes interoperability, and provides a clear pathway to success.

DoD Manual 3305.13-M, DoD Security Accreditation and Certification, mandates the Director, DSS, to apply for external accreditation of certification programs by the nationally

recognized certification accreditation body, the accrediting authority under the Institute for Credentialing Excellence (ICE).

DSS began the process in January 2012 to obtain NCCA review and engaged in an extensive application and standards review process using the DoD Security Training Council as the governing board.

The application package included statements and evidence to support compliance with NCCA's comprehensive standards and covered all aspects of the SFPC program including administration, assessment development and recertification.

The SPeD Program for the security career field is the first career field under USD(I) cognizance that has launched and received accreditation for its certification program. The intelligence career fields (i.e., Counterintelligence, GEOINT, etc.) are currently developing certification programs.

DSS/CDSE plans to seek accreditation for other certifications within the SPeD Certification Program, including core and specialty certifications.

## SPeD CERTIFICATION LEVELS



The **SFPC** is the foundational certification within the SPeD Certification Program and is a prerequisite for other certifications. In this certification, individuals demonstrate their understanding of foundational security concepts, principles, and practices.



The **Security Asset Protection Professional Certification (SAPPC)** requires individuals to apply foundational security concepts, principles, and practices.



The **Security Program Integration Professional Certification (SPIPC)** requires individuals to understand and apply risk management and security program management based on security concepts, principles, and practices. SPIPC is scheduled for release in FY13.



**Security Enterprise Professional Certification (SEPC)** is currently in the development phase. When fielded, it will require individuals to understand and apply concepts, principles, and practices for managing enterprise-wide security.

## TIMELINE

**2008**

DSS initiated the SPeD Program, and the first SPeD certifications were awarded.

**2011**

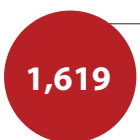
First SPeD certifications awarded for Security Fundamentals Professional Certification.

**2012**

First certifications awarded for Security Asset Protection Professional Certification.

## CERTIFICATION ACROSS DEPARTMENT OF DEFENSE

*As of January 9, 2013*



433

276



Security Fundamentals Professional Certification

Adjudicator Professional Certification

Security Asset Protection Professional Certification

## PARTICIPANTS

*The top five program participants within the Department are:*

**ARMY**

**AIR FORCE**

**NAVY**

**DSS**

**MISSILE DEFENSE  
AGENCY**



# DISCO MOVES TO DOD CAF



In May 2012, Ashton Carter, Deputy Secretary of Defense, directed a complete consolidation of the Department's personnel security adjudication functions, resources, and assets into the Department of Defense Consolidated Adjudication Facility (DoD CAF).

The new organization consolidates the Army, Navy, Air Force, Joint Staff, and Washington Headquarters Services adjudicative staffs, as well as that of the Defense Industrial Security Clearance Office (DISCO) and the Defense Office of Hearings and Appeals into a single organization under the authority, direction and control of the Director of Administration and Management. This total consolidation of the Department's personnel security adjudication functions was done to achieve the greatest efficiencies.

With the decision, DISCO, established in 1965, was absorbed into the consolidated CAF in October 2012 and no longer exists as an entity. A town hall was held in early October for DISCO personnel shortly before the consolidation to answer questions and thank personnel for their service to the Defense Security Service (DSS).

Laura Hickman, DISCO Director, opened the meeting and described consolidation as the latest in a series of complex changes for DISCO in the past year. The most significant change was the relocation in July 2011 from Columbus, Ohio, to Fort George G. Meade, Md. The move was in accordance with

the Base Realignment and Closure (BRAC) recommendations of 2005. With the move, DISCO lost almost 80 percent of its most experienced adjudicative workforce.

In spite of this, Hickman noted, DISCO was still able to meet the adjudicative timelines mandated in the Intelligence Reform and Terrorism Prevention Act (IRTPA).

"The ability to adapt has made DISCO successful," she said. "When IRTPA adjudicative timelines went into effect in 2008, CAF Directors didn't think we could meet the timelines," Hickman explained. "But Mr. Sims — who was Director of Security at the Office of the Under Secretary of Defense for Intelligence at the time — had a strategic vision for the CAFs. He asked each CAF director to leverage their best practices and the result is we're exceeding the timelines. Consolidation is just another step and example of change."

Stan Sims, DSS Director, echoed Hickman's remarks and also lauded the DISCO leadership for its success. "You have been able to pick good leaders, cultivate good advisory staffs and as a result, build great teams. We also recognized that co-

location under BRAC was just the first step," said Sims. "Everyone works from the same federal adjudicative standards. There is no reason for multiple agencies."

While Sims recognized the need for change and consolidation, he also acknowledged that it can be hard to change. "It is hard," he said. "But

## CONSOLIDATION TIMELINE:

- Oct. 21, 2012:** DISCO migrated to the DoD CAF
- Oct. 28, 2012:** DISCO adjudicative actions reflected DoD CAF, vice DISCO in the Joint Personnel Adjudication System (JPAS)
- Jan. 27, 2013:** Customers only see DoD CAF, DIA, NSA, NGA, NRO and DOHA reflected in JPAS

we all have to get used to change. It means you're looking for better ways to do things."

Sims noted that DISCO, at 47 years old, predated establishment of DSS. In fact, the adjudication mission was the longest continuous mission set in DSS. "DISCO was always part of DSS," said Sims. "The result [consolidation] is a significant change in how we do business. But we have to make the best of the change for our national security."

Sims reminded the DISCO employees of the importance of their mission. "When you make an eligibility determination, you are making a decision that not only affects the individual but affects our nation's security. Don't forget that," he said. "Focus on the mission and your role in the mission. The administrative details — who signs your paycheck, who owns the IT equipment — will all work out."

"The adjudication process has changed," Sims continued. "Now we have IRTPA and timelines. Last year was a stressful one for the agency and DISCO, with the move from Ohio, but DISCO is doing its job better now than it's ever been done. I am confident you will continue to do it well."

Sims went on to explain that not all DISCO employees were transitioning to the DoD CAF. The adjudicative function was transferred and consolidated, but DSS retained those functions that support DSS in its oversight role of the National Industrial Security Program.

DSS expects to stand up a Personnel Security Management and Oversight Office (PSMO) for industry to perform these functions which include the front-end of the personnel security investigation process and personnel security clearance management for over one million cleared contractors at over 13,000 cleared facilities.

Deputy Secretary Carter allowed for a one-year period of transition for complete consolidation with the various CAFs moving on a staggered schedule. The plan allows for initial operational capability by the beginning of fiscal year 2013, with full operational capability by the start of fiscal year 2014. Fiscal year 2013 is considered a year of execution and components are expected to fund civilian pay and support costs during the transition.

Sims explained that DISCO would use the year to "pull out" the pieces of the NISP mission. "We have to determine how to separate a true adjudication from the other essential steps," he said. "We will try to keep team integrity."

He closed by promising employees that regardless of how the final organizations looked, the DSS and DoD CAF missions would still be closely linked. "We are going to continue to work as a team," he said. "DSS will continue to be the interface between industry and the personnel security clearance process."

## DISCO THROUGH THE YEARS

2012

**2012:** DISCO transferred to DoD Consolidated Adjudication Facility.

**2011:** DISCO relocated from Columbus, Ohio, to Fort George G. Meade, Md., in accordance with the Base Realignment and Closure (BRAC) recommendations of 2005.

**1993:** In July, facility clearances processing was consolidated in DISCO as a result of the downsizing and consolidation of the DIS Regional offices. A new Facilities Branch was established in the Personnel Clearance Division, which created a focal point for User Agencies and prime contractors.

**1985:** On June 1, 1985, the Adjudication Division of DISCO was functionally transferred to the Directorate for Industrial Security Clearance Review (DISCR), Office of the DoD General Counsel. DISCR was subsequently changed to the Defense Office of Hearings and Appeals (DOHA). DISCO continued to process interim suspension cases and adverse information reports and retained responsibility to implement all DISCR decisions.

**1965:** DISCO became operational on March 1, 1965 for the purpose of determining on a nationally centralized basis the eligibility of industrial personnel for access to U.S. and foreign classified information. DISCO inherited the assets and personnel security clearance workload of approximately 115 Army, Navy and Air Force offices. It also absorbed from the Army the Central Index File containing the industrial security clearance records of approximately 16,000 contractor facilities and 1.5 million individuals working in those facilities.

1965



Stanley L. "Stan" Sims, Director DSS, held two town hall meetings for agency employees on Jan. 10, 2013, at the Russell-Knox Building, Quantico, Va. During the sessions, Sims spoke on a wide variety of topics that touched all aspects of the DSS mission. In holding the town halls, Sims said he wanted to provide a big picture view of the agency from his perspective that employees across DSS may not be aware of.

Sims reminded the audience that DSS celebrated a significant milestone in 2012 — its 40th anniversary. "I spent some time reviewing the history and did some research," he said. "While I was amazed at the changes at DSS, one theme emerged and it is just that: change. I expect this 'change' to continue in DSS in 2013 and beyond."

From those opening remarks, Sims looked back at 2012 describing it as a "phenomenal" year for the agency. "We have much to be proud of," he said. "While I may get to take the credit, you did the work."

He noted the agency's support of the Wounded Warrior Program and said that DSS leads the Office of the Under Secretary of Defense for Intelligence in recruiting and hiring under the program. He also discussed two significant achievements in information technology during 2012: establishment of Data Center West, and the Information Assurance assessment by the Defense Information Systems Agency (DISA). Data Center West provides enhanced IT services to the agency including redundancy to critical systems. DSS passed the DISA review with outstanding marks; in fact, the highest marks the agency has ever achieved.

A priority for Sims since his arrival at DSS in 2010 has been to emphasize the partnership between DSS and cleared industry as well as Government Contracting Activities. Sims stressed that this relationship has the biggest impact across the government and it's one that he is most proud of.

"This was a huge cultural shift," he said. "This was not a change in mission for DSS, but a change in how we do our mission. I receive positive feedback from industry almost daily which tells me we're on the right track. I had a vision, but you [DSS employees] executed."

A significant effort for DSS in 2012 was an initiative to deliver SIPRNet to field locations. While some timeframes have slipped a bit, Sims emphasized that the agency remained committed to the project and expected to see progress early in 2013.

Sims said the Center for Development of Security Excellence (CDSE) was leading the agency in its innovative delivery methods and making training accessible to a wider audience — in fact, CDSE saw 324,000 course completions in 2012. A number of CDSE courses are now eligible for college credit and CDSE began delivering a suite of graduate-level courses. Sims announced that Security Fundamentals Professional Certification, the first level of the Security Professional Education Program, is now nationally accredited and the first such program within the Department.

The director discussed the increasing emphasis in the Department and DSS on cyber threats and cyber security. He said DSS intends to establish a senior position within DSS to





# A LOOK AHEAD TO 2013 CHALLENGES



address cyber issues and to ensure the agency stays current and relevant with a rapidly changing cyber landscape.

Sims discussed a number of changes in how Industrial Security Field Operations conducts vulnerability assessments, from a change in vernacular, to the Security Rating Matrix, to prioritization to “find and fix.” The goal of these initiatives was to provide consistency, he said, but also to ensure that DSS was focusing its resources on the most critical facilities — those that were at the greatest risk. Sims also emphasized that these were not changes in policy, only a change in approach designed to better reflect DSS’s role and better manage resources.

He noted two other changes in Field Operations: Command Cyber Readiness Inspections (CCRI) and cyber notifications. “The CCRI mission is a natural fit for DSS,” he said. “Now, I know we are not resourced for it and this further stresses our ISSPs [Information Systems Security Professionals]. But it’s the right thing to do, and we have already seen success and industry welcomes our role.”

Established in 1965, the Defense Industrial Security Clearance Office (DISCO) predates the establishment of DSS and was its longest mission set. In October 2012, DISCO moved to the DoD Central Adjudication Facility.

Sims said that while it was hard to lose DISCO, it was the right thing to do for the Department and would ultimately result in adjudicative efficiencies. He said DSS would retain some functions previously performed by DISCO and is standing up a Personnel Security Management Office.

Sims’ look ahead for 2013 first addressed sequestration and the Department’s budget. Sims emphasized that his goal in any budgetary decision was to minimize the impact on the DSS workforce as much as possible, but ultimately DSS would have to do its share to absorb any final cuts along with the rest of the Department.

A primary goal for 2013 for DSS is to continue the partnership and outreach with industry and government partners. “For DSS to be successful, everyone has to embrace the concept and become involved,” Sims said.

Sims described his philosophy to effect change as: identify a problem, develop a strategy, and implement the change. “We will continue to look at process improvements and implement those that make sense,” he said.

He also tied process improvements to the employee climate survey conducted in the fall of 2012. “I appreciate your feedback and input,” he said. “I know we’re not perfect and there is always room for improvement. You gave us some ideas on how the agency and senior leadership could improve and we’ll take a look at them. I can’t say that all of the recommendations will be adopted, but we will look at those that had the greatest impact across the workforce.”

In his closing remarks, Sims challenged the workforce to not rest on past successes but to continue to change for the better. “Remember, it’s our agency, our mission, our responsibility. We are all responsible for DSS successes and we must always look to be better.”

# A Q&A WITH THE DIRECTOR,



**Richard Lawhorn** has been the Director, Industrial Security Field Operations since 2008. In this position, he is responsible for management, administration, and oversight of all DSS field elements. Field Operations is the single largest organization within DSS with over 400 employees scattered across the United States in 60 locations.

Since joining DSS, Lawhorn has held a number of positions of increasing responsibility within the Industrial Security Program, to include Industrial Security Representative (IS Rep), Regional Staff Specialist, Field Office Chief, and Deputy Director for Field Operations.

Lawhorn sat down with the ACCESS editorial staff to discuss changes in the National Industrial Security Program (NISP) as well as his goals for FY13.

## **How has the NISP changed since you were an IS Rep?**

The two biggest changes have been in automation and FOCI [Foreign Ownership, Control or Influence]. When I was in the field, there were very few accredited IT systems and the ones we did see were small, standalone units. I remember being worried about disposing of ribbons that had been used to type classified documents. Now, we see many more accredited systems and many of them are very complex systems and networks.

The second change is the number of cleared FOCI companies in response to increased globalization. It used to be that the average IS Rep didn't deal with FOCI companies; the regional staff handled them. Now, almost every IS Rep and Information Systems Security Professional (ISSP) has to deal with a FOCI firm.

Both of these changes have resulted in a more complex working environment for our field personnel. It requires our folks to have more in-depth knowledge in a variety of areas, but particularly in IT.

## **How do you see the role of the IS Rep changing in this increasingly cyber oriented environment?**

I believe there will always be a need for IS Reps. Yes, there is an increasing focus on cyber and that will continue. But IS Reps are still needed to look at all aspects of a company's security operation to include classification management, personnel security, export control, etc. Our IS Reps are the primary interface with cleared industry, and I don't see that changing.

As far as training for IS Reps, I want to look at updating the FISL [Fundamentals of Industrial Security] training to better meet the changing workload.

# INDUSTRIAL SECURITY FIELD OPERATIONS

I would also like to leverage the SPeD [Security Professional Education Development program] certification program and eventually see a specialty certification for industrial security — both IS Reps and ISSPs — similar to the Adjudicator Certification Program. We also need to develop a specialized training program for ISSPs.

## **Are there any plans to hire more ISSPs?**

We recognize the need for more trained ISSPs and we're looking at a ways to achieve that. Over the past six months, ISSPs have been the number one hiring priority for Field Operations. In fact, as IS Reps have left the agency, most of those positions were backfilled with ISSPs.

One thing I want to do is to look at career paths for our ISSPs so they have their own progression for advancement. It concerns me that we only hire ISSPs at the GG-13 level, which is their journeyman level. I'd like to look at hiring more junior ISSPs, open up more growth opportunities for our ISSPs, and create a cadre of senior technical experts.

## **DSS has made many changes to how it conducts security assessments — the Facilities of Interest List (FIL), the security rating matrix and new terminology to name a few. Are there more changes on the horizon?**

We are going to continue to refine the security rating matrix. We are also going to continue to focus on findings and fixing the security vulnerabilities we find in industry. I think both changes were needed and have been pretty successful. We are still refining our cyber notification process and I expect that to continue. So we'll continue to refine and adjust our processes, but I don't see near-term major changes in how we do business.

## **In the past year, DSS has closed a number of smaller offices and consolidated the workforce. Are there plans to do more of this?**

We are constantly evaluating the workload in the field. My goal is to equalize the workload across the regions as much as possible. We may continue to consolidate offices as we move forward, but it will be in response to a shifting workload.

For instance, we have the highest concentration of facilities in the Capital Region and there's not much we can do to change their workload. We expect the workload to increase in the Huntsville area due to some government agencies moving as a result of Base Realignment and Closure.

So again, we will continue to adjust, but I don't expect any major realignments.

## **I understand Field Operations has established new objectives for the organization for 2013. Can you comment on them?**

We did establish objectives, and a new one is strategic communications. The headquarters must do a better job of communicating with the field workforce. We are looking at different methods and how we can leverage technology to better share information.

For instance, we're going to conduct some webinars for the field and we're going to increasingly rely on our video conferencing capabilities. I am open to other ideas from the field on how we can do a better job of getting them the information they need.

Another new objective is to expand on our government partnerships. I think the field has embraced the Director's partnership with industry, and we've made great progress in that regard. Now we need to focus on our government partners, at all levels including mine, to get to know them and let them know what we're doing to protect their information.

# NEW CDSE COURSES RECOMMENDED FOR COLLEGE CREDIT



Two courses offered by the Center for Development of Security Excellence (CDSE) have been evaluated by the American Council on Education's College Credit Recommendation Service (ACE CREDIT) and recommended for college credit. The courses are:

**Special Access Programs 2nd Tier Review (SA202.16)** – One semester hour in the lower-division baccalaureate/associate degree category

**DoD Personnel Security Adjudications (PS101.01)** – Four semester hours in the lower division baccalaureate/associate degree category

These courses are the second wave of CDSE courses to achieve this distinction. In early 2012, the following were recommended for college credit:

- Introduction to Special Access Programs (SAP)
- Facility Security Officer (FSO) Orientation for Non-Possessing Facilities
- Facility Security Officer (FSO) Program Management for Possessing Facilities
- Special Access Programs (SAP) Mid-Level Security Management

ACE CREDIT connects workplace learning with colleges and universities by helping adults access academic credit at colleges and universities for formal courses and examinations taken in the workplace or other settings outside traditional higher education. Each student completing a course will receive a certificate of completion from CDSE that includes the credit recommendation.

If a student is enrolled in a program of study at a college or university and they would like the institution to accept transfer of the credit recommendation, they must submit the request directly to that institution. The college has the option of accepting the ACE recommendation as a transfer and granting the equivalent college credits. An estimated 60 percent of colleges and universities in the United States adhere to ACE standards.

CDSE continues to pursue ACE recommendations for its course offerings.



# CDSE RELEASES SECURITY SHORTS

To address the need for short and tightly-focused topical training, the Center for Development of Security Excellence (CDSE) is producing training videos, also referred to as "shorts," that are usually 10 minutes or less. Security Shorts are engaging, high-interest training tools.

The award-winning trailer, "What are Security Shorts?" uses cheerful background music, vibrant colors and campy still images and narration to lightly spoof 1950s-style advertisements. This format grabs the viewer's interest while communicating the message that Security Shorts are a quick, effective resource.

Based on the community's response in a 2010 survey and feedback in course evaluations, CDSE had determined a need for the short video training format as an alternative to courses of broader scope and greater length. The short-format learning refreshes knowledge for topics included in both existing and new CDSE courseware.



"Security Shorts" also enable delivery of training to increasingly large populations of students worldwide. Security professionals, including Facility Security Officers (FSOs), security managers,

security specialists, and other interested personnel are able to learn new information, refresh their knowledge of a critical topic, or quickly access information needed to complete a job. Security Short topics span multiple security topic areas including industrial, information, personnel security, and special programs. The graphic below lists all shorts offered by CDSE.

The security community's response has also attested to the value of this training format. According to Yvette C. Gilyard, Norfolk Naval Shipyard Business and Strategic Planning Office Security Assistant and Department Security Coordinator, "I watched the 'Disposal and Destruction' short, and it was clear, concise, short and very easy to understand. I especially enjoyed the interactive capability providing an actual hands-on experience of performing a facility's annual clean-out day."


CDSE launched six Security Shorts in 2011, and based on the community's interest, added 25 more in 2012. Security professionals can access the videos at [www.cdse.edu/shorts/index.html](http://www.cdse.edu/shorts/index.html). The videos are not intended for download, but downloadable student guides accompany each video. CDSE has 10 additional Security Shorts in development for FY13.

**JPAS Series:** A series of four individual courses covering the roles and responsibilities of Joint Personnel Adjudication System (JPAS) user levels 2-3, 4-6, 7-8, and 10.





**Suspicious Emails:** Provides a quick reference for recognizing and mitigating suspicious emails.

**Industrial Security for Senior Management:** Reviews the Facility Security Clearance process, importance of the Facility Security Officer position and the role of Senior Manager.





**Downgrading & Declassification:** Gives practice on the thought process involved in calculating the classification downgrading and/or declassification instructions of a derivatively classified document.

**SAP Types:** Provides an overview of SAP types and categories.





**Requirements for OCAs:** Provides an overview of the changes for Original Classification Authorities (OCAs) resulting from the promulgation of Executive Order 13526.

**DoD Locks Approved to Safeguard Classified & Sensitive Materials:** Helps users recognize DoD-approved locks for safeguarding classified or sensitive information.

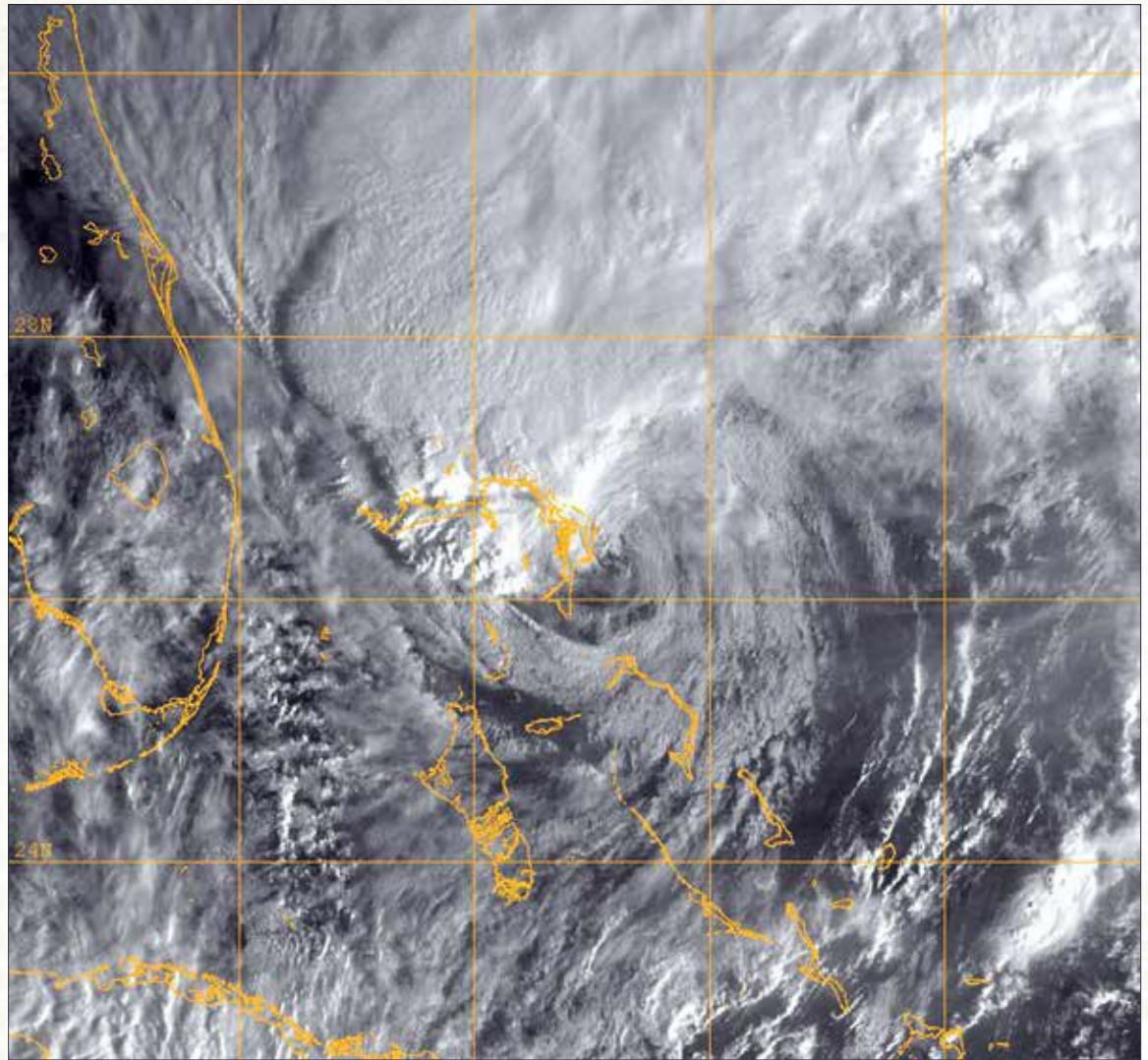


**DD Form 254:** Reviews the DD Form 254 and CDSE job aids and resources for completing and maintaining the form.

**Disposal & Destruction:** Reviews requirements for disposal and destruction of classified information per DoD Manual 5200.01, Vol. 3, "DoD Information Security Program: Protection of Classified Information."



**Adjudicative Guidelines Series:** A series of courses in a scenario-based format individually addressing one of 13 adjudicative guidelines to include concern, disqualifying conditions, and mitigating conditions.



## AN INFRARED SATELLITE IMAGE OF HURRICANE SANDY

**Oct. 26, 2012:** A GOES-13 infrared satellite image of Hurricane Sandy provided by the U.S. Naval Research Laboratory in Monterey, Calif., shows the storm at approximately 7 a.m. EST in the Atlantic Ocean.

*(U.S. Navy photo/Released)*



# SUPERSTORM SANDY

## POUNDS NORTHEAST OFFICES

**By Diane Craig**

*Mount Laurel Field Office*

On October 29, 2012, New Jersey and New York were hit with one of the worst storms in 100 years, Superstorm Sandy. This storm affected the Mount Laurel, N.J., and the New York Field Offices both in a professional and personal manner.

During the aftermath of Superstorm Sandy, although some DSS personnel were without power at times and some were on temporary duty, the entire Mount Laurel Field Office worked together to ensure the continued protection of classified information released to industry.

### **MOUNT LAUREL FIELD OFFICE**

The Mount Laurel Field Office, located in Mount Laurel, N.J., has cognizance over approximately 470 cleared facilities, and its area of responsibility includes New Jersey, Delaware, the Eastern Shore of Maryland and the Delmarva Peninsula area into Virginia. There are a

total of 16 personnel assigned to the field office — 13 are located at the Mount Laurel, N.J. location and three are located at a resident office in Parsippany, N.J.

As soon as the storm hit the area, all personnel were involved in preparing for the aftermath of the storm. Field office personnel were contacted by the field office chief to assure their safety and the safety of their families. Three personnel were en route to other DSS offices, as they were providing temporary support to other DSS field offices.

The Mount Laurel Field Office location was without power and phone service for two days, and the Parsippany Resident Office was without power for a week because the roads in the area were littered with downed trees and power lines.

When power was finally restored to the Parsippany Office, it took another two days to get the telephone

lines restored. In addition, several personnel lost power at their homes for an extended period of time.

Two personnel assigned to the Parsippany Resident Office were without power at their homes for a week and worked, under difficult situations, from locations near their homes which did have power, such as their local church or libraries.

## CLEARED CONTRACTORS

A mass e-mail was sent to all cleared contractors to determine if any were impacted by the storm, which could have affected their capability to safeguard classified information. In addition, field personnel contacted cleared facilities within the area, concentrating on those that have approved safeguarding capability, to include Freight Forwarder facilities that have approved supplemental controls, to determine the status of their controlled areas.

Most lost power for several days, and as a result, several contractors had to rely on cleared personnel to provide security oversight because Intrusion Detection Systems (IDS) were inoperable as a result of massive power issues. Although the facilities had back-up generators and emergency procedures in place, some of the generators ran out of gas. Due to severe gas shortages, the facilities, along with guidance from the field office, came up with alternative solutions to assure the continued protection of classified information.

"The effects of Superstorm Sandy were challenging, as well as devastating, to many areas under the cognizance of the Mount Laurel Field Office. However, the staff of the Mount Laurel Field Office worked diligently with the cleared Freight Forwarders and other cleared defense contractors to ensure that all classified material was properly safeguarded at all times," said Alice Kispert, Mount Laurel Field Office Chief.

"At times priorities had to change at a moment's notice," said Kispert. "But we understood we were all working together to oversee the DSS mission of overseeing the protection of U.S. and foreign classified information and technologies in the hands of industry under the National Industrial Security Program."

The warehouse location for two of the cleared Freight Forwarders is in Port Newark, N.J., which is located near the water and thereby sustained significant damage from the storm, as well as loss of power. Another cleared Freight Forwarder experienced power issues, which also affected their IDS and their backup generator ran out of gas.

At the time of the storm, none of the cleared Freight Forwarder facilities were storing any classified material. However, due to the power, water damage issues and generator issues, the safeguarding capability at these locations was temporarily removed until the issues could be resolved.

This action ensured that classified information was not sent to a location which could not provide adequate protection. The restoration of safeguarding capability took over two weeks to be completed.

## NEW YORK FIELD OFFICE

The New York Field Office was also affected by Superstorm Sandy on October 29. The New York Field Office is located in Westbury, Nassau County on Long Island, which is about 35 miles east of the two of the storm's most highly damaged areas, the boroughs of Queens and Staten Island.

There are approximately 270 cleared contractor facilities located between Staten Island, Brooklyn, Queens, Manhattan, Nassau and Suffolk Counties, which make up Long Island. The area is serviced by five Industrial Security Representatives and two Information Systems Security Professionals.

The major loss to the facilities in this area was from flooding and loss of power. No cleared contractor facility incurred serious losses, although some employees suffered losses to their homes and vehicles.

Before the storm hit, the New York Field Office ensured all employees were prepared to work remotely if the storm caused damage to the office. The planning and preparation proved beneficial as loss of power to the area was even greater than anticipated.

The Field Office was without power, telephone, and internet for five days and intermittently for another two. Almost all assigned personnel were without power at their homes for between two and 12 days. Three personnel were grateful to have purchased generators in advance of the storm, especially one hurricane "veteran" who purchased a propane generator knowing gasoline is in short supply after devastating storms.

Employees without generators were able to charge phones and computers at libraries, relatives' homes and one even ran extension cords to a neighbor's home that had a generator. The IS Reps also charged their Blackberries in their cars to ensure they could maintain contact with the office, their coworkers and cleared contractors. None





A warehouse utilized by a cleared Freight Forwarder company depicts the amount of damage along the Port of New Jersey. The packages in the photo do not contain classified information.



Residents of a Staten Island neighborhood look at properties destroyed by Hurricane Sandy. Homes will be removed because they are blocking street access. (Andrea Booher/FEMA)

*(Editor's Note: Information for this article was also provided by the Northern Region and the New York Field Office.)*

suffered any serious damage to their homes, just minor shingle damage and downed trees.

As soon as the storm ended, office personnel were on their Blackberries and computers, contacting all the cleared contractors to assess the level of damage to their facilities and ensure all classified information was safeguarded. Emails were sent to all facility security officers.

One IS Rep was commended by a major defense contractor in the area, as she drove her personal vehicle to their site within a few hours of the end of the storm to ensure the facility and its personnel were safe.

All of the facilities had plans in place and ensured all classified information was safe through the use of 24 hour guards, back-up generators, and transfer of classified to other cleared contractor facilities in the area.

## LESSONS LEARNED

"Many lessons were learned during this experience; the most important of which was the super planning we engaged in prior to the storm," said Marcella Beiling, New York Field Office Chief.

"The New York Field Office was well prepared," Beiling said, "and the personnel from the Resident Offices in Williamsville, Syracuse and Watervleit, N.Y., all rapidly stepped up to assist their coworkers in the Westbury location to ensure the security of the classified information located at affected cleared contractors at this location was secure."

"The Northeast is no stranger to significant natural disasters, and Superstorm Sandy had the most impact in recent memory primarily due to the strength and scope of the storm," said Mike Halter, director of the Northern Region.

"The people of the Northeast are resilient and the region will recover, but only after much hardship and expense," said Halter. "I was so proud of how the DSS family pulled together professionally and personally to take care of our families, neighbors, and responsibilities to national security."





# CHIEF FINANCIAL OFFICER

## WHAT IS THEIR ROLE?

**By Shana Dittamo**

*Industrial Policy and Programs*

DSS should carefully examine the principal players involved in a company's leadership to ensure protection of the industrial security program. One often overlooked member of a company's executive management team is the Chief Financial Officer (CFO).

DSS must determine which members of senior management need to have access to classified information. A thorough understanding of the CFO's responsibilities will help in making an informed decision whether to clear or formally exclude the company's CFO.

Historically, the CFO (or equivalent position) has been responsible for supervising and implementing a full and accurate set of accounting books, oversight and implementation of financial and audit control systems, monitoring the annual budget to include all subsidiary budgets, and coordination of the annual audit.

Today's CFO is still responsible for these functions; however, in many instances, the scope of involvement and influence over corporate management has expanded greatly.

The expansion of the CFO role in recent years was accelerated with the enactment of the Sarbanes-Oxley Act of 2002 (commonly referred to as SOX), which adds rigor and additional compliance measures to the reporting requirements of publicly held companies. The SOX was passed by Congress in response to a spate of corporate accounting scandals that were uncovered in 2001.

The financial markets and public were stunned as investigators revealed billions of dollars of fraud at massive companies such as Enron, WorldCom, and Tyco. The legislation expressly assigns responsibility to the CEO and CFO of publicly held companies to personally attest to, and certify the accuracy of the financial reports. This measure further entrenches the CFO in the company's highest echelon of management.

Due to their fiduciary role at the company, the CFO is required to engage in all activities contributing to the financial health and growth prospects of a company. According to a recent study by global executive search firm Spencer

Stuart, CFOs have emerged as key business partners to the CEO. They must balance regulatory compliance and accountability to the board and shareholders, with the procurement of valuable business prospects.

As CFOs spend more time on strategy, they must have the ability to clarify business models in order to take advantage of profitable business opportunities. CFOs evaluate and advise on long-range planning goals, the introduction of new programs and strategies, and their impact on the financial health and regulatory compliance of the company.

Operational duties of a CFO can include the oversight of a subsidiary

company's financial operations, the management of third parties to which functions have been outsourced, and the supervision of due diligence and negotiation of acquisitions. Additionally, today's companies have increasing multinational exposure and are dependent on foreign markets. Multinational operations bring a barrage of compliance issues and necessary expertise in risk management and international tax issues.

CFOs must also understand a host of essential drivers including sales pipelines, capital budgets, new competitors, currency movement and product placement in order to keep the company competitive in this increasingly global market.

Today's CFOs are deeply-rooted in the corporate decision process and may impact the direction of the company. This is why DSS may include an assessment of the authorities and actions of the CFO in the cleared company when conducting its industrial security oversight mission.

THE FINANCIAL  
MARKETS AND PUBLIC  
WERE STUNNED  
AS INVESTIGATORS  
REVEALED BILLIONS  
OF DOLLARS OF  
FRAUD AT MASSIVE  
COMPANIES SUCH AS  
ENRON, WORLDCOM,  
AND TYCO.

# FOCI OPERATIONS DIVISION

## AFFILIATED OPERATIONS PLAN

**By Erin Bruce**

*Industrial Policy and Programs*

Cleared contractors are becoming leaner and exercising synergies now more than ever, and sharing administrative and other internal services is an effective cost-cutting method for companies under Foreign Ownership, Control or Influence (FOCI).

However, shared administrative services have continually been a lengthy and confusing piece of the FOCI mitigation process. To assist companies, the FOCI Operations Division has developed a new product to help streamline this sometimes difficult process. The product, the "Affiliated Operations Plan" (AOP), was posted to the DSS website in early 2013 and solidifies guidelines for industry requests, procedures for internal processing, and techniques for annual review.

### THE GOAL

The primary goal of the AOP is standardization for all stakeholders. The template plan provides industry with DSS' expectation for affiliated operations requests in advance, reducing instances of unapproved affiliated operations, as well as the time it takes to acquire supporting information from industry after receipt.

Internal procedures, to include timelines and specified roles and responsibilities, will help DSS expedite processing of the plan responses. The requirement for a single plan, rather than numerous approval and disapproval letters, as well as assessment aids, will support efficient and consistent evaluation of the approved operations.

### THE PARTS

The AOP consists of three parts for each shared operation type: description; risks/risk mitigation; and assessment tools. The description section includes detailed information relevant for DSS to make an informed and risk-based decision. Dependent on the service type, some examples of potential data points in this section could include whether key management personnel (KMP) will be involved in the operations and whether IT will be implicated.

The risks/risk mitigation section is intended to detail the risks inherent in the provision of the service and how the company intends to mitigate that risk. DSS expects the Government Security Committee (GSC) to appropriately consider risks, and provide thoughtful and effective methods for reducing or eliminating them.





# CREATES NEW TOOL

## DESIGNED TO STREAMLINE THE MITIGATION PROCESS

Finally, in the assessment section, the company should propose methods for assessment of compliance with the risk mitigation strategies for the GSC and DSS. This section may include review of paperwork, interviews, visitation logs, demonstrations, etc.

However, DSS is not limited to the suggestions in AOP Section 3. Though the intent is to standardize the AOP process as much as possible, the operations themselves will differ from company to company, and it is critical that each service be reviewed in light of the circumstances at that facility.

As more operations are moving to electronic applications, DSS may often see similar software packages or service providers. However these programs are highly customizable and it is important to evaluate the relationships and information sharing in making a recommendation.

### THE BENEFITS

Additionally, DSS will likely see an increasing level of interdependence between the AOP and the Electronic Communications Plan. DSS Information Security Systems Professional (ISSP) and FOCI Operations Division personnel

will be collaborating closely on these plans to ensure consistency between both documents.

There are numerous benefits stemming from a formal AOP. Improved timelines can be expected because DSS is more likely to have the information necessary to render a decision up front. Also, negotiating a single document is a more streamlined technique than approving, disapproving, and requesting information via formal correspondence.

DSS can then use risk- based criteria for the evaluation of services, rather than attempt to maintain consistency based on few facts. Finally, the AOP should provide standardized evaluation of shared services during vulnerability assessments.

With the AOP template, the confusion surrounding shared services from all stakeholders should be significantly reduced. DSS expectations will be clearly spelled out, giving industry more flexibility in implementation options. Similarly, assessment techniques will be supported, enhancing the Industrial Security Representative's knowledge of each service, providing numerous mechanisms to assess any risks or concerns.





# THE IMPORTANCE OF PROTECTING CRITICAL

**By Robert Ayer**  
*Counterintelligence Directorate*

The advantage gained by a unique weapon system or advanced technology can be fleeting. Once the secrets of a system or technology are revealed, adversaries can copy it and/or develop countermeasures to mitigate the impact of the system.

One of the best examples of successful protection of critical program information (CPI) providing a decisive advantage on the battlefield is the case of "Greek fire." In fact, the protection of Greek fire's CPI was so effective that eventually the secret to Greek fire was lost.

Greek fire was truly a weapons system: it consisted of the incendiary mixture itself; the specialized galley (oared ship) called a dromon from which it was deployed; a device that preheated and pressurized the mixture; the siphon, a bronze tube through which the mixture was projected from the ship; and the specialized training of the sailors and operators on the ship.

The exact makeup of the mixture is unknown to this day, but it may have involved some combination of quicklime, calcium phosphide, naphtha, resin, and saltpeter. Not only did this

IN FACT, THE  
PROTECTION OF  
GREEK FIRE'S CPI WAS  
SO EFFECTIVE THAT  
EVENTUALLY THE  
SECRET TO GREEK FIRE  
WAS LOST.

mixture burn spontaneously while in flight and on contact, but even in water. The dromon would maneuver close enough that its pumps could shoot burning liquid onto the enemy ship and its crew.

The Byzantines strove to prevent others from learning about the technology. In order to keep the secret of the technology, they severely compartmentalized its CPI. The specialized knowledge needed for each part and step of the process was divided between the shipwrights who built the dromons







## PROGRAM INFORMATION: *A Historical Perspective*

and installed the special equipment; the ironworkers who made the cauldrons and the bronzeworkers who made the siphon tubes; the chemists who made up the mixture; and the operators who worked the weapons system at sea.

Along with protecting the system's secrets, they also protected the actual technology. The mixture was made up and stored at one central plant. From there it was issued to fleet commanders only when necessary. The onboard equipment for heating and pressurizing the mixture was installed below decks, away from prying eyes.

Just as the Byzantines recognized the importance of protecting its CPI, it is Department of Defense (DoD) policy to provide uncompromised and secure military systems to the warfighter by performing comprehensive protection of CPI through the integrated and synchronized application of counterintelligence, intelligence, security, systems engineering, and other defensive countermeasures to mitigate risk.

In the late seventh century, the Byzantine Empire stood as a bulwark against the aggressive Islamic forces. In 678, the caliph's armies and fleets were invading Constantinople, the capital of the orthodox Christian, Byzantine Empire, for the fifth year in a row. To break the siege, the Byzantine emperor

sent out his fleet, including the fire-bearing ships, and drove off the opposing fleet.

A generation later, in 717, the empire faced an even greater threat with the city again besieged by Arab forces. To defeat the Arab forces, the Byzantine forces held the invading army at the city walls while the defending fleet's Greek fire scorched the attacking ships. With their fleet burned, the fighters invading the city fled.

Greek fire was used remarkably little beyond this crucial historical juncture. Over the centuries, Byzantine forces lost many other naval encounters yet did not deploy Greek fire, even though it might have turned the tide of battle. Despite the effectiveness of Greek fire as a weapons system, the complicated nature of the technology and the desire to keep it secret meant that any break in the chain of transmission of CPI by any of the key groups of knowledge workers would lead to the breakdown of the whole system.

The Byzantines learned the hard way that failure to apply consistent protection of CPI may result in the loss of confidentiality, integrity, or availability of CPI, resulting in the impairment of the warfighter's capability and technological superiority. Put simply, the Byzantines eventually forgot how to make and use Greek fire.





# BAD BURN RUN

### WHAT HAPPENED:

A cleared contractor employee left several burn bags containing classified information unattended and in plain view in a public area after attempting to take the bags to a destruction facility. The investigation revealed that the contractor had not been properly briefed on safeguarding responsibilities as a courier and had never been issued a courier authorization card/memorandum.

A Government Contracting Activity (GCA) notified DSS of a security violation committed by a contractor employee supporting the GCA on the government site.

Security guards in a public parking garage co-located with the GCA were alerted to a vehicle in the garage that had its trunk open, with what appeared to be seven brown paper bags with red strips, commonly associated with classified material. Upon investigating, security guards ran the license tag of the vehicle and found it was owned by a contract employee who supported the GCA.

The security guards took possession of the burn bags and notified the GCA. The employee works as a mail courier for the GCA. His duties include handling unclassified and classified mail and transporting burn bags containing classified information from the government work site to a separate government destruction facility.

When questioned by security personnel, the employee stated he had placed the burn bags in his personally owned vehicle (POV) while he looked for an item in his vehicle and forgot to retrieve the burn bags. Security personnel for the GCA returned the burn bags to the employee and allowed him to complete the burn run.

### WHAT WE LEARNED:

The employee attempted to make the burn run earlier in the day, but discovered the destruction facility was not accepting burn bags at that time.

He returned to the parking garage at the GCA's location and realized his wallet was missing. He first looked in the government vehicle and when he couldn't find it there, he returned to look in his POV.

The employee placed the burn bags in the open trunk of his POV, looked for his wallet and then returned to his office leaving the burn bags unattended. Security guards later found him in his office after determining the bags were in his POV.

The incident highlighted the fact that the GCA did not have standard operating procedures in place for conducting burn runs; did not conduct training on the proper handling of classified material for its employees; did not issue courier cards; and did not have a process or tracking mechanism for transporting classified material to the destruction facility.

It also revealed that the destruction facility did not have logs or tracking mechanisms in place for the receipt of classified material for destruction. The GCA agreed to put procedures in place as a result of this security violation.

### RESULTS:

The facility conducted an administrative inquiry and found no compromise of classified information.

DSS disagreed with this finding and concluded that this was a suspected compromise of classified information, and the employee was culpable.



DSS assisted the facility in addressing training and procedures for the transmission of classified information. The employee received the appropriate training and was issued a letter (equivalent to a courier card) authorizing him to transport classified material.

## **SECURITY EDUCATION, TRAINING AND AWARENESS:**

An effective security education, training and awareness program is the key to ensuring situations like this don't occur at your facility. There are resources available to assist you.

The DSS Center for Development of Security Excellence (CDSE) offers courses and video overview (listed at right) to help cleared employees better understand their responsibilities as they relates to the proper handling, transmission and destruction of classified information.

### **Safeguarding Classified Information in the NISP (IS109.16)**

[www.dss.mil/cdse/catalog/elearning/IS109.html](http://www.dss.mil/cdse/catalog/elearning/IS109.html)

**Course description:** This interactive Web-based course (approximate run time is 2.5 hours) covers rules and procedures for protecting classified information and material in the National Industrial Security Program (NISP).

Course content is derived primarily from the National Industrial Security Program Operating Manual, DoD 5220.22M, Ch. 5.

Lessons cover requirements and procedures for safeguarding classified information including requirements for control and accountability, storage, disclosure, reproduction, and disposition of classified information.

### **Transmission and Transportation for Industry (IS107.16)**

[www.dss.mil/cdse/catalog/elearning/IS107.html](http://www.dss.mil/cdse/catalog/elearning/IS107.html)

**Course description:** This eLearning course (approximate run time is two hours) examines the requirements and methods for transmitting or transporting classified information and other classified material in accordance with NISP requirements.

Lessons explain policy, documentation, preparation, dissemination requirements for specific types of information, and authorized transmission and transportation methods.

### **Disposal and Destruction Security Short**

[www.dss.mil/cdse/shorts/information-security.html](http://www.dss.mil/cdse/shorts/information-security.html)

**Course description:** This Security Short (approximate run time is 10-15 minutes) provides an overview of the requirements for disposal and destruction of classified information as addressed in DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information."

Identifies what types of classified information are authorized to be destroyed, why classified information must be destroyed, who is authorized to destroy it, when it must be destroyed, and the methods available for its destruction.

For assistance with CDSE security education, training or awareness products please contact [industrialsecurity.training@dss.mil](mailto:industrialsecurity.training@dss.mil).

# REGIONAL IT PROJECT MANAGERS



CONNECT THE FIELD

WITH A NEW LEVEL

OF IT SUPPORT

In years past, when a representative of the Office of the Chief Information Officer (OCIO) briefed at the regional all-hands conferences, a barrage of questions and complaints followed the presentation. Often, the OCIO didn't know about these systemic issues because field leadership didn't know who in the OCIO to contact for help.

The OCIO leadership seized the opportunity to improve and reassigned government employees to serve as Regional IT project managers. Each of the four project managers (representing each DSS region) maintain full awareness of operations in their regions and serve as main points of contact for projects and the IT enterprise. They also serve as the customer advocates for the regions and ensure issues get the attention they deserve.

"We're here to interact with the field and be a liaison," said Matthew Powell, Chief of IT Field Operations and Capital Region Manager. "We track requests, meet constantly with OCIO leadership, and keep the regional leadership updated on efforts and projects in their respective areas."

"Our goal is to make sure everyone has what they need to accomplish the mission," Chris Bowman, Western Region Manager, added.

Feedback from the field has been extremely positive. "We're told that having one person to contact has made it a lot easier

on the field," said Matt Kroelinger, Northern Region Manager. "We sit down, hear their concerns, and are able to route them through the proper channels to resolve issues in a quick manner. Without the field worrying about their IT and telecommunication systems, they are able to focus more of their time on the DSS mission.

"During these discussions, we'll help clarify the needs, and formalize the requests," Marcus Evans, Southern Region Manager, added.

One major project currently underway is the SIPRNet to the field project, which will eventually provide robust, reliable, and secure SIPRNet communications at 26 DSS field locations. Together with Luis Garcia, the OCIO SIPRNet project lead; the DSS Security Office; and the Support Services Division (SSD),



**THE REGIONAL IT TEAM IS:**

**Chris Bowman** – *Western Region Manager*  
**Marcus Evans** – *Southern Region Manager*  
**Matt Kroelinger** – *Northern Region Manager*  
**Matthew Powell** – *Chief of IT Field Operations and Capital Region Manager*



the regional IT managers have had their hands full. Some of the many tasks involved in the project include:

1. Gathering construction, security, and IT requirements from each field office to get the space ready for Secret Open Storage.
2. Installing the new high performance external connections needed before SIPRNet can be deployed to the office.
3. Ensuring all construction, security, and IT requirements are successfully completed so the space can be accredited.
4. Deploying the necessary network, desktop, and printer equipment at each site.
5. Providing training and in-person assistance with the new systems.

“The initial investment will pay huge dividends in the end,” Bowman said.

Matt King, Deputy Chief of Support Services said, “A project of this caliber takes tremendous teamwork and coordination between not only internal stakeholders but external stakeholders. Moreover, constant communication with the customer is a must, and OCIO, in particular, Luis Garcia, who is the point man for this project, has done a superb job keeping the customer informed.”

“The physical security team has been working countless hours along with OCIO, and SSD ensuring each field office location is positioned to support DSS customers” said Chief of Security, Timothy Harrison. Security specialist Angelo Reece added: “This will forever enhance DSS’ footprint and capability to process classified information within a controlled environment.”

Western Region Director Karl Hellman said “The SIPRNet to the Field Project will bring much needed capability to DSS field elements. The project is another step toward fully integrated IT systems for all DSS personnel. This project directly aligns with one of highest priorities, cybersecurity.”

Another initiative benefitting the field is Video Teleconferencing (VTC). This capability wasn’t reliable or widely available at DSS until two years ago. Within the last year, a new infrastructure has been installed and accredited, and the use of VTC “has exploded,” said Powell. “The regional offices are holding weekly meetings with the field offices via VTC, and we’re seeing approximately 75 calls a day.”

“It’s become another means of communication, and a life-line to the many offices,” added Kroelinger. The SIPRNet to the field project and VTC communication expansion are just some of the projects that the regional IT project managers have been supporting.

Since the introduction of regional IT project managers, the annual all-hands conferences have a different outcome. Compliments and thanks for a job well done have replaced the questions and complaints.

“We collaborate with every office in the agency,” Powell said. “Teamwork is crucial to our success, as we’re dependent on everyone else. It’s a huge team effort.”



John Morrow (left), Senior Industrial Security Representative, receives IT assistance from Justin Milum (right), as Chris Bowman looks on, at the OCIO Help Desk during the Southern/Capital Region All Hands Training Workshop in April 2012.



# DSS OFFICE OF INNOVATION:


The world is changing, and changing fast. While we know that change is prevalent, we cannot predict the specific issues, threats, or challenges that will require DSS to adapt, nor how DSS employees will have to adapt. So how is DSS preparing to meet these uncertainties?


The Office of Innovation was created for just this purpose: To help DSS continue to meet its mission in the face of uncertainty. This office will enable DSS to remain proactive in meeting all of its assigned responsibilities by developing insight into future needs and capabilities of DSS, and promoting the right initiatives, knowledge, capabilities, methods, and tools to help DSS meet those needs.

One of the most important roles of the office is to listen carefully and leverage the extensive knowledge and specific needs and responsibilities of the entire agency to inform our work. The Office of Innovation held its inaugural Design Forum Workshop on Nov. 14, 2012, and welcomed a diverse group of over 30 representatives from all facets of the organization to explore the future operating environment. To envision that environment, the Office of Innovation applied the Scenario Planning approach to examine the nature of the security threats facing government and industry partners and DSS missions to assist them in protecting our nation's secrets and technology.

Scenario planning is a proven approach to look to the future not as a matter of making predictions but rather by examining possibilities. It is a wide-ranging, intellectually stimulating exercise in large-scale "what-if" situations that gives the participants deep and compelling insight into the future, and exposes risks and possibilities that might otherwise remain hidden. By considering topics such as cyberwarfare, terrorism, changing technologies, energy security, and industrial espionage, the Office of Innovation gained a deeper insight into the methods and capabilities that DSS must develop going forward.

The workshop yielded themes and recommendations across a wide range of issues including:

 Workforce development is essential to ensuring DSS future capabilities. The entire workforce must be engaged in continuing to develop their own abilities across the full scope of our mission.

 DSS tools and technology must continue to rapidly evolve and keep pace with a dynamic external environment. Administrative tasks must be simplified and technologies such as data analytics and integration must be applied to leverage the uniquely human skills of judgment, acumen, and decision-making.

## >> AT ATTENTION!

# DSS OFFERS CISSP BOOT CAMP

**By Selena Hutchinson**  
*Industrial Security Field Operations*

The Office of the Designated Approving Authority (ODAA), Industrial Security Field Operations, is providing the opportunity for DSS candidates to participate in a Certified Information System Security Professional (CISSP) Boot Camp and take the certification examination.

Richard Lawhorn, Director of Field Operations, has made technical training and hiring Information Systems Security Professionals (ISSPs) top goals for his directorate.

"This CISSP Boot Camp training is just one of the initiatives we have planned for FY13 and FY14," he said. "My aim is to

provide our personnel with top-of-the-line technical training and keep pace with the ever changing cyber environment."

The first course offering is scheduled for March 2013 followed by a September 2013 class. There are two additional boot camp offerings planned in 2014.

The CISSP is the premier credential in the field of information security, accredited by the ANSI (American National Standards Institute) to ISO (International Standards Organization) Standard 17024:2003. CISSP certification is not only an objective measure of excellence, but a globally recognized standard of achievement.

According to Randall Riley, ODAA, locally sponsoring a CISSP



# DESIGN FORUM KICKS OFF NEW INITIATIVE

- ⚡ Potential changes to the DSS mission must be anticipated, and to the extent practicable, planned for.
- ⚡ DSS must develop a surge strategy to adjust quickly to changing or new requirements in the event that unexpected threats emerge.
- ⚡ DSS needs to explore the concept of simulation and virtual world modelling for both threat assessment and capability development.
- ⚡ DSS will continue to examine human capital dimensions including telework, dynamic staff allocation, recruiting, retention, and training and development.

The above highlight the range and depth of the dialogue. It was a significant learning experience for the Office of Innovation team, and hopefully for all of the participants as well.

The workshop concluded with a strong shared understanding of the importance of preparing for the future, and the key role that the Office of Innovation can and will play in this essential task as DSS enhances its ability to anticipate future needs – improving its ability to manage our agency strategically and proactively. Over the coming months, the Office of Innovation will use the insights developed in this workshop, interviews,

and a survey to gather broad-based input from the DSS workforce to produce an integrated Innovation Master Plan that will guide its major programs and initiatives.



Heather Green (left), Industrial Security Field Operations, Scott Hill and Adele Clagett, both from the Center for Development of Security Excellence, provide input during a team activity at the inaugural Office of Innovation Design Forum Workshop.

## Course Description and Overview

The DSS Boot Camp course was contracted to the (ISC)2 CISSP Training Camp vendor. The company's seven-day CISSP program is the only all-inclusive boot camp endorsed by (ISC)2 to familiarize students with the CISSP Common Body of Knowledge and prepare them for the official CISSP examination.

This blended-learning course employs outcome-based delivery that focuses on preparing students with the real-world skills required to pass the CISSP exam and hit the ground running in their career.

Through lecture, lab work, and group discussion, students will learn the following 10 domains: Information Security Governance and Risk Management; Application Security; Business Continuity & Disaster Recovery Planning; Operations Security; Legal, Regulations, Compliance & Investigations; Security Architecture & Design; Telecommunications & Network Security; Access Control; Physical (Environmental) Security; and, Cryptography.

boot camp and certification test will, in many instances, lessen travel and training costs for DSS personnel who would otherwise take the class individually at locations throughout the country.

A centralized course offering will ensure consistent training and enhance the likelihood of employees passing the required exam on their first attempt. Further, candidates are able to take their examination closer to home, saving both time and money.

DSS information assurance personnel, personnel assigned to the Office of the Chief Information Officer, as well as ISSPs, are required to obtain and maintain CISSP certification consistent with DoD 8570.1M Information Assurance Workforce Improvement Program (IA WIP). The CISSP certification also meets compliance with the Federal Information Security Management Act.

# DSS MOVES OUT WITH DEFENSE AGENCIES INITIATIVE

**By Dee Marlow**

*DAI Program Manager, Financial Management Division*

The Financial Management Division is pleased to announce the successful deployment of the Defense Agencies Initiative (DAI) at DSS. DAI is an enterprise resource planning tool that provides a fully integrated budgeting, accounting, and mission capability and allows the flow of resource information between business functions inside the agency.

DAI is intended to transform the budget, finance, and accounting operations of the Defense Agencies to achieve accurate and reliable financial information in support of financial accountability. It is also designed to provide effective and efficient decision-making, modernize financial management capabilities and achieve auditable financial systems.

"The DAI is a leap forward for DSS in planning, executing, accounting for, and analysis of its resources," said Barry Sterling, DSS Chief Financial Officer and director of Business Enterprise. "In prior years we used accounting tools that required a lot of manual intervention to produce an output that was only basic required information. DAI will now allow us to have documented and repeatable processes that increase the reliability of information."

DSS is the eighth agency to fully deploy the DAI suite of systems; an effort that required the Financial Management Division to cleanse and convert close to 3,000 transactions, train more than 80 new system users, realign roles and responsibilities, and re-engineer related business processes.

The DSS legacy operating environment included over 12 outdated, disparate financial systems that required manual intervention from the staff in order to maintain financial operations. DAI integrates and automates these otherwise manual processes into a transparent, lifecycle-based environment which allows the staff to better analyze financial information for decision making.

The DAI system actually consists of six fully integrated business modules; the first and most significant of which is the DAI Timekeeping system deployed in August 2011.

During the deployment, DSS expressed its commitment to automation by becoming the first defense agency to pass a multi-phased system acceptance testing in the first phase, allowing the agency to implement the new system ahead of schedule. The DAI Timekeeping system has also streamlined a largely paper-based timecard process with a CAC-enabled, self-service, web-based system.

Through the DAI Business Intelligence module, program managers have the ability to view the impact of financial transactions on a program's performance and determine the status of those transactions across its lifecycle. This feature provides the program manager with the real-time program performance data needed to proactively manage program resources and more specifically review obligation and execution rates against prescribed budget targets and spending plans.

The module also includes a "dashboard" that provides graphical views of transactions as they occur and summarizes this data into the prescribed formats needed for analysis and reporting.

The DAI Cost Accounting module provides agency program managers with a mission-focused view of financial performance not available to them with legacy systems, where resources are grouped into projects aligned to program requirements.

"Not only do we achieve a savings in processing time using DAI, but we obtain data that we can better analyze to help increase the bang for the buck of each precious resource," Sterling said. "Repeatable processes and accurate accounting systems now provide DSS the capability to attest to the American taxpayer that we are good stewards of their tax dollars and through better analysis make more informed decisions to get more out of each dollar."

The DAI deployment has also allowed the agency to eliminate financial management material weaknesses and deficiencies, and improve financial management business processes. Planned enhancements to the DAI system include fully-integrated procurement, acquisitions, and budget formulation modules.



WHO'S WHO  
IN THE NISP?

NISPPAC?

**By Keith Minard**

*Industrial Policy and Programs*

All organizations and programs have acronyms and buzz words unique to them that can be difficult for the newcomer or outsider to understand. The National Industrial Security Program (NISP) is no different and is replete with its share of acronyms. In this column, we decipher the National Industrial Security Program Policy Advisory Committee or NISPPAC and its role in the NISP.

The NISPPAC was created on January 8, 1993 under Section 103 of Executive Order 12829, "National Industrial Security Program." It is comprised of government and industry representatives and is responsible for recommending changes in industrial security policy through modifications to Executive Order 12829, the implementing directive, and the National Industrial Security Program Operating Manual.

The NISPPAC advises its chairman, the Director of the Information Security Oversight Office (ISOO), on all matters concerning the policies of the NISP, to include recommending changes to those policies, and serves as a forum to discuss policy issues in dispute. ISOO is responsible to the President for policy and oversight of the Government-wide security classification system and the NISP.

The members of the NISPPAC are representatives from those departments and agencies most affected by the NISP, as well as non-government representatives of companies involved with classified contracts, licenses, or grants. The NISPPAC membership includes 16 representatives from executive branch agencies (including the chairman) and eight representatives from cleared industry. All members are nominated by their government agency or through industry recommendation to the NISPPAC chairman, who then appoints them to four year terms of service. The NISPPAC meets at least twice a year at the discretion of the chair and its meetings are open to the public.

The NISPPAC uses a working group process that enables both government and industry members to participate in program review and problem solving activities that are reported to the NISPPAC.

Current working groups are addressing issues related to personnel security clearances, the certification and accreditation of information systems, Special Access Programs, updates to the NISPOM and the DD Form 254, as well as industry implementation of the information sharing and insider threat standards established under Executive Order 13587.

These NISPPAC working groups have been instrumental in addressing issues of critical concern to industry and for recommending policy changes that enhance operation of the NISP. Reports of NISP and NISPPAC activities are included in ISOO's Annual Report to the President, which is available on the ISOO website at <http://www.archives.gov/isoo/>.

Further information concerning the NISPPAC's charter and bylaws, meeting minutes, and contact information for its members is available on the ISOO website.

*(Editor's Note: The original source for the above information is the Information Security Oversight Office website.)*

**Current Government Members:**

*Information Security Oversight Office*

- Central Intelligence Agency
- Defense Security Service
- Department of the Air Force
- Department of the Army
- Department of Commerce
- Department of Defense
- Department of Energy
- Department of Homeland Security
- Department of Justice
- Department of the Navy
- Department of State
- National Aeronautics and Space Administration
- National Security Agency
- Nuclear Regulatory Commission
- Office of the Director of National Intelligence



# FACILITATING PARTNERSHIP THROUGH EFFECTIVE COMMUNICATION

By John Massey

*Industrial Security Specialist, Crystal City Field Office*

Continuous interaction with industry through effective communication is key to facilitating a partnership between DSS and cleared industry. In that vein, DSS launched a number of initiatives in 2012 designed to foster better understanding and communication.

Emails from Industrial Security Specialists or Field Office Chiefs are designed to alert industrial security personnel and facility security officers of changes in DSS representation, current or forthcoming DSS initiatives, and topics that may be relevant to a specific field office or area.

In June, DSS announced its Triage Outreach Program which was designed to maintain communication with industry between assessment visits. Because DSS must maintain accurate data on cleared facilities as part of its oversight role, regular communication is necessary to help detect and mitigate vulnerabilities and assist facilities in building robust security programs.

The Partnership with Industry (PWI) Program has achieved great success through 12 one-week exchanges between DSS and industry partners. There are 10 active industry partners in the program that is designed to increase the level of awareness of DSS employees with issues faced by industry while also allowing industry personnel to work closely with DSS employees.


In addition to these initiatives, the DSS website is regularly updated with news that may be of interest to industry. DSS personnel actively support professional organizations by serving as guest speakers on changes within the agency or on specific topics, such as the DSS security rating matrix and counterintelligence.

For industry representatives, in particular new Facility Security Officers, the suggestions at right are a few avenues to help you better communicate with DSS.

DSS success is dependent upon industry's success. We both have the same ultimate goals: protecting the warfighter, safeguarding classified information and detecting and mitigating vulnerabilities. Through effective communication, DSS and industry can create a spirit of partnership that allows both to be successful, achieve our goals, and accomplish the mission.

## **Self-Inspections:**

Be proactive in communicating your self-inspection planning and results. Establish a dialogue with your DSS representative before and after your self-inspection. Consider sharing your self-inspection results with DSS and communicate any issues or concerns that you may have encountered.



**Advice and Assistance:**

Have a question? Facing a unique or complex issue that you have not encountered before? Reach out for guidance from your IS Rep or local field office. They are ready to help!

**Reporting Changed Conditions:**

Change is inevitable. Is your facility moving? Did you receive a new contract that now requires safeguarding? Has your company been purchased? Is a member of key management leaving? These, along with other conditions, are all required to be reported to DSS. Some of these changes may affect a facility clearance. When you are made aware of any upcoming change, approach your IS Rep early and often so there is a full awareness on both sides as to the change that is to take place and the status of the change as it occurs.

**Security Education and Training:**

Reach out to your IS Rep and discuss Center for Development of Security Excellence (CDSE) courses that may benefit you. If you are developing a security briefing, feel free to share it with your IS Rep for suggestions.

**Security Violations:**

Has an incident occurred at your facility that may constitute a security violation? Is this the first time you've encountered a violation or infraction? If so, contact DSS. We can help you with the violation process and provide guidance, which will help investigate and mitigate any vulnerabilities or security concerns. When security incidents occur that involve a loss, compromise, or suspected compromise of classified information, report this information to DSS as quickly as possible.

**Pre-Assessment Preparation:**

As you prepare for your DSS security vulnerability assessment, you may encounter problems or issues that you may not have enough time to correct or may leave you perplexed. Work with your IS Rep to address these items before the assessment. Often, an IS Rep will request this information in advance. While you are not required to provide it, doing so helps ensure adequate preparation for the assessment and to allow the IS Rep to tailor the assessment to the facility.

# VIRGINIA BEACH FIELD OFFICE

Since his arrival at DSS, Stan Sims, DSS Director, has made outreach to and partnership with cleared industry and government stakeholders a priority for the agency.

Each office has its own unique approach to implementing Sims' vision. For the Virginia Beach Field Office, it was an Open House held on Dec. 19, 2012. The office moved to a new location in the Town Center area of Virginia Beach, Va., in May 2011, and decided to open its doors to its industry and government partners within their geographic area.

Approximately 160 attendees visited, including Facility Security Officers (FSOs) and corporate management officials, government security personnel and the local law enforcement/counterintelligence community from as far away as Charleston, S.C. (approximately seven hours away from the Field Office). Another group of FSOs joined together to visit from Charlottesville, Va.

"The Open House was an example of partnership with industry at its finest," said Braden Harrison, Industrial Security Representative. "Not only did it allow us the opportunity to interact with our FSOs outside of an assessment, it also allowed us to interact with FSOs outside of our primary work area and to share ideas, discuss issues and gain additional perspective. It also allowed FSOs to talk among themselves, trade knowledge, and possibly be a resource for each other in the future."

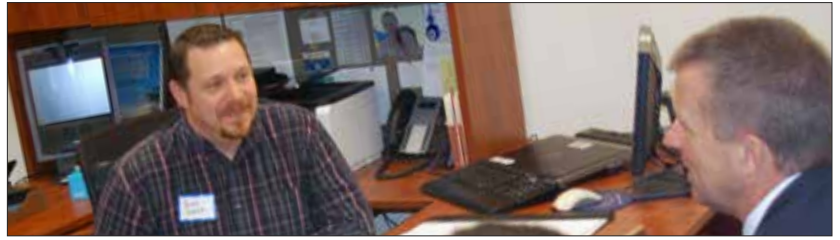
In addition to the tours of the office and peer-to-peer exchange, contact information and business card swaps were encouraged, as many of the attendees were new to the National Industrial Security Program. "The Open House was a rewarding experience for all of us," said Virginia Beach Field Office Chief Beth Whatley. "It was great to see how the Virginia Beach team worked together to organize the event!"



**LEFT:** Members of Alexandria Field Offices 1 and 2, from left, Matt Roche, Brian Linnane, Linda Crossman and Mike Irvine, volunteered at a Habitat for Humanity project. **RIGHT:** Brian Linnane helps frame part of the house.



# OPENS ITS DOORS TO INDUSTRY



## HELPING HABITAT FOR HUMANITY

### ALEXANDRIA FIELD OFFICES LEND SUPPORT

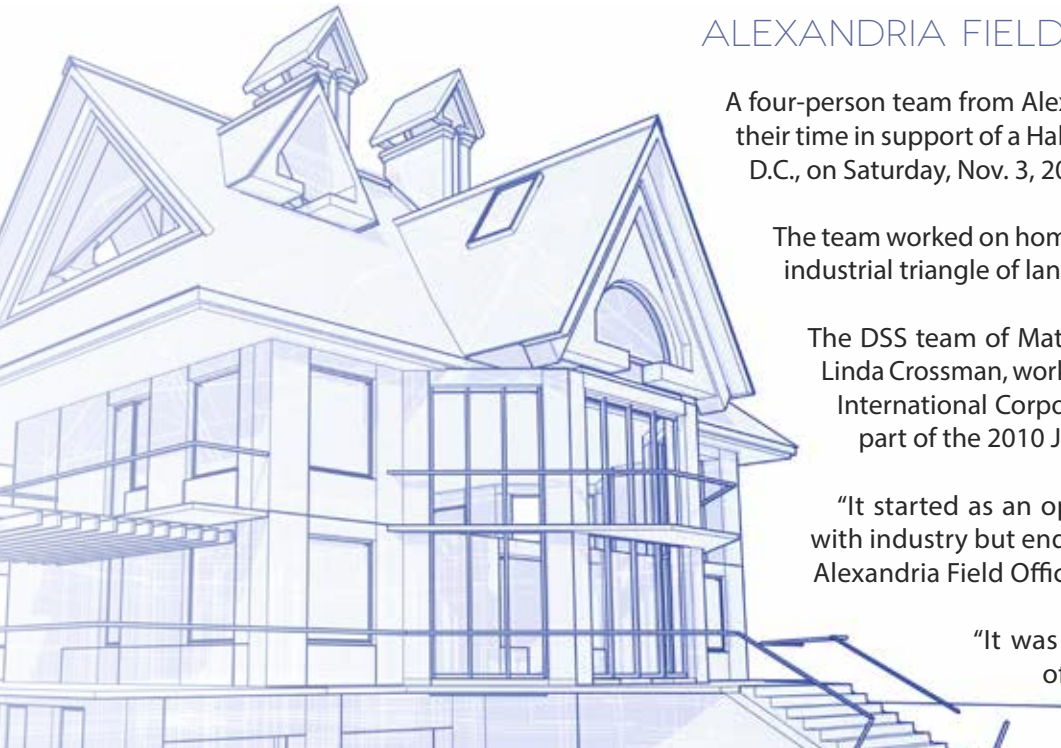
A four-person team from Alexandria Field Offices 1 and 2 volunteered their time in support of a Habitat for Humanity project in Washington, D.C., on Saturday, Nov. 3, 2012.

The team worked on homes in the Ivy City neighborhood, a largely industrial triangle of land in the Northeast quadrant of D.C.

The DSS team of Matt Roche, Brian Linnane, Mike Irvine and Linda Crossman, worked with members of Science Applications International Corporation on the renovations of homes as a part of the 2010 Jimmy & Rosalynn Carter Work Project.

"It started as an opportunity to enhance our partnership with industry but ended up being so much more," said Roche, Alexandria Field Office 1 Chief.

"It was such a privilege to work the building of a home that would ultimately end up fulfilling a family's dream to have a safe and comfortable place to live."



# DEFENSE SECURITY SERVICE

