

DSS ACCESS

OFFICIAL MAGAZINE OF THE DEFENSE SECURITY SERVICE

Volume 3, Issue 4



OCIO DEVELOPS LONG-TERM STRATEGY **TO SUPPORT FIELD OPERATIONS**



WINTER 2014

Volume 3, Issue 4



SPOTLIGHT

Office of the Chief Information Officer Develops Long-Term Strategy to Support Field Operations	4
---	---

Inside

Tiger Team Seeks to Bridge the Gap Between Directorates	6
A Day in the Life of ... An Industrial Security Representative	7
CI Enhancements: A Results-Oriented Measurement	8
First Virtual DoD Security Conference Spans the Globe	12
DSS Hosts Training for Information Assurance Professionals	13
DSS Kicks Off Phase II of the National Industrial Security System	14
DSS Counterintelligence Partners with Industry to Mitigate Foreign Intelligence Threats	16

Ask The Leadership

A Q&A with Karl Hellmann, Regional Director, Western Region	10
---	----

Deciphering the Acronym

What is a PCL?	17
----------------------	----

Around the Regions

Capital Region Stands Up New Field Office	18
DSS Cybersecurity Operations Division Receives DoD Award	18
Unique Program Grows Leaders Through Hands-On Training	19
Counterintelligence Integration in the Field Office: Best Practices from the Andover Field Office	20
Field Operations Director Retires After 30 Years of Service	21
DSS Helps Feed Families During Sixth Annual Campaign	22

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



Anyone who has heard me speak or read the pages of this magazine knows that I view partnership with industry as key to the success of the National Industrial Security Program (NISP). Inherent in this partnership model is the acknowledgement on the part of industry that each cleared individual and facility has primary accountability for securing the assets in their possession. Industry should also engage actively with and demand government support.

On the other side of the equation, DSS cannot be a reliable, consistent partner without maintaining a professional DSS field workforce. The DSS field workforce is the first, and in many cases the only, interface with cleared industry. In the pages of this issue of the ACCESS, you will see a number of internal initiatives we have taken to strengthen and support the field from a number of DSS offices.

The cover article addresses automation concerns and demonstrates a new partnership between Field Operations and our Office of the Chief Information Officer (OCIO) to address them. As the saying goes, you can never judge people until you have walked a mile in their shoes. Our OCIO has always been committed to providing outstanding support to the entire agency but, until they had visited some of our remote locations and seen firsthand the challenges our Industrial Security Representatives, Information Systems Security Professionals and Counterintelligence Special Agents experience on a daily basis, they were not able to help.

Our Industrial Policy and Programs directorate also recognized the need to better understand the needs of our field personnel and in a survey, asked how they could be more effective. Then they sent teams to the field to follow-up and talk to people. This "Tiger Team" initiative has eliminated barriers between the two directorates, and fosters a better understanding of their respective missions and how best to support the field, industry and the NISP.

You will also notice a heavy Counterintelligence (CI) emphasis in this issue as we highlight a number of CI initiatives to look internally at best practices and also better partner with industry. The most visible example is the new CI enhancement to the Security Rating Matrix. By elevating CI to a separate enhancement, it clearly demonstrates the value DSS places on the program and CI awareness.

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



OFFICE OF THE CHIEF INFORMATION OFFICER

DEVELOPS LONG-TERM STRATEGY TO SUPPORT FIELD OPERATIONS

by Beth Alber
Office of Public and Legislative Affairs

To increase awareness of the information technology (IT) needs of DSS employees working in field locations, the Office of the Chief Information Officer (OCIO) took two actions — it created the position of Business Relationship Manager (BRM) and then deployed individuals to observe the field in action.

The goal is to develop a long-term strategy that outlines how OCIO can help field personnel perform their part of the DSS mission and to have an advocate at DSS headquarters to be able to assess needs, research solutions, and have it included as a strategic initiative.

“This effort really brings IT closer to the crux of the DSS mission and ensures that IT is responsive to not only today's needs, but those that will make the agency successful in the future as well,” said Kevin Baker, Chief Technology Officer and chief of service design within OCIO.

“This provides us a better understanding of the day-to-day needs of our mission partners in the field,” said Christopher Bowman, Western Region BRM. “It also



allows us to start working on the requirements earlier, which in turn speeds up the process.”

Each of the four DSS regions has a dedicated BRM who acts as a liaison between OCIO and field personnel. Originally the BRMs were known as Regional IT Project Managers, whose sole responsibility was to maintain awareness of ongoing projects. But with the new title came a new focus.

“These new positions are more focused on finding technologically efficient solutions to resolve an issue voiced by the field vice physically maintaining awareness of a project,” said Marcus Evans, Southern Region BRM.

“Plus, each region now has an advocate at headquarters who they can reach out to,” said Bowman. “We can honestly tell them whether a proposed solution can help or if there is a better approach to take.”

The open communication was originally cultivated by the BRMs while working with the field on the “SIPRNet to the Field” project, but on a more superficial level than where they are headed now.

“We’re leveraging the relationships we built as project managers and working to deepen the partnership between the OCIO and the field,” said Matt Kroelinger, Northern Region BRM. “That way, we get a better understanding of what they’re doing and can determine the level of customer satisfaction the field has with OCIO initiatives.”

To better understand the IT needs of field personnel, the OCIO worked with Industrial Security Field Operations (IO) senior leadership to have the BRMs observe a team Security Vulnerability Assessment. To date, the BRMs have each been able to observe an assessment at a large facility within their respective region.

The first ride along occurred in March 2014, and since then, the goal has been to observe the different types of assessments performed and to see challenges faced not only during large assessments, but also ones that are smaller and more remote. All agreed that the experience has been enlightening.

“The logistics of an assessment, and including us as part of the team, were extensive, but the field was great in working with us ahead of time to get all the requirements taken care of,” said Mubarak “Moe” Allotey, Capital Region BRM. “During the assessment I participated in, the company chief information officer came to the facility and gave us a briefing, which I thought was great.”

“It was great to see the DSS partnership with industry in action,” said Bowman.

The DSS personnel in the field also agreed that the ride alongs were a valuable tool.

“It was good to see OCIO in the field experiencing first-hand what is involved with a vulnerability assessment,” said Chad Puffer, Information Systems Security Professional (ISSP) in the New York Field Office. “I am optimistic that the interaction between OCIO and the IO field staff will lead to better, more useful technology for the field. We need to get away from binders, notebooks and pens.”

One example of a project that OCIO is working on is a SIPRNet solution for smaller field offices. The challenges faced by DSS ISSPs working without a hardline SIPRNet solution was raised by Darcey Mulkey, Tucson Resident Office, during a security vulnerability assessment.

In response, OCIO found a GSA-approved container that houses the secure IT equipment and allows two people to work securely without having to renovate the office space to Secret open storage specifications.

“During a visit to the Southern Region, Kevin Baker, Marcus Evans, and Matthew Powell listened attentively to challenges concerning latency issues on the hardwired SIPRNet that was essentially precluding my ability to back up important data files,” said Jay Cable, deputy chief of the Counterintelligence division for the Southern Region. “Within a couple weeks, they produced a back-up program that has worked flawlessly! I encourage its use agency-wide as it is a simple yet effective way for backing data up on the SIPRNet and can probably be used on the NIPRNet as well. My thanks to OCIO for this fix!”

“We ask every level of personnel in the region and field what challenges they are facing that OCIO can help resolve,” said Matt Powell, Chief of Business Relationship Management.

Another area that OCIO is researching is an automated security vulnerability assessment scheduling system. Jennifer Norden, chief of the Irving Field Office, said scheduling assessments for over 400 facilities is complex and time consuming.

OCIO is working with software research organizations and industry to find an automated solution, and the requirement has been included in the National Industrial Security System project.

“Having OCIO experience first-hand how and why we do certain things allows the field to show why certain ideas are preferred,” said Paul Stalvig, ISSP in the Minnesota Resident Office. “Being able to discuss some of the issues concerning projected/possible projects makes us feel as if we’re more involved with the decisions and ultimately enabling OCIO to provide the best possible products, solutions and services to the field.”

TIGER TEAM SEEKS TO BRIDGE THE GAP BETWEEN DIRECTORATES

by **Rebecca Bernier**
Industrial Policy and Programs

In June 2014, the Industrial Policy and Programs (IP) directorate surveyed the regional directors and field office staff asking them to identify their needs and interests pertaining to each of the IP mission areas: Foreign Ownership, Control or Influence (FOCI) Operations, FOCI Analytics, International, Policy, Special Access Programs, and Assessments and Evaluations.

Based on the feedback, IP developed an initiative to improve communications and integration between IP and Industrial Security Field Operations (IO) through a series of outreach visits, otherwise known as the “Tiger Team” initiative. The Tiger Teams provide guidance and informal discussions on current changes in processes using real time examples and scenarios with field operations staff.



Additionally, IP sought to provide opportunities for the field staff to ask the “why” of what IP does, how each IP division plays a role in supporting the agency’s mission, and how IP impacts the work of field personnel.

Tiger Team members worked with IO’s senior leadership and coordinated across mission areas — IO, IP, Counterintelligence (CI), Center for Development of Security Excellence (CDSE) — to schedule the dates, locations and discussion agenda for the various field offices. Once those were determined, a subject matter expert was selected by the respective division chiefs, and an IP team was assembled, pre-briefed on topics to be included in the discussions with the field, and ready to travel to a single or multiple field offices.

Conversely, to enhance the IP team’s knowledge of the work accomplished in the field, team members were immersed in the daily work of the field staff, to include that of the Industrial Security Representatives, Counterintelligence Special Agents and Information Systems Security Professionals (ISSP).

When possible, the IP staff shadowed the field staff during their daily routine and participated in various activities, such as ride-a-longs to Security Vulnerability Assessments, CI facility visits and ISSP visits. Feedback from the IP participants has been extremely positive about getting to know the field, and the work challenges they face every day.

The Tiger Team focused their initial outreach on the Northern and Southern Regions, with visits to Atlanta, St. Louis, Irving, Andover, Detroit, Philadelphia, Boston and New York field offices during FY14.

The IP team will schedule visits to the Western and Capital Regions during FY15. The feedback from field personnel has been extremely positive, as several field office chiefs have commented, the IP Tiger Team visits are “... a great initiative and well executed.” As one field office chief commented on the Tiger Team, IP has “hit a home run!”

The Tiger Team members had the following positive comments:

“The time spent at the field office was invaluable because it allowed [me] to build a better working relationship with the personnel in the field office while providing them with helpful information regarding DSS headquarters. The trip was also valuable because I learned several items to note regarding industrial security procedures when I visited the different facilities with the ISRs.”

“The informal nature of the Tiger Team visits appears to elicit more questions by the field staff.”

(Deborah Keefe and Miladys Golden also contributed to this article.)

A Day in the Life of ...

AN INDUSTRIAL SECURITY REPRESENTATIVE

by Dahlia Thomas

Office of Public and Legislative Affairs

(Editor's Note: The following article is a first-person account of a day spent with a Capital Region industrial security representative on a vulnerability assessment.)

One word comes to my mind when I think of Industrial Security Field Operations (IO): "indispensable." My experience observing a day in the life of an Industrial Security Representative (ISR) was eye-opening. The opportunity to see an ISR conduct a Security Vulnerability Assessment (SVA) confirmed the integral role IO plays in protecting sensitive and classified information in the hands of industry, and at the same time, maintaining a sense of mutual trust.

I began preparing for my trip — my first SVA — by speaking with Field Operations staff at DSS headquarters about their experiences as ISRs. I also reviewed the Self-Inspection Handbook, researched the company online, and read sections of the National Industrial Security Program Operating Manual.

The ride-along, I admit, created a bit of anxiety on my part because the trip was venturing into uncharted territory for me, but the ISR quickly dispelled my fears with her professional demeanor.

I met the ISR at the facility, and we walked into the office as a DSS team. She introduced me as an "observer" and colleague at the agency. We were escorted into the reception area where we were given visitors' badges, and the president of the company welcomed us to the facility.

The Assessment

The primary goal of our visit was to review the security posture of the facility and the company's response to the vulnerabilities and violations identified in a previous SVA.

The ISR began the entrance briefing by explaining the reason for our visit and the expectations for the day: review corporate documents, JPAS report and CI annual threat briefing; conduct employee interviews; assess how well classified information was being safeguarded, and perform security checks of containers.

She also informed the Facility Security Officer (FSO) of changes that had taken place in the agency that would impact her organization. For example, the new opening of a Capital Region Field Office and the possibility of being assigned a new ISR.

The assessment included a review of the facilities' corporate documents, including the: DoD Security Agreement (DD 441),

SF 328, DD 254 and several other documents. The FSO provided a JPAS report, which reported changes in the status of key management personnel, all of which could impact the company's facility clearance.

The FSO informed the ISR of self-inspections she conducted previously, which included random inspections, CI annual refresher training, an onsite movie, overseas employee briefing and tracking employees' participation. The company was prepared for the assessment, but the ISR realized that some information needed for the assessment was missing. The FSO was cooperative and immediately researched the necessary information.

Reviewing the Findings

While the company had taken creative steps to improve its overall security program, ultimately the SVA revealed that the company had a few critical vulnerabilities. During the exit briefing, the president assured us that the company would take the necessary steps to correct the vulnerabilities.

The Masterful Work of the ISR

I was impressed with how the ISR handled the discovery of the critical vulnerabilities. I observed the FSO becoming concerned and anxious as risk areas were identified.

The ISR, however, remained calm and professional throughout the process. She patiently took the time to review the vulnerabilities with the FSO and president, explaining the ramifications, making recommendations, and ensuring the FSO understood the NISP requirements and the agency's role in providing oversight and a fair security vulnerability assessment. Her reassuring attitude and ability to manage the relationship, despite the negative findings, ultimately created an atmosphere of trust.

My Takeaways

As I reflect on my experience, I realized that the scope of my understanding of the agency's mission has increased, and I am better able to connect the dots when I hear reports from Field Operations. I can also better articulate the DSS story and not be challenged by the many acronyms associated with the DSS mission.

Of the 13,500 cleared industrial security facilities that the agency oversees, this facility represents just a tiny fraction of cleared industry. I have a better awareness of the value of DSS oversight, ensuring no vulnerability is left unchecked to cause grave damage to the nation. It was a valuable professional development activity.

CI ENHANCEMENTS: A

According to DSS records, since 2009, the proportion of cleared industry suspicious contact reporting has fluctuated between 15 and 22 percent. Current statistics show industry reporting is declining at 12 percent, and only six percent of cleared industry provides reporting that has a counterintelligence (CI) nexus.

In comparison, DSS estimates that foreign intelligence entities (FIEs) target approximately 40 percent of cleared contractors. The gap between what is reported and what could be reported is significant.

DSS Counterintelligence directorate (CI) estimates this reporting shortfall translates to over 2,000 response-worthy events that go unreported each year within cleared industry. The shared risk this gap embodies must be addressed by both cleared industry and DSS, with assistance from our federal law enforcement and intelligence community partners.

To encourage increased reporting, DSS CI, in collaboration with DSS Industrial Security Field Operations, developed a CI Enhancement to the security rating matrix that leverages the partnership between DSS and cleared industry. The first CI Enhancement, Category 7a, Threat Identification and Management, encourages National Industrial Security Program members to become aggressive in establishing a CI-focused culture within their companies.

This CI-focused culture should promote the detection and deterrence of FIE collection efforts and insider threats through preventive programs with an emphasis on the timely reporting of suspicious activities. DSS will recognize those cleared contractors that are committed to stopping the threat and have established vigorous and effective CI programs.

DSS also added a second CI Enhancement, Category 7b, Threat Mitigation. This category recognizes the cleared contractor who achieves success in Category 7a, and that commitment results in an open investigation during the evaluation period. In short, Category 7b is the direct result of success in Category 7a.

Where to Start

The basic tenets of a vigorous CI program include: understanding the threat environment unique to your company; committing to timely reporting; and making agile and authoritative decisions that focus on neutralizing or mitigating vulnerabilities and threats. These basic tenets, when implemented effectively, will provide your company with a CI Enhancement in Category 7a and the best chance to neutralize threats to your company, personnel, and technologies (Category 7b).

These rating matrix changes allow cleared industry and DSS to continue the move away from prescriptive checklists and instead, meet the growing challenge by empowering risk managers to recognize the threat, address the vulnerability, and understand the consequence/value of our technologies to the adversary.

27 Years a SPY:

Dongfan "Greg" Chung, a cleared contractor with high-level security clearance employed as a stress analyst, spied for China from 1979 to 2006. He provided trade secrets to China on the U.S. Space Shuttle, the Delta IV rocket, and the C-17 military cargo jet.

RESULTS-ORIENTED MEASUREMENT

Director of National Intelligence
James Clapper, from his testimony
to the Senate Select Committee on
Intelligence, March 12, 2012:

“We assess that highly networked business practices and information technology are providing opportunities for foreign intelligence and security services, trusted insiders, hackers, and others to target and collect sensitive U.S. national security and economic data. This is almost certainly allowing our adversaries to close the technological gap between our respective militaries, slowly neutralizing one of our key advantages in the international arena.”

20+Years a SPY:

Chi Mak, a cleared contractor, admitted to entering the United States with orders from the Chinese government to steal U.S. defense secrets. Over a 20-year career, Mak provided the Chinese government information on quiet propulsion systems for the next generation of U.S. submarines, details on the AEGIS radar system, and stealth technology associated with the U.S. Navy.

To Get Started:

Promote suspicious contact reporting throughout your facility/company. Review the reporting received from your employees for items of CI interest. Refer any questions to your assigned DSS CI Special Agent (CISA) and Industrial Security Representative (ISR). Report CI-related information quickly to your ISR and CISA; DSS will then refer CI matters to the appropriate investigative agency for action.

Understand your technologies and the threats to them. Consult your assigned CISA and ISR for sources for threat information; no one understands your company better than you, so no one can pinpoint the potential entry points and vulnerabilities as well as you can. Reporting will flow when you, the facility security officer, personally engage with critical points of contact within your own company.

When you find vulnerabilities, act immediately. If you know of vulnerabilities within a facility, take steps now to mitigate the risk before the vulnerability is exploited. Consult your ISR and CISA for community best practices to reduce your risk.

CI Enhancement Key Points

The CI enhancement focuses one enhancement category on “process” (Category 7a) and the other on “performance” (Category 7b).

Scoring for the rating matrix will remain the same with the addition of one enhancement category. Achievement of Category 7b will be “bonus” points for facilities with suspicious contact reports provided to DSS and actioned by federal and military investigative agencies.

A cleared company must be awarded Category 7a to be considered for Category 7b. Why? The cleared company’s CI program must have played a role in the identification of the threat to receive credit for its neutralization.

A cleared company can increase the likelihood of another government agency taking the case for action through timely and thorough reporting. The success of law enforcement and intelligence community response is directly linked to how quickly they are able to engage with the threat.

To be awarded credit for Category 7b, DSS must be able to validate the investigation with the investigative agency. The date DSS is advised of the open investigation by the investigative agency is the date used for considering the enhancement credit.



Editor’s Note: The following is the first 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.

Karl Hellmann, Regional Director (RD) of the Western Region, assumed his current position in March 2009 and is the longest serving RD at DSS. Hellmann is responsible for all DSS field activities west of North Dakota and New Mexico, to include Alaska, Hawaii and Guam.

He began his federal service in 2006 as an Information Systems Security Professional (ISSP) with DSS in Chantilly, Va. In this position, he was responsible for reviewing and implementing established DoD policy regarding industrial security procedures, systems, standards, and regulations governing the safeguarding of classified information on information systems utilized by contractors functioning in the National Industrial Security Program (NISP).

In July 2007, Mr. Hellmann was appointed Acting Regional Designated Approval Authority (RDAA) for the National Capital Region and in October, he was selected as the RDAA. In this position, he led a team in support of certification and accreditation of industry classified systems as well as subsequent annual assessments. He served as the Designated Approving Authority for the NISP on government contractor information systems within boundaries prescribed in the RDAA appointment letter.

Tell us about the Western Region. What makes it different from the three other regions?

The Western Region has responsibility for the two largest cleared facilities in the NISP. The region is also the largest and most geographically dispersed in DSS. As a result, our field personnel spend about one-third of their time on TDY; for some, it’s as high as 50 percent. We have approximately 3,100 cleared facilities with 100 personnel assigned to one of six field offices or seven resident offices.

Are there unique challenges in the region?

I think the most unique aspect to the Western Region is the time and distance from DSS headquarters. In terms of the time difference, we have just about five hours a day we can work with headquarters on issues — whether it’s the Facility Clearance branch or financial management or logistics management.

Some employees at headquarters are halfway through their day when we come to work and are leaving for the day when it’s lunchtime here.

The distance is also a challenge. We are not able to participate in working groups or some meetings because it doesn’t make sense to send someone TDY for three days to attend a one or two hour meeting.

As a result, there’s less participation from the Western Region in some of these events and less exposure to our personnel. I think we have good people doing good work, but given their location, they aren’t always seen by headquarters.

One way we’ve overcome some of this challenge was to locate our information technology (IT) support at the region level, rather than all at headquarters. We are able to respond much more quickly within the region, but we still have some challenges. For instance, it still takes two days to FedEx equipment to the Tacoma Field Office from the regional office in San Diego.

I think another aspect of the geographic separation is better integration on our part. Because each field office is so self-contained, the personnel at each have to work together to get things done and I think they’re very effective. With small staffs at each office, there is no, “it’s not my job,” or “I’ll leave it for someone else to do.” There isn’t anyone else to do it.

REGIONAL DIRECTOR OF THE WESTERN REGION

It seems almost every year the region must deal with wildfires. A few years ago, there were fires very close to the Colorado Springs office. How do you prepare for this and how do you work with industry to prepare?

For us, the Emergency Operations Plan (EOP) is not just a paperwork drill, it's a way of life. We execute a recall roster every year and regularly do telework drills to ensure all employees can work from home.

We've also had to implement our EOP several times. We had to evacuate the San Diego office in 2007, and in 2012, the Colorado Springs Field Office was packed and ready to go if they had to.

We maintain situational awareness on all of our facilities to monitor how the events will affect them. For us, it's a routine part of our outreach to industry.

You are the longest serving RD at DSS. How has the position of RD changed since you've been in the position?

The biggest change I've seen in the RD position is a move from the operational to the strategic. When I started in the position, it was more operationally focused, and it has evolved into a leadership position within DSS.

My job is to take the mission and vision from DSS and Field Operations and apply it throughout the region. As a result, I spend most of my time looking outside the region and basically allow the field office chiefs to run their offices.

For instance, I might be working with the other RDs to determine if Field Operations has the right formula for the facilities of interest list or updating the rating matrix. Both apply across DSS, not just the Western Region.

Our gathering and reporting of metrics has also changed the role of the RD and the regional staff. The metrics help us prioritize our workload from an operational

perspective. They also give us better insight into our workload and our facilities.

The other major change since 2009 is the size of the regional staff. When I came to San Diego, the staff was two employees, now we have eight. There was no regional counterintelligence manager and no local support for FOCI [Foreign Ownership Control or Influence].

With the increased staff, we've been able to better integrate our operations across the region. Having FOCI expertise here has allowed us to participate in annual meetings at the local facility level and remain engaged with our facilities.

You came to the RD position from the ISSP side rather than the industrial security representative side of DSS. How did that help/hinder you when you became the RD?

I think my IT background was initially a hindrance because there was so much I didn't know about being an IS Rep or a Field Office Chief.

But I also think it was a benefit. Because I didn't have that background, I didn't have any biases or any set way of doing things. So I was more apt to say, okay, let's try something new or something different.

I think I'm also open to allowing my field office chiefs to manage their areas of operation; I'm not going to tell them how to do their jobs.

I think my background has also helped create the integration we have at the field level. As a former ISSP, I do bring a different perspective to the position, and I understand the importance of the ODAA mission and how it must be integrated into the larger assessment and oversight mission.

If employees see the senior position in the region comes from a different background, then that opens up more opportunities for the junior personnel. So ultimately, I think it's been good at all levels.



FIRST VIRTUAL DOD SECURITY CONFERENCE SPANS THE GLOBE

On Sept. 25, 2014, the Center for Development of Security Excellence (CDSE) hosted the first virtual DoD Security Conference. The virtual conference format allowed over 1,100 civilian and military security professionals from across the globe to attend from their locations and still have direct contact with security community leaders and policy experts.

The theme for this conference was “Countering Today’s Security Threats.” The conference agenda included sessions representing community-requested topics. Insider threat, one of today’s biggest security concerns, was addressed in many presentations.

Conference presenters hailed from DSS, but also from the Office of the Under Secretary of Defense for Intelligence, DoD Consolidated Adjudication Facility, Department of the Army and the Office of Personnel Management.

Presenters discussed the harm to national security and personnel from recent insider threats and how policies are changing as a result. Additionally, sessions on the personnel security program provided detailed information on new policies and the importance of this first line of defense in combating the insider threat.

In addition to insider threat and personnel security, the agenda included a session on security workforce professionalization and provided key information on DoD security skill standards, Security Professional Education Development (SPeD) Certifications, and certification maintenance.

Participants appreciated the ability to have two-way dialogue with presenters directly from their desktops or mobile devices. During the breaks, the chat rooms hosted a steady stream of dialogue regarding lessons learned and best practices. The chat feature allowed for the dynamic sharing of knowledge across the DoD security community regarding policy and procedures better protecting our nation’s information, operations, and resources.

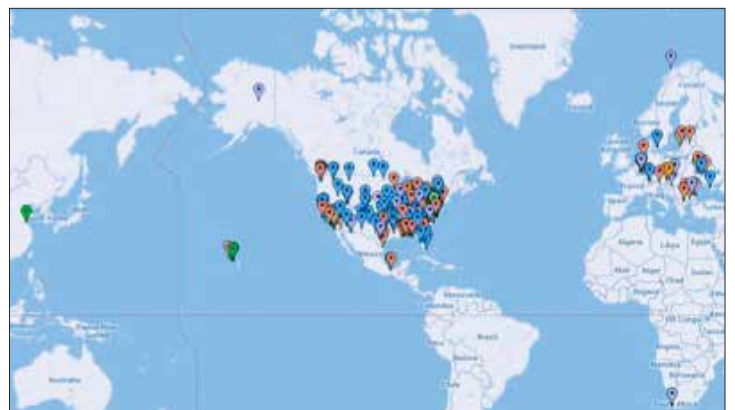
Due to budget constraints, the DoD Security Conference had been on hiatus since 2011. At the last conference, 485 security professionals came together at an in-person setting. DSS’s ability to

leverage the virtual format allowed a 100% increase in the number of participants, provided a professional development venue for the security professional not otherwise available, and realized a significant cost savings in lodging, travel, and preparation costs.

Based on post-conference survey results, the DoD security community has greatly benefited from having this additional workforce professionalization tool. A phenomenal 80% said they would not only attend a virtual conference in the future, but would recommend it to their colleagues.

“Thanks again for this virtual conference! My folks in CONUS and OCONUS were very grateful for this opportunity, as many of them have never had the chance to take part in a DoD security conference. This was a great first effort, even down to the chats during the breaks and the commercials. Looking forward to future iterations.”

Joy Assent, SPIPC
Chief, Security Division, Defense Logistics Agency



Worldwide Participation in the 2014 Virtual DoD Security Conference

DSS HOSTS TRAINING FOR INFORMATION ASSURANCE PROFESSIONALS

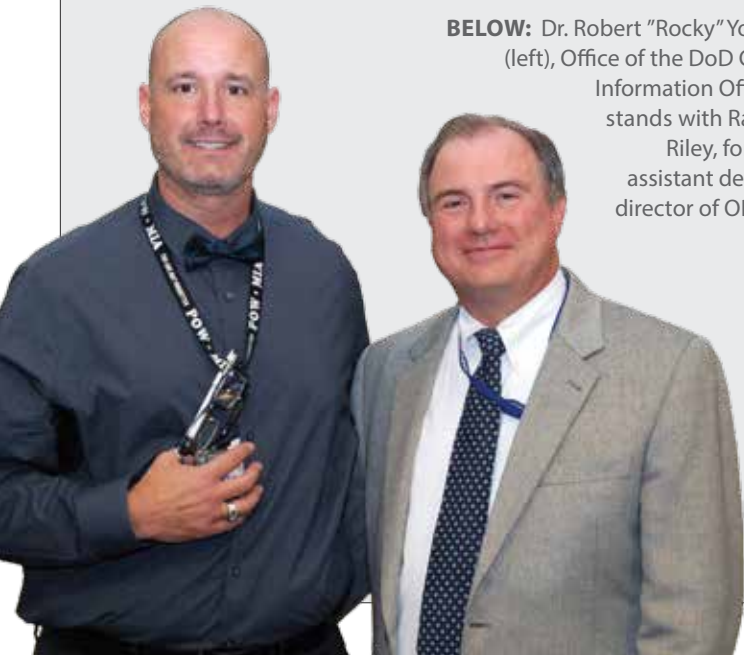
by Selena Hutchinson
Industrial Security Field Operations

In August, over 80 DSS information assurance professionals gathered at the Russell-Knox Building in Quantico, Va., for the 9th Annual Information Systems Security Professional (ISSP) training. The event was hosted by the Office of the Designated Approving Authority (ODAA) and featured a three-day meeting agenda covering a variety of cyber-related topics.

The ISSP training meeting is attended by information assurance (IA) professionals from across the agency. An event that started as a user group meeting, the training meeting has blossomed into a full technical training event with nationally-known speakers and top notch technical sessions.

DSS IA professionals receive continuing professional education (CPE) credit by attending that supports the annual training requirements to maintain DoD 8570 certifications. The ISSPs and other DSS IA professionals also have opportunities for networking, professional development, and a centralized forum to address inconsistencies.

"This year we nudged attendees to break out of the mold of checklist risk avoidance and toward a risk management framework approach, a goal I think we achieved through carefully selected speakers and topics," noted Randy Riley, former assistant deputy director of ODAA. "The feedback from this year's meeting was overwhelmingly positive, and we look forward to again upping the game in 2015."



BELOW: Dr. Robert "Rocky" Young (left), Office of the DoD Chief Information Officer, stands with Randy Riley, former assistant deputy director of ODAA.



DSS Director Stan Sims provides opening remarks at the 9th Annual ISSP Training Meeting.

Meeting highlights included Tony Sager, Director, SANS Innovation Center, who spoke on "The Fog of More: A Cyber Security Community Challenge;" Martin Linder, a returning presenter from Carnegie Mellon University (CMU) and member of the defense industrial base; "Securing the Internet of Things — Separating Hype from Reality," by John Pescatore, SANS Institute; technical sessions covering topics such as critical controls, cloud computing, risk management framework, CCR; and regional break-out sessions. Industry partners included SANS, BAE Systems, Inc., CMU, and the MITRE Corporation.

Dr. Robert "Rocky" Young, Office of the Department of Defense, Chief Information Officer, provided an entertaining yet hard-hitting "Status of the Cyber War" presentation and reminded the audience of their ethical obligations as 8570 certified IA professionals.

Young also shared some of the things that keep him up at night including: the cyber work force, cloud services, supply chain management, commercial mobile devices, insider threat, continuous monitoring, and digital monitoring.

The Regional Designated Approving Authorities were allocated time on the schedule to host separate regional break-out sessions with their respective teams for other relevant discussions. The DSS Office of the Chief Information Office issued equipment to the ISSPs during the meeting, thus avoiding unnecessary expense to the agency from shipping the equipment remotely.

At the end of the training meeting, DSS Director Stan Sims made closing remarks and recognized 12 individuals for various accomplishments and contributions made by those in attendance.

As cyber threats increase and become more sophisticated, ISSPs find themselves operating in a fast-paced environment along with our industry partners. By hosting events such as this, DSS helps ensure its technical workforce can take timely training that helps it stay ahead of the threat.

DSS KICKS OFF **PHASE II** OF THE

"Business Process Reengineering (BPR) ensures we place a good system on good processes to maximize return on investment and optimize operations."

by **Ryan Deloney**
Industrial Security Field Operations



The industrial base, in which the Department of Defense invests approximately \$350 billion annually, is the backbone of U.S. warfighter technical capability superiority and faces an increased volume of threats and growing diversity of penetration efforts by hostile foreign and insider threats.

Assigned to partner with and oversee the security of classified information within the industrial base, DSS operates within the constraints of a dispersed, complex and labor-intensive mission;

budget restrictions; and stove piped, legacy information systems. All of these factors contribute to the need for a data-driven, collaborative, automated, online environment accessible to government and industry users that delivers industrial security services, training, and oversight with interoperability and efficiency.

The solution? The National Industrial Security System or NISS. NISS is the DSS future information system architecture that will replace legacy capabilities (Industrial Security Facilities Database

NATIONAL INDUSTRIAL SECURITY SYSTEM

[ISFD], Electronic Facility Clearance System [e-FCL], and assorted custom tools), while integrating access to additional DSS and partner applications and data.

The goal of NISS is to improve processes and tools to help people across the National Industrial Security Program (NISP) maximize efficiency and eliminate administrative burdens.

In April 2014, DSS completed an almost year-long process to capture the technical and non-technical solutions needed to realize the NISS vision. Phase I of the Business Process Reengineering (BPR) included the support of over 150 DSS, government, and industry stakeholders across 14 key mission areas.

The BPR will result in short and long term benefits with process improvements and technical system requirements all tied to NISP implementation challenges and operational constraints.

NISS Phase I processes enhanced through the BPR:

- Facility Clearance processing
- On-site and telephonic surveys
- Foreign Ownership, Control, or Influence (FOCI) due diligence
- Electronic Communication Plans
- Information System Certification & Accreditation
- Security Vulnerability Assessments
- Command Cyber Readiness Inspections
- NATO Control Point Inspections
- Foreign classified visit requests
- Triage Outreach Program
- NISP FOCI/financial change monitoring
- Key Management Personnel clearance oversight
- Security Violations
- Suspicious Contact Reporting

The NISS BPR identified over 90 non-material solutions to improve NISP operations, specifically in the areas of training, policy, organization and process. For example, realigning roles and responsibilities between the DSS Facilities Clearance Branch, field Industrial Security Representatives, and FOCI Analytics Division will further

streamline the initial Facility Clearance process resulting in expedited clearance issuance for Industry partners. DSS is currently developing an implementation strategy with a goal of rolling out these enhancements in 2015. Even before the NISS technical solution is implemented industry, government, and DSS stakeholders will benefit from improved timeliness and quality in the areas identified above.

For the technical solution, the NISS BPR identified over 1,500 detailed requirements across the spectrum of workflow management, content management, reporting and analytics, integration, dashboard user interface, mobile capabilities, and notifications and messaging.

As the technical solution is developed, DSS will continue government and industry stakeholder outreach for participation in prototype reviews, acceptance testing, and training to ensure the final solution meets the expectations of all involved. The NISS BPR is a significant effort from which the NISP community will receive substantial return on investment for years to come.

The DoD Deputy Chief Management Officer issued validation of the process in August 2014, noting DSS is driving “business processes that are as streamlined and efficient as practicable.”

Additionally, following a presentation to the Office of Management and Budget Performance Accountability Council in July 2014, their chairwoman noted, “how incredibly thoughtful, thorough, and inclusive the design effort has been to date. NISS design is truly a model we need to promote as a best practice across government. The potential that will be realized with full NISS implementation is incredibly exciting!”

DSS began NISS Phase II in July 2014 and will complete it in July 2015. During this phase, focus will be on an additional 10 key NISP mission areas for a new BPR, execution of the non-material solutions recommended in NISS Phase I, and establishing a foundation for technical solution development.

Ultimately, the NISS technical solution will place the best tools on the best processes to minimize administrative burden and maximize proactive, risk-based security functions for DSS, industry, and government stakeholders.

For any questions, please contact NISS@dss.mil.

DSS COUNTERINTELLIGENCE PARTNERS WITH INDUSTRY TO MITIGATE FOREIGN INTELLIGENCE THREATS

The stakes are high in the battle against foreign collection efforts and espionage that targets U.S. national security information, intellectual property, trade secrets, and proprietary information.

To help mitigate the persistent foreign intelligence threat, the Defense Security Service partners closely with cleared industry at both the field office and headquarters levels.

Established in 2012, the Counterintelligence Partnership with Cleared Industry (CIPCI) program provides cleared industry the opportunity to work closely with headquarters elements of the DSS Counterintelligence (CI) directorate to facilitate communication, information sharing, understanding, awareness, and resolutions to promote the CI directorate's mission of identifying unlawful penetrators of cleared U.S. defense industry and articulating the threat for industry and U.S. government leadership.

Enhanced collaboration between cleared industry and DSS CI allows cleared contractors and the CI directorate to share threat information, and analytical methodology, and to identify opportunities for CI successes.

This program also provides participating members a non-attribution environment to discuss pitfalls, successes, best practices, and lessons learned. While participating in the program, cleared industry representatives have access to DSS information systems to analyze threat information relevant to their company.

Strategically, the program facilitates U.S. government efforts to foster sophisticated security and counterintelligence capabilities within cleared industry, enabling cleared contractors to better protect our nation's most critical and sensitive technologies.

Benefits to DSS

- Comprehensive understanding of participating companies' security and counterintelligence structure and capabilities
- Increased understanding of participating companies' contracts, technologies, and government programs
- Real-time two-way information sharing
- Increase in the number of quality suspicious contact reports submitted by participating contractors
- Direct line of communication with company CI and security leadership

Benefits to Industry

- Access to near real-time threat information via DSS channels
- Strategic level analysis to enhance their security posture

- Access to subject matter experts to assist in recognition of suspicious indicators
- Increased understanding of DSS CI efforts and processes

To date, both the agency and participants have experienced several successes:

Identified an illicit procurement network — Stemmed from a close working relationship with corporate security elements of a CIPCI participant.

Assisted in making an informed business decision — Collaboration between a CIPCI participant and DSS CI personnel led one participating company to not engage in business with a foreign entity and to reexamine internal business practices to quickly identify developing business relationships with foreign entities of concern.

Communicating/disseminating classified information — Collaboratively developed communication nodes leveraging existing government systems to facilitate the dissemination of classified information to cleared industry representatives throughout the country.

Reporting Increase (Quality and Quantity) — Developed process by which companies identified suspicious activity previously going unrecognized and reported it to DSS CI through the CIPCI program. Subsequently, DSS analyzed and referred these reports to applicable government agencies for action. Reporting related to this initiative accounted for approximately 10 percent of all reporting submitted to DSS, corporate-wide, for this company.

Crosstalk/Collaboration — Program criticality lies in a participant's ability to share initiatives with other participating members. Crosstalk and collaboration have enabled other members to institute best practices learned within this shared environment.

Membership Requirements

The details of this year long program are outlined in a written agreement signed by both parties. At the end of the year, both DSS and the contractor can dedicate resources to support this initiative. Both parties reserve the option of renewing participation annually.

The program is currently open to companies operating under the NISP participating in the Gray Torch program; others will be considered on a case-by-case basis. Companies may apply individually or as part of a consortium.

While participating in the program, contractor representatives working in DSS facilities may have access to non-public

WHAT IS A PCL?

information about other contractors or contractor employees and must sign a non-disclosure agreement.

For additional information, contact the Gray Torch team at GrayTorch@dss.mil.

Participant Comments

“ Defense Security Service CI Partnership with Cleared Industry Program is a win-win for Industry and the U.S. Government. The program fosters collaboration, opens lines of communication, and allows both to be more responsive to issues impacting each other. We are about to graduate this partnership to a new level with the identification of our critical assets and a better understanding of where our adversary might be in their development and shortfalls. Our hope is to proactively work with the government to further secure our critical technology.”

Doug Thomas

Director, Counterintelligence (CI) Operations and Corporate Investigations,
Lockheed Martin Corporation (LMC)

“ L-3 Communications developed a valuable and trusted partnership with DSS Counterintelligence (CI) resulting in the increased strength and resiliency of the L-3 CI program. Our alliance and the subsequent mitigation strategies developed have greatly assisted the corporation in protecting L-3 products and information.

We believe it is imperative to foster an even closer working relationship through the mutual development and support of a classified communication capability to effectively share real time threat information between DSS CI and cleared defense contractors. L-3 looks forward to a continuation of our close working relationship with DSS CI, based in mutual trust and respect.”

Vincent Jarvie

Vice President, Corporate Security
L-3 Communications Corporation

WHAT IS A PERSONNEL (SECURITY) CLEARANCE?

by Lisa Gearhart

Industrial Policy and Programs

According to DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), a personnel security clearance (PCL) is “an administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.”

The determination to grant eligibility is made by the government, and for industry that determination is made by the DoD Consolidated Adjudications Facility.

Eligibility is not enough, though, to grant a person access to classified information, they must also have a “need to know” the information. Need to know, according to the NISPOM, is a “determination made by an authorized holder of classified information that a prospective recipient has a requirement for access to, knowledge, or possession of the classified information to perform tasks or services essential to the fulfillment of a classified contract or program.”

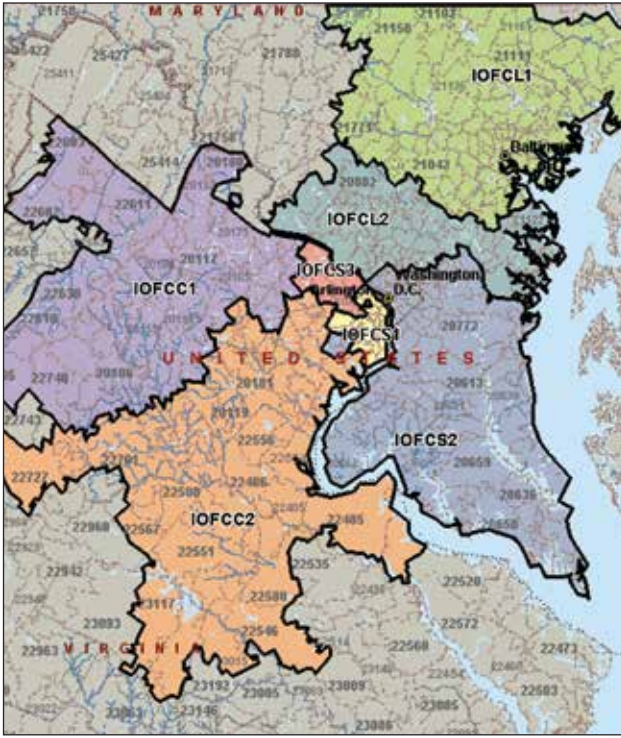
A person may be granted access to classified information when it is essential in the performance of tasks or services related to a classified contract, and the individual has been determined to have the appropriate level of eligibility and a valid need to know the classified information.

In simple terms: eligibility + need to know = access



Contractors use the Joint Personnel Adjudication System (JPAS) to maintain the accuracy of their employees' access records. In order to maintain a JPAS account, contractors must comply with Defense Manpower Data Center's (DMDC) processes and procedures related to account management. See the DMDC website for additional information.

For additional information on managing PCL records in JPAS, see the recently posted DSS guidance, “Eligibility, Break in Access and Break in Employment,” which can be found on the DSS website.



Capital Region Stands Up New Field Office

by Grant Shackelford
Office of Public and Legislative Affairs

On Oct. 1, 2014, the Capital Region stood up a seventh field office, Alexandria 3, the third to operate from Alexandria, Va. The establishment of the new office comes as a part of a larger reorganization taking place within the region.

The impetus for reorganization is twofold: balance the increasing workload with the other Capital Region field offices; and facilitate a redistribution of cleared facilities within individual industrial security representative portfolios.

“Some of our field office chiefs have had to manage upwards of 1,000-1,100 facilities,” said Sarah Laylo, Chief of the Alexandria 3 Field Office. By adding the new field office and restructuring the various areas of operation, DSS will increase its ability to provide support, oversight, and appropriate customer service.

“When the transition is complete all field offices within Capital Region will have an average of 700 to 720 facilities each, with the more complex work also balanced across the seven field offices,” said Laylo.

The Capital Region has oversight of over 5,000 cleared facilities, the largest contingent of cleared facilities in the United States, in addition to being the agency’s smallest geographic region. The region began transitioning

DSS Cybersecurity Operations Division Receives DoD Award

The DSS Cybersecurity Operations division recently received the Department of Defense Counterintelligence and Human Intelligence (CI/HUMINT), Community Award.

The DoD CI/HUMINT Awards Program, sponsored by the Defense Intelligence Agency, recognizes exemplary achievement in applying, developing, promoting, expanding and improving CI or SUMINT support to the DoD and the nation.

The DSS Cybersecurity Operations team was recognized for developing and implementing a process that uses functional services capabilities directed at specific cleared contractor locations to proactively develop cyber threat information.

Using these sources, the Cybersecurity Operations team effectively produced analysis-driven actions to direct functional services at specific cleared contractors with significant technologies at high risk of compromise.

These efforts disclosed new intricate cyber software that compromised cleared contractor networks. The discovery of the threat initiated mitigation efforts and the production of preemptive threat products, preventing the further loss of technology critical to national defense.

facilities to reflect the new organization on October 1 with the goal of Jan. 1, 2015 for full transition.

“The transition takes time,” said Heather Green, Regional Director, Capital Region. “Some facilities will see new Industrial Security Representatives (ISR) and Information Systems Security Professionals assigned to their facilities. In some cases, the ISR and Facility Security Officer have worked together for a long time and in those cases, we want to ensure a smooth, seamless handoff. We also schedule our assessments on an annual basis, so we had to factor scheduling into our transition plan as well.”

Since assuming the position of field office chief in March of this year, Laylo has been standing up the office, a duty that includes hiring and training personnel and the logistics to support them and establishing the new area of operation for all seven field offices.

The area of operation for Alexandria 3 includes the following areas in Virginia: McLean, Dunn Loring, Great Falls, and Reston.



Unique Program Grows Leaders Through Hands-On Training

In June 2014, two DSS employees graduated from the Department of Defense Executive Leadership Development Program (ELDP) — a unique program that includes aggressive hands-on immersion training.

During the 10-month training program, Earl Parker, a senior industrial security specialist in the Charleston Resident Office, and former DSS employee Brian Reissaus were exposed to the joint and interagency perspective through intense, hands-on field experience with all uniformed branches of the Department of Defense (DoD) and other executive branch agencies.

Training for the Class of 2014 started in November 2013, with the initial two weeks of training, known as Core Curriculum, at a residential training facility in Southbridge, Mass. Although classroom instruction is included, the program does not follow the traditional leadership training model found in the OPM leadership courses and other government leadership programs.

ELDP focuses on application of leadership skills through practice rather than simple discussions and role playing. From day one, each student is thrust into leadership, team building, and followership roles through daily individual and team assignments, guided discussions, and critical thinking exercises.

Students study DoD organization and policy, practice public speaking, and prepare individual and group presentations on various DoD topics. Students are pushed to work outside their comfort zone and experiment with varying leadership styles.

“Failure is an expected part of the learning process and used as a tool to help students improve leadership and presentation skills in a safe environment,” said Parker.

After the Core Curriculum, the program shifts focus from leadership principles to understanding how the DoD enterprise works. Leadership development remains a constant theme and challenge throughout the program, but the various “deployments” to different components of DoD and partner agencies provide a first-hand view of the complexities and challenges faced by DoD.

The program’s hallmark experiential training allows students an opportunity to get hands on experience with the warfighter. Students are given the opportunity to speak and train with all levels of military men and women, ranging from new Army, Marine Corps, and Air Force recruits to General Officers and Senior Executive Service civilians from all military departments.

“Although the experiential aspect of the training is often fun and sometimes challenging, the greatest benefit is the way it opens the door to candid dialog with active duty members of our armed services,” Parker said. “Visiting the warfighter in their ‘home environment’ allowed a more candid rapport; one that can’t be achieved sitting in a classroom or speaking with a Public Affairs Officer.”

Over the course of the training, the ELDP Class of 2014 visited 37 commands and military units throughout the United States and overseas. The class typically conducted one seven to 10-day deployment each month, where ELDP students participated in events as varied as firearms and modern combatives training to rappelling and practicing underwater escape methods from simulated crashed aircraft.

The members of ELDP Class of 2014 prepared closing remarks, which were presented during graduation week at the Pentagon, and best sum up the overall impact of the program: “ELDP provided us with exposure to the joint arena and offered opportunities to experience problem solving across the enterprise. We participated in extensive immersion experiences in the field alongside each of our military components, and with combined and allied forces. We now have a greater appreciation and understanding of the mission of our warfighters, the complex challenges they face, and the role that we will have as future leaders.”

Beth Whatley, Virginia Beach Field Office Chief, attended the graduation and commented about what a challenging and positive experience the ELDP has been for Parker. “My goal for Earl was to gain an even greater exposure to the DoD enterprise and to observe how our work in DSS directly links to the warfighter. It has also been beneficial for him to share that knowledge with his colleagues.”

Counterintelligence Integration in the Field: Best Practices from the Andover Field Office

by John Wetzel

Andover Field Office Counterintelligence Special Agent

DSS Counterintelligence is a diverse mission and has brought valuable equities to our primary mission of providing oversight of the National Industrial Security Program (NISP). Counterintelligence Agents are powerful assets to the DSS mission.

In accordance with DSS Director Stan Sims' directives, DSS Field Operations has actively fostered productive partnerships with cleared industry security professionals and management. These partnerships have assisted in securing our nation's secrets within the cleared contractor community.

But partnership must also be practiced at home. At the field office level, creating partnerships between CI Special Agents (CISA), Industrial Security Representatives (ISR), and Information System Security Professionals (ISSP) is essential to the continued success of the DSS mission and establishes a positive culture of teamwork.

Continued revelations of cyber threats, insider threats, and supply chain risk highlight the importance of accomplishing our mission of protecting the technologies that keep the warfighter safe.

The Andover Field Office, led by Field Office Chief John "Sean" Donnelly, possesses one of the most complex portfolios of cleared facilities in the United States and maintain one of highest percentages of cleared contractor suspicious contact reporting (SCR) in the NISP. "Our ISRs and CI Agents are fully integrated, constantly work side by side, and with few exceptions, show up at our contractor facilities as a DSS team," said Donnelly.

In addition to having a highly experienced cadre of ISRs, ISSPs, and CI Agents, the office has continually found success by identifying synergies between industrial security, information assurance, and counterintelligence.

We foster an environment of teamwork and collaboration through consistent communication, supporting the industrial security mission, educating our DSS colleagues on the CI mission, and actively participating in field office activities.

Communication is Key

Counterintelligence is a mysterious process to many outside of our profession, partially by the very nature of the work, and DSS CI agents are drawn from a wide variety of experience levels and backgrounds. The three CI Agents assigned to Andover break down these walls through very simple methods of communication.

First, we communicate our schedules to the rest of the field office, but even more, we communicate our CI actions at the facilities with the cognizant ISR, as well as the Field Office chief. We understand the importance of keeping the chief informed of our activities in the field, and find this helps deconflict actions among DSS components, while minimizing activity for our industry partners.

Second, we ensure Facility Security Officers (FSO) understand their primary point of contact within DSS is always the ISR as the ISR is ultimately responsible for the facility's compliance with the NISP. Depending on our relationship, and in coordination with the ISR, we may take the lead on a specific CI matter; however we ensure that the ISR is copied on pertinent issues.

Equally important is the SCR process. CI Agents ensure the cognizant ISR is aware of our process, highlight particularly sensitive or interesting reports, and share feedback on suspicious reports with the ISR and the FOC.

Lastly, we share all successes with the field office team, both individually, and in field office meetings and emails. Communicating the CI successes encourages our industrial security colleagues to support the CI mission, as well as supporting the concept that everything the DSS CI team does is directly related to field office team.

Support the Industrial Security Mission

The Andover CISAs support the DSS oversight mission in multiple ways, including participation at security vulnerability assessments (SVA), reviews of adverse information reports submitted by industry, and off-site support of facilities.

The Andover CISAs attempt to support as many SVAs as possible and prioritize them according to the Facilities of Interest List when necessary. By sharing assessment schedules in advance, we can have a dialogue about the CI mission and how we can provide off-site support.

During on-site CI support to the SVA, we ask questions focused on counterintelligence issues but also work as a "force multiplier", by addressing industrial security issues during our interviews. These questions may include the security clearance level, the date the individual last accessed classified information, verifying security education, identifying security vulnerabilities, and other issues of industrial security concern. This assists our ISRs in their workload, and provides incentive to include CI questions during the course of their interviews.

CISAs review all violation reports submitted to the field office and provide comments to the ISR as necessary. Occasionally, these reports contain matters of CI interest, particularly concerning culpable individuals with multiple security violations.

We prioritize our feedback to ensure timely responses to the industrial security team, and discuss concerns with the ISR or ISSP, and synchronize communications with various headquarters elements, including the Operations Analysis Group.

Not all SVAs can be supported, of course, and we maintain an inventory of counterintelligence materials, brochures, fliers, and pamphlets, as well as the unclassified "Targeting U.S. Technologies," mouse pads, and letters signed by the CI agent for facilities to read.

Director of Field Operations Retires After 30 Years of Service

Rick Lawhorn, director of Industrial Security Field Operations (IO), retired Oct. 2, 2014, after more than 30 years of service, the majority of his career with the Defense Security Service.

Over the years, Lawhorn held a number of progressively responsible positions at DSS, to include Regional Staff Specialist; Field Office Chief; Chief, Program Integration Branch; and ultimately, director of IO.

He was promoted first to the Defense Intelligence Senior Level in 2009 and then to the Defense Intelligence Senior Executive Service in 2011.

At his retirement ceremony, Lawhorn received several awards and was presented with his Senior Executive Service flag and with a United States flag that was flown over the Capitol Building in recognition of his dedicated service.



Director of Industrial Security Field Operations Rick Lawhorn, right, is honored for more than 30 years of government service.

“ Counterintelligence is a mysterious process to many outside of our profession.

The letters address suspicious contact reporting, foreign travel, cyber events, and provide our contact information.

If we are unable to connect with a cleared facility prior to the SVA, we reach out to the FSO after the SVA to ensure we can answer any questions or concerns they may have. Potential counterintelligence actions have been discovered as a result of in-person or telephonic outreach after an SVA. Additionally, this provides a valuable avenue to “tell the DSS story.”

A key asset to this process, as well as our field office’s success, is our knowledge of the National Industrial Security Program Operating Manual (NISPOM). One of our CISAs was previously an ISR for 28 years before becoming a CI Agent.

Each CISA in our field office has taken the Facility Industrial Security, level 1 course. This knowledge underlines all of our interactions with cleared facility management and security staff. Understanding the nexus to the NISPOM in all of our actions involving the cleared contractor community is paramount.

When cleared contractor facilities are involved, not everything is a counterintelligence concern, however everything is related to industrial security.

CI Education

Just as we take pains to understand the NISPOM and the industrial security mission, we want to encourage our industrial security and information assurance colleagues to propagate CI awareness

and education. We provide ISRs with CI pertinent questions to ask during interviews of personnel, and solicit feedback regarding other facility issues which may be of CI concern. ISRs are welcome to attend CI education events and briefings at the contractor facilities, and encouraged to ask questions regarding suspicious contacts and the CI process.

Field Office Participation

CI agents in the Andover Field Office are continually seeking ways to integrate into field office activities. Recently, CISAs coordinated the first Andover Field Office Open House, which garnered much positive feedback from cleared industry.

Andover CISAs are well integrated into the field office and enjoy the support of the ISRs, ISSPs, and the FOC. Through consistent communication, actively supporting the industrial security mission, educating our DSS colleagues on the CI mission, and actively participating in field office activities, we have created a culture of collaboration and partnership within our field office, while achieving success in our CI mission.

Together, the Andover Field Office has accomplished one of the highest percentages of cleared contractor reporting, identifying potential penetrators of the defense industrial base, and mitigating CI vulnerabilities. We believe this internal partnership is integral to our continued success.

(Frank Bonner, CI Special Agent in the Andover Field Office, contributed to this article.)

DSS Helps Feed Families During Sixth Annual Campaign

By Shobha M. Ramaswamy

Capital Region Office, Industrial Security Field Operations

"We make a living by what we get. We make a life by what we give."
— Winston S. Churchill

The Defense Security Service joined the 6th annual government-wide "Feds Feed Families" campaign this summer to donate food and help combat hunger in local communities across the country.

The U.S. Department of Agriculture (USDA) led the campaign, running from June through the end of August, with support from the Department of Defense, Chief Human Capital Officers Council and other federal agencies. The campaign is a voluntary effort undertaken by federal employees to bring nonperishable food items to their offices for distribution to local food banks.

Since the campaign began in 2009, Federal workers have donated and collected 24.1 million pounds of food and other non-perishable items to support families across America. According to the USDA, food banks traditionally encounter lulls in the level of giving due to holidays and other demands on donors' time.

This year's campaign was a huge success for DSS. The agency collected over 3,300 pounds of non-perishable donations nationwide, exceeding its goal of 2,500 pounds. Non-perishable and monetary donations were provided to over 25 food banks and non-profit organizations around the country.


In the National Capital Region, donations were made to the Capital and Maryland area food banks, which serve more than 700 food pantries, soup kitchens and other service organizations in Washington, D.C., Virginia, and Maryland. In addition, several monetary donations were made by DSS employees to various food banks and non-profit organizations.

New this year to the campaign were opportunities to "glean." Feds Feed Families partnered with farmers across the country to prevent the unnecessary wasting of produce and simultaneously provide access to fresh and nutritious foods for low-income populations through gleaning.

Capital Region DSS employees participated in several gleaning events with the Mid-Atlantic Gleaning Network (MAGNET), bagging several hundreds of pounds of produce from the fields at Miller Farms in Clinton, Md., and at the MAGNET warehouse in Cheltenham, Md. The food was subsequently distributed to food banks in the Mid-Atlantic region.

DSS offices nationwide made the DoD Hall of Fame 2014 by donating to the campaign. The Hanover Field Office and the Personnel Security Management Office for Industry team, "Hanover Souperstars," in Hanover, Md., raised the most donations in the agency, with over 700 pounds of donations to the campaign, earning them "Gold" Hall of Fame status.

By the Numbers



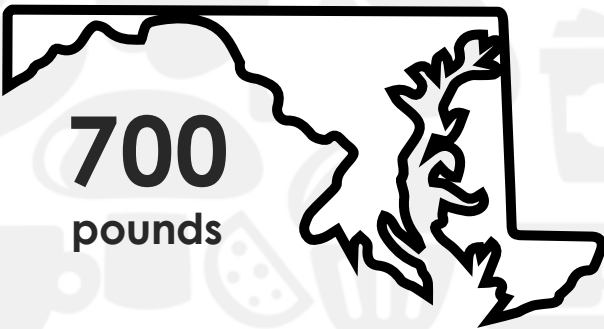
3,300
pounds

of non-perishable
donations collected
nationwide by DSS



25

food banks and non-profit organizations
around the country received non-perishable
and monetary donations



700
pounds

of donations collected by the Hanover
Field Office, the most in the agency



CLOCKWISE, FROM TOP: DSS Hanover, Md., Office "Superstars" donated over 700 pounds of food to the 2014 FFF Campaign. DSS Andover, Mass., & Northern Region Office "Northern Stars" donated over 250 pounds of food to the 2014 FFF Campaign. Laura Baker (right, Capital Region Senior Action Officer) & Pam Hunter (Hanover-1 Field Office Chief) gleaning at Miller Farms.



Defense Security Service