DSS ACCESS

Official Magazine of the Defense Security Service | Volume 7, Issue 2

THIS ISSUE

Assessing the implementation of the first phase of DSS in Transition

DEFENSE SECURITY SERVICE | PARTNERING WITH INDUSTRY TO PROTECT NATIONAL SECURITY

DSS ACCESS

Published by the
Defense Security Service
Public Affairs Office

27130 Telegraph Rd.
Quantico, VA 22134

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

DSS LEADERSHIP

Director | Dan Payne

Chief of Staff | Troy Littles

Chief, Public Affairs |
Cindy McGovern

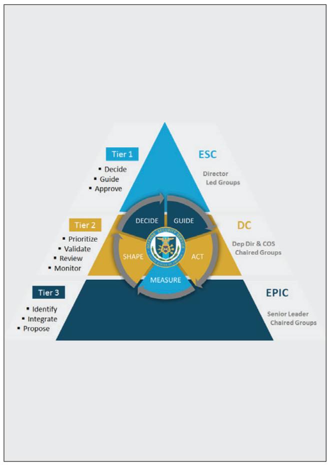
Editor | Elizabeth Alber

Layout and Graphics |
Marc Pulliam

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

The views expressed by the authors are not necessarily the official views of, or endorsed by, the U.S. Government, the Department of Defense, or DSS.

All pictures are DoD photos, unless otherwise identified.



COVER STORY: ASSESSING THE IMPLEMENTATION OF THE FIRST PHASE OF DSS IN TRANSITION (DiT)

INSIDE

DIRECTOR AWARDS

ASK THE LEADERSHIP

From the Director

I held a town hall in mid-April where I shared my top priorities with the DSS workforce. I said at the time that I expected some decisions within the next few weeks so I am very aware that anything I say here may be overcome by events before this is even published. But I want to share some of those comments and thoughts here.

DSS has a unique perspective to, and relationship with, our industry partners. As a result, DSS is a key player in the protection of critical technology; in fact, I would argue, we are the preeminent authority on the subject. I want to leverage this relationship and the institutional knowledge we have to play a larger and earlier role in the acquisition process. The protection of critical technology is an integral part of our core mission, and I will continue to push to have DSS input and expertise incorporated into senior level DoD decisions.

This is also why we must continue to implement a new assessment methodology. I know there is some angst in the field and within industry, but as you can see from the articles in this issue, we are taking a very careful, methodical approach to this and incorporating lessons learned as we go. I know the new approach is taking up a lot of resources right now, but that's because we are all learning. We will get better at this and the process will get faster and more agile. Our first set of assessments found concerns we would not have found under the old protocol, further validating the need for the change and the value in looking at key technologies from a cross functional approach.

I also want to highlight two other agency initiatives that we are working on: the uncompromised delivery of products to the warfighter, and a different approach to assessing foreign ownership, control, or influence (FOCI). In discussions with industry, it's clear that many companies treat security as a cost center, not a profit maker. As a result, security may be understaffed and underfunded. Our goal is to make security the fourth pillar of the acquisition process (along with cost, performance and schedule). If we can make that paradigm shift, security then becomes a differentiator in acquisition decisions rather than a cost drain.

In regard to FOCI, we may not be looking at the totality of FOCI and missing the actual threat. Traditionally, we linked FOCI to ownership and management concerns, but that's not the only kind of influence foreign countries can exert. We're finding influence can come from foreign sales, or foreign products embedded in the supply chain. We are just beginning to delve into this but I think this aligns with our new assessment approach and ultimately our core mission of protecting critical technology.

Finally, I want to touch on the background investigation mission. As a result of the National Defense Authorization Act for Fiscal Year 2017, DSS developed a three-phased approach to assume the DoD background investigation mission from the National Background Investigations Bureau. Since then, there has been discussion at senior government levels of moving the entire NBIB infrastructure and mission to the Department and DSS. Regardless of the final decision, it is clear that the current system used to vet personnel for positions of trust is no longer sustainable. Whether the mission comes to DSS in total or in part, we must develop a new way of vetting personnel. We must also develop a comprehensive plan to merge this new mission and infrastructure into DSS. A key component of any merger will be the expansion of our support staff to facilitate the transfer. Again, I don't know yet what this change will look like for DSS, but I urge everyone to remain flexible and not to be distracted by the latest new idea or plan that is floated.

Thank you for all you do.

Dan Payne
Director

Assessing the first phase of DSS in Transition (DiT) implementation

by John B. Massey
Industrial Security Field Operations

In 2017, DSS began an enterprise-wide change initiative called "DSS in Transition" (DiT). The goal of this effort was to begin moving DSS from a schedule-driven compliance model of industrial security oversight to one that is intelligence-led, asset-focused, and threat-driven. To help facilitate this change, DSS established a Change Management Office (CMO), which led multiple initiatives and working groups comprised of a cadre of professionals and subject matter experts representing each agency directorate. These groups worked tirelessly for over a year in developing a concept of operations for the new methodology.

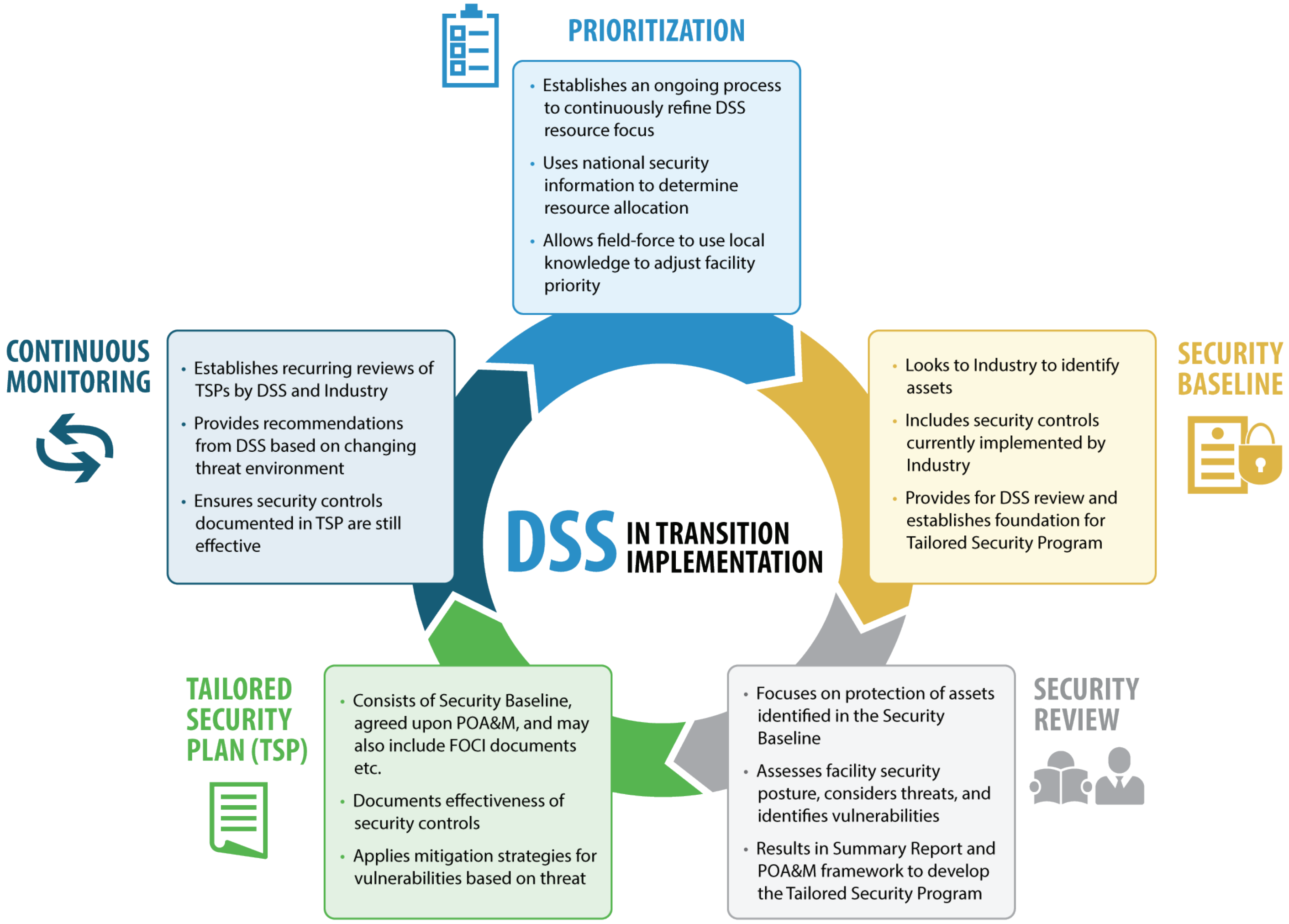
The new model identifies assets at each cleared facility, prioritizes those assets and facility engagements based on national intelligence information, considers threats and vulnerabilities, and partners with cleared industry to develop tailored security programs. In January 2018, DSS began implementing the new methodology in an incremental way, starting with the selection and review of four cleared facilities supporting top priority technologies.

One facility was selected in each of the four DSS regions. A cross-functional team of industrial security, industrial policy, information systems, and counterintelligence professionals then conducted a comprehensive risk-based security review of each facility. The DSS team used a security baseline to identify assets and associated security controls, conducted a security review to examine vulnerabilities and compliance with the National Industrial Security Program Operating Manual (NISPOM), and worked with industry participants in developing a tailored security plan.

The reviews conducted during the first phase of implementation have improved partnerships between DSS and industry participants. Some of the comments received include:

- The entrance briefing enhanced the dynamic of the DSS-industry partnership by being more collaborative and providing industry partners with specific threat information.
- There was greater collaboration among DSS team members. Team members communicated and discussed information effectively, sharing a variety of insights and information on the threat, personnel security, information systems security, industrial security, and counterintelligence.
- As a result of sharing threat information, industry participants demonstrated an appreciation of the partnership demonstrated in being provided specific threat information with relevancy to their assets.

The first phase of implementation also included a greater emphasis on government stakeholder engagement. The CMO communicated the implementation plan to a core group of overnment stakeholders and DSS leaders briefed the stakeholders on implementation efforts in March 2018. Further, review teams from the first phase coordinated with Government Contracting Activities in advance of security reviews to gain a better understanding of their priorities and how the participating industry contractors support their higher priority programs. This dialogue led to an improved focus on assets, security controls, and vulnerabilities. It also resulted in a greater understanding for both DSS and the industry partner in understanding the government partner's security expectations.



DSS IN TRANSITION IMPLEMENTATION

PRIORITIZATION

- Establishes an ongoing process to continuously refine DSS resource focus
- Uses national security information to determine resource allocation
- Allows field-force to use local knowledge to adjust facility priority

SECURITY BASELINE

- Looks to Industry to identify assets
- Includes security controls currently implemented by Industry
- Provides for DSS review and establishes foundation for Tailored Security Program

SECURITY REVIEW

- Focuses on protection of assets identified in the Security Baseline
- Assesses facility security posture, considers threats, and identifies vulnerabilities
- Results in Summary Report and POA&M framework to develop the Tailored Security Program

TAILORED SECURITY PLAN (TSP)

- Consists of Security Baseline, agreed upon POA&M, and may also include FOCI documents etc.
- Documents effectiveness of security controls
- Applies mitigation strategies for vulnerabilities based on threat

CONTINUOUS MONITORING

- Establishes recurring reviews of TSPs by DSS and Industry
- Provides recommendations from DSS based on changing threat environment
- Ensures security controls documented in TSP are still effective

Planning was one of the key factors contributing to the success of the first phase of implementation. Review teams conducted rehearsal of concept drills to discuss roles and responsibilities and obtain threat vector and technical guidance from subject matter experts in order to better understand technologies and associated threats. This was beneficial to both the DSS team and the industry partner who had a better understanding of the focus and scope of each DSS team member's review.

Following the first phase of implementation, DSS will pause to assess the process and incorporate lessons learned. Best practices and other adjustments and refinements will also be incorporated into the methodology for the second phase of implementation. The second phase will involve the comprehensive risk-based security review of two cleared facilities per region, for a total of eight. The third phase will follow with 16 total reviews and the fourth and final phase will comprise 32 reviews.

DSS will pause after each additional implementation phase and continuously seek ways to improve the process. By the end of 2018, DSS will have reviewed approximately 60 facilities under the new DiT methodology. Concurrently, DSS will conduct a training needs analysis that will help inform the long-term training required for industry, Government partners, and DSS personnel.

After a year and a half of work, 2018 will continue to be a year of transition for DSS. The change that has led this transition is driven by the recognition that while it is an excellent security foundation, the NISPOM does not go far enough in protecting our critical technologies and assets from loss or compromise. The new DiT methodology has taken that foundation and built upon it, and industry's continued involvement and feedback will be invaluable to a successful DSS transition.

In their own WORDS

Editor's Note: *Kevin Flowers is the Field Office Chief of the San Francisco Field Office. Steve Eisenberger is a Senior Industrial Security Representative in the Philadelphia Field Office. Both were region leads for Phase I of the DiT initiative which piloted the new assessment methodology at one facility in their area of operation. The following, in their own words, are lessons learned and experiences to help the next team become familiar with the new methodology.*

Kevin Flowers

We were under some pretty strict time constraints as a result of the Operational Training Event (OTE), which was held in early April in San Diego. We wanted to conduct the assessment and capture the lessons learned so we could share them at the OTE and we knew we had a difficult challenge ahead of us.

One of our first concerns was in picking the correct facility to test this on. We wanted to pick a small facility, but also one large enough that it would provide a good training event and baseline. So we picked one, but ultimately went with a different facility that was a manufacturer with about 100 employees.

We did a tremendous amount of work upfront. We had to work very closely with the facility to get their buy-in. Like many smaller companies that we see in the National Industrial Security Program, the facility security officer (FSO) wore many hats. And, the classified work this company did was just a small portion of their business; most of it is with commercial customers, not the government. I knew our DSS footprint was going to be larger than our normal assessment and I didn't want to overwhelm them. In fact, as we went through the process we found the FSO wasn't the best person to help us. We needed to talk to the senior management official (SMO) and the technology people to understand the business process flow at the company. The SMO ended up being the most helpful at the company. Fortunately the company was willing to participate and was eager to protect their information.

Our first challenge was the identification of assets and security controls. This process took about a month. We didn't know it at the time, but this was during a major technology conference for the company and we were dealing with possible furloughs at DSS, so the process ended up taking much longer than we expected.

We also didn't expect the business flow we found at the company. Our vision turned out to be totally wrong. We had expected a linear step-by-step process, when in fact, it was totally non-linear with many inputs from different departments. And again, the company actually possessed very little classified information so this was unfamiliar territory for the company as well. In fact, the company became frustrated at the effort at times and began to think we were asking for too much information. We spent a lot of time coordinating with them.

Ultimately, I think we made a good choice with this company and it provided a good foundation for us moving forward.

Everyone in the field office was involved in the process as well as the regional operations manager for a total of about 15 DSS employees.

Normally, when doing a team assessment, each subject matter expert does their own thing and the team meets at the end of the day to share their findings and bring the team lead up to speed. We knew in this case, that we wanted to do cross functional interviews so each specialist [industrial security representative, information systems security professional or counterintelligence special agent] had to know what their counterparts were interested in.

Working through the steps, we found we needed to coordinate much more in advance of the assessment; for instance who would take the lead on which interview, how would others interject, etc. We found ourselves mapping out the interviews in advance. Given our time constraints with the OTE, we didn't finish the tailored security plan with the company so we still have to do that.

The company actually was very pleased with the review. They said we had some good recommendations and they've agreed to put increased security controls in place. We have also seen a marked increase in their suspicious contact reporting; more than in the past three years combined. The SMO has also bought into the new process and agreed to invest more in the security staff, so I see a lot of wins here.

Our next step for the region is to select two more facilities. We had pulled in people from across the region for our pilot, so the next field office won't have to start from scratch. And our field office can serve as consultants as needed and provide lessons learned and also subject matter expertise.

We will also share our lessons learned at the OTE as I will be serving as one of the facilitators. The OTE will present the concept of operations to the entire field workforce, but we can provide insights since we implemented the process. Hopefully we can add some nuggets of wisdom.

Steve Eisenberger

The comprehensive security review was very much different than the traditional NISPOM compliance-based security vulnerability assessment. Extensive pre-security review research, planning and coordination with the team members, risk owner and prime contractor was conducted. Several meetings and phone calls with the facility senior management staff was completed to facilitate company buy-in on the process and to explain the comprehensive risk based security review vice the traditional NISPOM compliance-based assessment.

The pre-security review planning was needed to conduct the security review in an efficient and timely manner. Detailed and comprehensive planning in order to conduct the security review is imperative in this process. Facility buy-in, particularly if the facility is a small, non-possessor (as was ours) as the amount of time required of the facility in the comprehensive risk based security review process is more extensive than a traditional NISPOM-based review, is critical.

The meeting with the SMO and FSO in advance, as well as the detailed explanation of the asset identification and security control process that created the security baseline was extremely helpful to the facility in identifying their critical national security assets. The baseline was provided as requested, and the FSO and facility staff obviously worked hard to produce a well thought out baseline. The identification of the three key assets by the facility allowed the DSS integrated team to organize the security review and divide the team into three separate inter-disciplinary groups each independently conducting the review of the identified assets: People, Information and Operations/Suppliers. The team was able to complete the review in an efficient manner in large part due to the security baseline provided by the facility and because of our extensive pre-security review planning.

Eight vulnerabilities without citation were identified that previously would not have been identified under a traditional NISPOM-based approach. Several recommendations were made and it is anticipated there will be suspicious contact reporting due to the contributions of team members who heightened overall security awareness at the facility. It is imperative to have involvement of the counterintelligence special agents (CISA) as they can provide threat data for the review that will heighten overall security awareness of the facility as well as the DSS team members. This contribution may result in an increase in not only the quantity but also the quality of suspicious contact reporting. The facility has provided seven or eight potential suspicious contacts since the conclusion of the security review and these are under review by the local CISAs.

The facility submitted their response to the plan of actions and milestones (POA&M), and the team is in the process of reviewing these replies to determine their adequacy to mitigate the identified vulnerabilities and the adequacy of the response to the recommendations. Once the review is completed, the team will work with the facility to create the facility specific tailored security plan (TSP).

The vast majority of vulnerabilities and the potential loss of national security assets likely come from the exploitation of facility's unclassified computer systems. The information systems security professionals (ISSPs) who participated in this security review were instrumental in identifying these vulnerabilities that could be mitigated relatively easily and without an inordinate amount of time and effort from the facility. The SMOs agreed that these identified vulnerabilities and recommendations were noteworthy not only to protect national security assets but their own intellectual property; their lifeblood. The rehearsal of concept (ROC) process, while well intended, was scheduled prematurely in our case. It was virtually impossible to complete it prior to having the security baseline without identified assets and security controls. In our office we conduct a ROC prior to every team review, we just call it a pre-inspection team meeting. It's the same concept but semantically different, but the ROC in this case was scheduled before the team was in a position to discuss specific team member assignments.

One area that needs significant improvement is the security baseline and POA&M templates. We did not find them to be user friendly and there was an over reliance on using cumbersome spreadsheets. Since DSS is venturing into a new way of business, it's expected that there will be bumps in the road. Phase 1 should be used as a roadmap to streamline and improve the security review process and to more adequately protect our critical national defense assets.

Employees, teams receive recognition at annual award ceremony

The seventh annual Director Awards ceremony, held in March, recognized those employees who exhibit the highest standards of excellence, dedication, and accomplishment in advancing the agency's mission during the calendar year. Awards were presented for Humanitarian of the Year; Excellence in Innovation of the Year; Team of the Year; Employee of the Year; and Employee of the Year Senior.

During the event, La Shawn Kelley, chief of the Human Capital Management Office (HCMO), was recognized as a recipient of a Presidential Rank Award, Meritorious Senior Career Employee for 2017.

"These past nine years, I have been fortunate to be at the helm of a team of human resources professionals," Kelley said. "It is because of them, all they have done and the countless hours spent advancing the DSS mission, that I am standing here today.

"I look back on my career at DSS with pride," she continued. "This moment is a significant milestone and a collective achievement by HCMO, for which I am forever grateful. I'll end with a most sincere and profound thank you."

In his opening remarks, Dan Payne, DSS Director, said of the Director Awards program, "During a time of transition, is it more important than ever to keep employees engaged and demonstrate to them that their work is vital to the agency's overall success. The Director Awards Program embodies attributes that shine a light on the great work we accomplish every day; it validates the impact our products and services provided to both industry and the community; and conveys our work ethics and dedication to the mission."

Payne continued, "This is an exciting time for us to recognize our outstanding employees on their successes and contributions to the overall mission. Whether you were an award recipient or an award nominee, you competed among a group of highly competitive employees and teams, and this program is a win-win for us all.

"As managers and leaders of DSS, we should continue taking a vested interest in the recognition of our workforce by supporting the Director Awards Program, which inspires, motivates, and encourages the highest levels of performance excellence," he concluded.

Employee of the Year

The Employee of the Year award is presented to the DSS employee who best exemplifies initiative, has made outstanding contributions, and whose achievement created sustainable results that most advanced the agency's mission. The winner of Employee of the Year for 2017 is Andrew Winters,

Employee of the Year Andrew Winters (left), Industrial Security Field Operations, stands with DSS Director Dan Payne.

Regional Action Officer, Capital Region, Industrial Security Field Operations.

Winters was instrumental in building partnerships as the agency project manager for a foreign ownership, control or influence threat, vulnerability, impact (TVI) experiment. He led a multi-disciplinary team to develop new processes to evaluate a broad range of TVI information to employ strategies to mitigate risk. He briefed DSS senior leaders on the experiment's progress, and closely coordinated with the DSS Change Management Office to ensure his team's efforts directly aligned with DSS in Transition efforts. Additionally, he closely collaborated with the cleared company to maintain their active participation in the successful completion of the first risk assessment, spurring development of a tailored security plan.

In accepting the award, Winters said, "I am truly honored and have been very fortunate to be given a number of opportunities to excel."

He continued, "As some may know, I suffered a personal loss this past year, and the support I received from within the DSS family was extremely important and ultimately critical to my success. That support we can provide to each other will be more important than ever as we face resource constraints and other challenges during this period of transition.

"The support from the family we have outside DSS is also very important, and I'll be thanking my family, and ensuring they know how much I appreciate them, later," he said.

Employee of the Year Senior

The Employee of the Year Senior award is presented to the DSS employee who exhibits the highest standards of excellence, dedication, and accomplishment in support of advancing the DSS mission. The winner of Employee of the Year Senior for 2017 is Keith Minard, Industrial Security Integration and Application.

Employee of the Year Senior Keith Minard (left), Industrial Security Integration and Application, stands with DSS Director Dan Payne.

Minard wrote national-level security policy; shaped a risk assessment product line for DSS; and his thorough knowledge of policy and his ability to develop clear-eyed strategies helped set the stage for the first jointly produced tailored security plan. He influenced policy within the inter-agency and with the Information Security Oversight Office, responding to more than 500 responses to policy questions posed by the DSS workforce, government customers, and industry partners. He served as the policy "face" of DSS and DoD with government and industry stakeholders through his support of several associations and was viewed by all as a trusted officer attentive to government needs and industry equities.

In accepting the award, Minard said, "I've got to highlight the IP Policy staff for all the work they do for me to be successful. My job gives me the opportunity to work with agency information systems security professionals, industrial security representatives and counterintelligence special agents, as well as external agencies to accomplish the mission. It's important that we work together."

Minard continued, "The bottom line is that it takes collaboration and partnership for us all to be successful."

Team of the Year

The Team of the Year award recognizes teams who, as a group, exhibit the highest standards of excellence, dedication, and accomplishment in support of the DSS mission. The 2017 Team of the Year is the National Defense Authorization Act for Fiscal Year 2017, Section 951 Core Team.

The Section 951 Core Team's work directly contributed to Congressional language, forwarded to the President, and subsequently signed into law. This team authored the Secretary of Defense's response to congressionally mandated language to develop plans

2017 Team of the Year/NDAA 2017, Section 951 Core Team members:

Thomas Badoud, *Counterintelligence*
Derrick Broussard, *Industrial Security Integration and Application*
Michael Buckley, *Counterintelligence*
Nancy De La Garza, *Industrial Security Field Operations*
Matthew Guy, *Counterintelligence*
Heather Sims, *Industrial Security Field Operations*

and reports in support of transferring government investigative personnel and contracted resources from the National Background Investigations Bureau (NBIB) to DoD. This effort included guidance for DSS to conduct background investigations (BIs) for DoD and an estimate of the number of full-time equivalents required to carry out the plan. The plan consists of three phases and was structured using new and innovative methods related to BI execution, in sync with the Department's National Background Investigation Service development. It was designed to transform DoD's investment in its personnel security clearance portfolio to achieve timely, responsive, high-quality security and suitability investigations that ultimately lead to informed adjudicative determinations. The team collaborated, co-authored and submitted the congressionally mandated reports ahead of schedule, and oversaw the coordination process, resulting in the Secretary of Defense's signature and delivery to Congress. As a result of the team's efforts, DSS is positioned to accept and execute a national security mission valued in excess of $1 billion, affecting every federal agency, and significantly transforming DSS operations and organization.

In accepting the award on behalf of the team, Michael Buckley, Counterintelligence chief of staff, said, "It was a very challenging, but very rewarding year. The burgeoning background investigation mission build has been and will continue to be an opportunity for everyone to excel.

"We've been at this now for 14 months, 4 days, 5 hours and about 11 minutes, and I know some of you may feel a little Section 925 fatigue," he continued. "And I know there are some of you who may take a deep breath before answering a phone call from us, but please know that we push for a reason. Not because Congress is watching; not because DoD invests a billion plus dollars a year on this mission – granted, these are good reasons, but we need to get this right.

"We are positioned and responsible for determining how DoD will define what a successful background investigation looks like and how that will fit under the larger construct of the Department's personnel vetting mission," Buckley said. "Much has been done – this award recognizes those efforts. But there is much still be accomplished."

Members of the 2017 Team of the Year, National Defense Authorization Act 2017, Section 951 Core Team, stand with DSS Director Dan Payne.

Excellence in Innovation of the Year

The Excellence in Innovation of the Year award is presented to an individual or team that develops and implements innovative products, services, processes, or technologies to meet new or existing requirements, articulate needs, and improve the way government operates. The purpose of this award is to develop new solutions that go beyond marginal improvements in existing products, services, processes or technologies. It is designed to encourage dialogue across the community, challenge peers to think and work differently, and take calculated risks to move government in a new direction.

The winner of the 2017 Excellence in Innovation of the Year is the DSS in Transition Methodology Development Team (MDT). The team created an operational framework that includes industry identification of assets, threat information shared between DSS and industry, identification of vulnerabilities that impact the delivery of uncompromised products, and the creation of tailored security plans that outline the acceptable risk at industry sites. The cross directorate team included representatives from Industrial Security Field Operations, Industrial Security Integration and Application, Counterintelligence, and the Center for Development of Security Excellence, and each team member provided insight from their respective business units.

2017 Excellence in Innovation/DSS in Transition Methodology Development Team members:

Andrianna Backhus, *Industrial Security Field Operations*
Elizabeth Bruinsma, *Industrial Security Field Operations*
Virgil Capollari, *Counterintelligence*
Misty Crabtree, *Industrial Security Field Operations*
Joseph Fountain, *Counterintelligence*
Christopher Hartnett, *Industrial Security Integration and Application*
Dustin Sievers, *Industrial Security Field Operations*
Kevin Williamson, *Industrial Security Field Operations*

The MDT framework evolved from concepts received from several integrated process teams, as well as practical exercise feedback into an executable process. The MDT created a new process that includes the creation of over 30 different products, to include a concept of operations, testing procedures, 25 different templates and job aids, interactive data capturing tools to ease the industry time burden, and a toolkit to share tools and information.

In accepting the award on behalf of the team, Andrianna Backhus, Chief, Quality Assurance and Field Support Branch, Field Operations said, “Betsy Bruinsma, the lead for this project, should be standing here. She was given a daunting task, as our team

Members of the 2017 Excellence in Innovation of the Year winners, DSS in Transition Methodology Development Team, stand with DSS Director Dan Payne.

was comprised of seven very diverse personalities who were locked in a room to come up with a new methodology."

She continued by thanking the DSS senior leaders for believing in the team, to include DSS Deputy Director James Kren, "who steered us in the right direction when we went rogue – which was often."

Backhus also thanked her teammates, "we did it together and supported each other. If we stick together, we can do anything."

Humanitarian of the Year

The Humanitarian of the Year award is presented to the employee or team who contributes to human welfare, and improving the quality of life and health of a group of individuals in the United States or abroad. The employee or team nominated must demonstrate significant leadership and outstanding volunteer service accomplishments and through the scope of work undertaken a commitment to humanity and selflessness, without regard to personal or organizational gain or profit. The employee or team established or furthered a legacy and/or sustainable program that is of ongoing value and benefit to others.

The 2017 Humanitarians of the Year award is awarded to Boyd Crouse, management and program analyst at the Center for Development of Security Excellence, for performing as Santa Claus at 35 events throughout the year.

Crouse and his wife (Mrs. Claus) committed over 200 hours to providing cheer and hope to the elderly, infirmed, disadvantaged, and children of all ages through visits to retirement communities, churches, shelters, and women's crisis centers. He supports the Eastside Family Shelter which attends to the needs of hundreds of local families. He also serves the greater Baltimore community and refuses to take any pay, giving any compensation received to the Family Crisis Center of Baltimore County, a private non-profit service agency providing comprehensive and life-saving services to families experiencing conflict and family violence.

In accepting his award, Crouse said, "My wife and I have tried to instill in our three sons the value of giving back, to pay it forward," he said. "As Santa Claus, my efforts are worth it to see that smile and get that hug."

Crouse thanked his wife for all her support, and concluded with, "Many months ahead, Merry Christmas."

The 2017 Humanitarian of the Year Boyd Crouse (left), Center for Development of Security Excellence, stands with DSS Director Dan Payne.

Employee of the Quarter

Recognized during the ceremony were the Employees of the Quarter for 2017:

First Quarter: **Misty Crabtree**, Industrial Security Field Operations

Second Quarter: **Jeff Swafford**, Counterintelligence

Third Quarter: **Andrew Winters**, Industrial Security Field Operations

Fourth Quarter: **Nicole Rhodes**, Headquarters

Employee of the Quarter Senior

Recognized during the ceremony were the Employees of the Quarter Senior for 2017:

First Quarter: **Delice-Nicole Bernhard**, DoD Insider Threat Management and Analysis Center, Counterintelligence

Second Quarter: **Jeffrey Blood**, Industrial Security Field Operations

Third Quarter: **Edwin Kobeski**, Counterintelligence

Fourth Quarter: **Tracheta Irons**, Industrial Security Integration and Application

NOMINATIONS

Nominated for Employee of the Year

William Cooper, Industrial Security Integration and Application

Monica Hurui, Headquarters

Nancy McKeown, Center for Development of Security Excellence

Ronald Wooten, Counterintelligence

Nominated for Employee of the Year Senior

Thomas Badoud, Headquarters

Delice-Nicole Bernhard, Counterintelligence

Jeffrey Blood, Industrial Security Field Operations.

Kimberly Knobel, Center for Development of Security Excellence

Nominated for Team of the Year

Hard Targets and Production Team, Counterintelligence

Insider Threat Team, Center for Development of Security Excellence

National Industrial Security Program (NISP) Authorizing Office Team, Industrial Security Field Operations

International Security Team, Industrial Security Integration and Application

Nominated for Excellence in Innovation

Leadership Advisory Board, Headquarters
NISP Mission Mapping in Support of DSS in Transition Information Systems, Industrial Security Integration and Application

DoD Insider Threat Management and Analysis Center, Counterintelligence

A Q&A with **Booker Bland**, Director, Operations Analysis Group and the DSS Insider Threat Program Manager

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

Booker Bland is the Director, Operations Analysis Group (OAG) and the DSS Insider Threat Program Manager. As such, he oversees two mission sets that emphasize collaboration across the agency, information sharing, gap analysis, and the implementation of solutions using risk management principles to foster interdependent processes to better identify threats and reduce security vulnerabilities internal to DSS and within cleared industry.

Prior to this assignment within the Counterintelligence directorate, he served as a senior industrial security specialist and the functional lead for the National Industrial Security Program (NISP) Contract Classification System (aka DD Form 254 database) within the Industrial Security Integration and Applications directorate. In that capacity, he also provided timely and relevant interpretation of national policy that impacts the NISP and classified information sharing with state, local, tribal, and private sector entities.

Before joining DSS in 2013, Bland served as the Research, Development, and Acquisition policy chief and Insider Threat Program manager within the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) where he published DoD component, Intelligence Community, and Military service policies and issuances. He retired from the U.S. Air Force in 2004, serving as a special agent with the Air Force Office of Special Investigations. Bland served in a variety of security, counterintelligence, law enforcement and staff positions at multiple levels within the military, Federal Government and industry.

Q: Tell us about your background.

During my 34 years of service to the Department of Defense, I have moved around to a variety of positions supporting multiple defense agencies, military service components at installations, major commands, combatant commands and the Office of the Secretary of Defense. In each, I served as a technical subject matter expert for technology protection, security, law enforcement, counterintelligence, and executive protection. I spent 20 years in the Air Force working primarily as a special agent with the Air Force Office of Special Investigations. After retirement, I supported research, development, test and evaluation activities at the Missile Defense Agency and the Counterintelligence Field Activity before ultimately moving on to OUSD(I).

Q: What led you to this position?

The short answer—the challenge, the promotion and ultimately the increased responsibility and influence that came with the position. I observed the position from a distance but candidly admit I knew little about it before I threw my name in the hat and applied. My exposure to the Operations Analysis Group was limited and centered on responding to taskings and queries that came out of their daily meetings. I occasionally sat in on an energetic significant activities briefing so I would be apprised of the previous month's metrics, significant cases, and systemic issues. Having experience in counterintelligence and security give me a nonsensical belief that I would somehow be a "good" fit for the position. Fast forward 30 months and I'm still learning as I go, adjusting on the run, and equipping the next generation of critical thinkers while keeping my finger on the pulse of the agency.

Q: You wear two hats. One is as the director of the Operations Analysis Group. Tell us about the mission of OAG? What should readers know about the office?

In the midst of DSS in Transition, the biggest takeaway I want the reader to know -- especially the personnel doing the work in the field -- is that we are still in business. The 15 OAG reporting thresholds are still active and OAG is still taking cases to identify opportunities for additional industrial security options, counterintelligence leads, and personnel security actions. I also want the reader to know that the OAG is a second chance work center not a second guess cadre. We understand that increased operations tempo can lead to missed opportunities. The pace at which our field personnel are expected to operate means they may not have the ability to spend the desired time on an incident to conduct deep-dive research. The OAG can take the time to pump the brakes, take a second look, and discuss the nuances to ensure we (DSS) didn't miss an opportunity to take additional actions or disseminate the information to an internal or external government stakeholder for their action. The OAG's existence is incumbent upon its ability to flow information in a timely manner across organizational boundaries to promote the protection of classified information in the hands of industry under the NISP.

Q: Your other hat is director of the agency's insider threat program. Can you briefly explain the goal of the insider threat program writ large? How it came to be, etc?

In 2011, Executive Order 13587 required the establishment of Insider Threat Programs in executive branch departments and agencies for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or unauthorized disclosure. Within DSS, the insider threat Programs consists of an integrated capability to monitor and audit information for insider threat detection and mitigation leveraging counterintelligence, security, cybersecurity (information assurance), and human resources information. We also rely heavily on input from the Office of the Inspector General and the Office of General Counsel to ensure we remain cognizant of any privacy and civil liberties issues we may encounter. In addition to protecting classified national security information, procedures are in place to protect controlled unclassified information, and monitor situations with the potential to evolve into a kinetic threat including, but not limited to, counter-productive workplace behaviors. [Kinetic cyber refers to a class of cyber attacks that can cause direct or indirect physical damage, injury or death solely though the exploitation of vulnerable information systems and processes.] Personnel within the program assess risk, refer recommendations for action, synchronize responses, and monitor resolution of identified issues.

Q: Can you explain the DSS approach to insider threat? What are you finding at DSS that you would like to share?

We are extremely interested in protecting the DSS employees, information, and resources. DSS as an agency would like to get left of boom—engage the situation before there is a problem or incident. With that premise, insider threat is somewhat of a misnomer as we liken ourselves to be a Director's assistance program. Preventing a problem is a much better option than responding to one. For that reason we spend a disproportionate amount of time on relatively low-level incidents. We take stock in our ability to intervene at the earliest possible point and bring to light opportunities for first-line supervisor engagements with their subordinates. Awareness and training are equally important to the effectiveness of this program which is why Insider Threat Awareness training is part of the annual required training for all DSS personnel.

Q: What do you tell an employee who thinks you're monitoring their email?

I tell them that "we are!!!" We are monitoring email for signs of patterns of behavior and actions that are indicative of an insider threat. We monitor behaviors and not people unless we have a predicate and legal justification for focused observation. We do not read emails unless absolutely necessary to provide context to an anomalous situation we believe could lead to individuals harming themselves, their co-workers, compromising DSS information, or damaging DSS resources. In every situation we look at only what is necessary to make an informed decision as to the context of the dialog/written exchange, or information technology action. We adhere to individual privacy and civil liberties throughout the process when identifying concerning events, notifying the impacted Insider Threat hub personnel, and ultimately determining what action, if any is taken on behalf of the agency.

What changes do you see coming to the OAG and insider threat missions?

DSS in transition (DiT) is having a major impact on the agency and the OAG and Insider Threat program will not be immune from change. In the near-term, both missions will be under the leadership of my current deputies as I am embarking on a detail to be the DoD Senior Advisor to the National Insider Threat Task Force, National Counterintelligence and Security Center, Office of the Director for National Intelligence. I suspect the 15 thresholds currently used by the OAG, many of which align with a compliance-based approach to NISP oversight will have to pivot to address mission sets with greater priority brought about through DiT initiatives. Whatever the Director and DSS senior leaders deem as important will receive greater attention from the OAG. In that same vein, the DSS Insider Threat program will have to adjust is size, scope, and complexity due in part to pending changes in insider threat policy with greater emphasis being placed on kinetic threat and the influx of personnel to DSS as part of the background investigative mission coming to DSS.

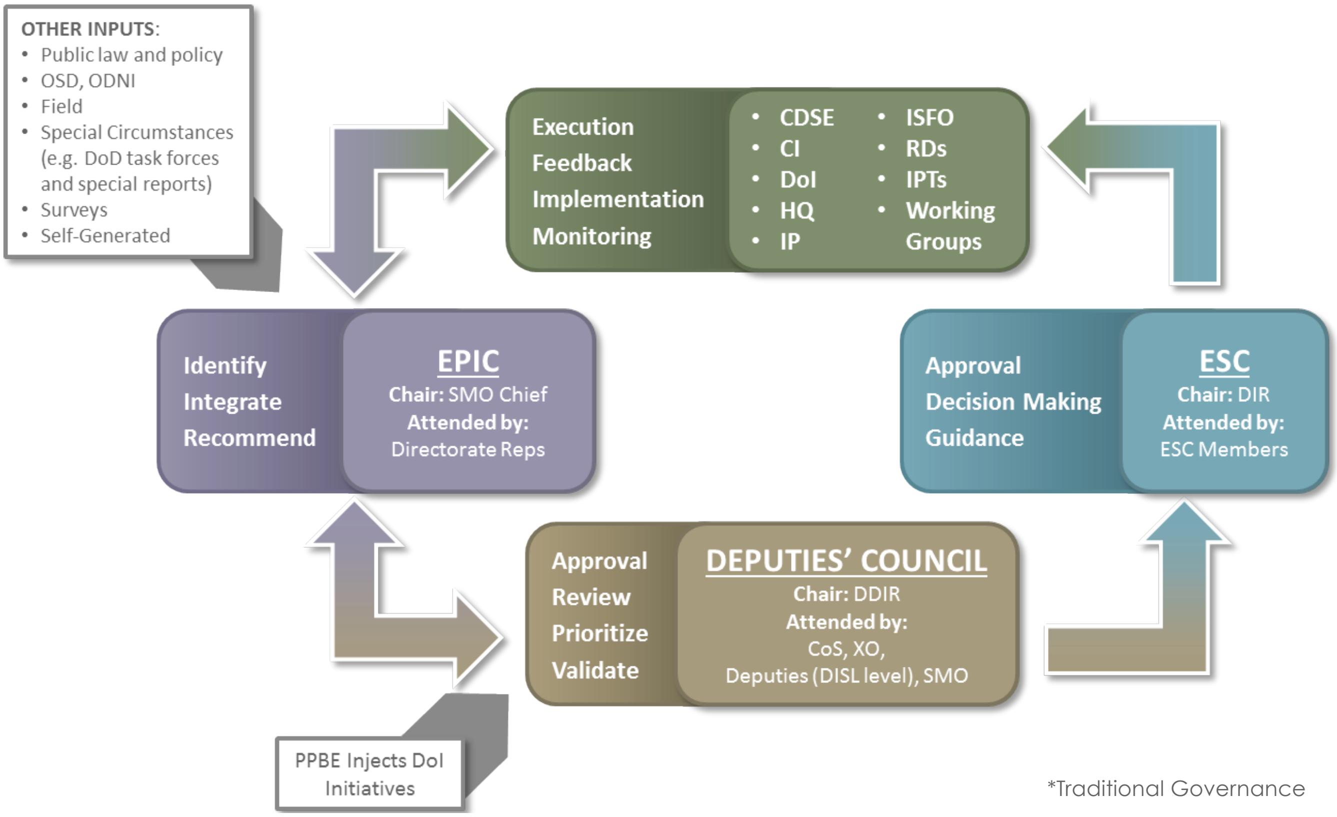
Enhancements to DSS governance provides more access and engagement with decision makers

by Andrew Ivanchishin
Strategic Management Office

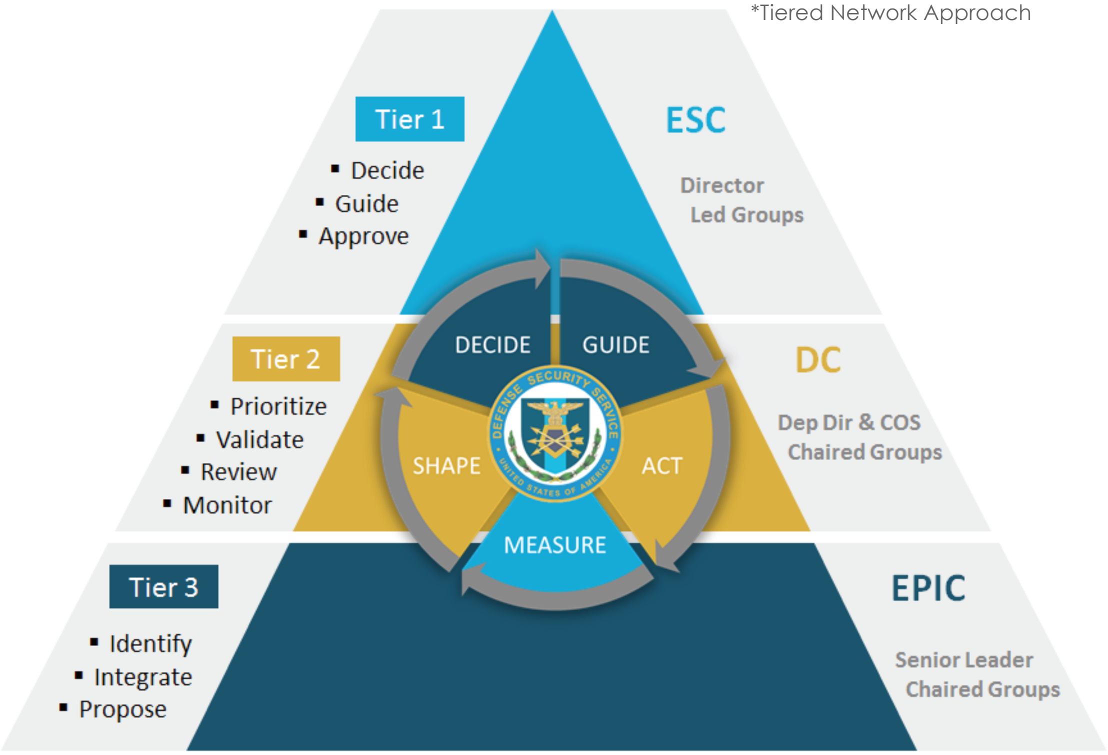
In an effort to increase workforce awareness of agency issues, the Strategic Management Office (SMO) recently implemented enhancements to the DSS governance process.

DSS governance is an organizational process that facilitates senior leader review and dialogue, and enables transparent, informed decision-making on issues, initiatives, and topics with enterprise-wide implications. Agency employees may be familiar with recurring governance meetings if they've briefed senior leaders on issues or presented their respective directorate/division equities. However, DSS leadership recognized the need for a more comprehensive governance process to address mission growth, improve coordination across all levels, and enhance workforce awareness. DSS Director Dan Payne approved recommendations to enhance the sharing of decisions and outcomes from formal governance councils and established integrated planning teams (IPTs), working groups, and panels.

When SMO implemented the enhancements, it changed the governance process. Under the traditional governance structure, issues were reviewed through three formal councils: the Enterprise Planning and Integration Council (EPIC), the Deputies' Council (DC), and the Executive Steering Committee (ESC). The EPIC typically served as the feeder council in this process, as it determines which issues to forward to the ESC or DC where decisions are made. While this structure did ensure a thorough review by directorates and support elements, it did not allow for short-notice inclusion of issues.



*Traditional Governance



*Tiered Network Approach

The recent enhancements involved "growing" the traditional governance structure by identifying IPTs and working groups coordinating on enterprise-wide issues and incorporating them into the process through a tiered network approach. This new approach expanded the existing governance structure from three governing councils to three tiers of governance, linking established IPTs, working groups, and panels coordinating agency initiatives to the EPIC, DC, and ESC. This linkage now offers the flexibility of obtaining thorough directorate and supporting element reviews through the governance councils and quicker, targeted reviews through the IPTs, working groups, and panels.

In the new tiered structure, the DSS workforce has more access to senior leaders and the decision making process without consuming large amounts of time through meetings. Participants in governance, or those empowered to act on their behalf, can receive immediate feedback from senior leaders. Tier 1 groups, like the ESC, are chaired by the agency director and provide decisions on staff-vetted courses of action and new initiatives critical to strategy and operations. Tier 2 groups are typically chaired by the agency deputy director or executive director, like the DC. Tier 3 groups represent all of the IPTs, working groups, boards, and other bodies that conduct business for DSS at the enterprise level. Tier 3 groups represent the majority of discussions in governance, and regularly provide valuable insight and illuminate critical issues to senior leadership.

Critical to enhanced governance is the effective management and dissemination of information from both traditional governance councils and established IPTs, working groups, and panels. SMO established a Knowledge Management Environment (KME) on the agency intranet, which provides all members of the DSS workforce access to a directory of governance councils and ancillary groups, along with links to their respective web pages, resource libraries, and related information. All identified governance groups are organized by tier, along with their chairs or points of contact. Additionally, other governance enhancement products, such as standardized briefing templates are available on the site.

While the goal of these enhancements is greater awareness of governance discussions and decision making, it requires active participation on the part of the workforce to be effective. Recently, DSS Executive Director Troy Littles emphasized that all DSS personnel are obligated to actively seek knowledge from across the enterprise for their own professional development. He then encouraged all members of the DSS workforce to explore the Knowledge Management Environment to maintain their situational awareness on all major enterprise activities and initiatives.

New job aid provides clarity on traditional security for CCRI reviews

by Ehren M. Thompson
San Diego Field Office

Editor's Note: *This job aid was developed by Ehren Thompson with the assistance of Stephen Raymond of the Center for Development of Security Excellence. The idea has roots in an earlier course Thompson had taken at CDSE.*

DSS field offices are seeing the deployment of more and more Secret Internet Protocol Router Network (SIPRNet) systems in industry. The *Command Cyber Readiness Inspection Traditional Security Reviewer Job Aid* was created to provide a greater understanding of the Command Cyber Readiness Inspection (CCRI) process for industrial security representatives (ISRs) and information systems security professionals (ISSPs), who are not certified and trained CCRI traditional security reviewers, but might find themselves having to provide CCRI traditional security guidance. Specifically, this job aid outlines the role of traditional security in CCRIs and the requirements defined in the Security Technical Implementation Guide (STIG) for SIPRNet systems.

Background

The Defense Information Systems Agency (DISA) and DSS signed a Memorandum of Agreement (MOA) on Sept. 9, 2011, which outlines the roles and responsibilities of both agencies, as it relates to CCRIs. DSS currently conducts many of these CCRIs

(for industry) on behalf of DISA, as agreed upon in the MOA. CCRIs are a compliance inspection of Defense Information Systems Networks (DISN). These interconnected computer networks transmit classified information via the SIPRNet. STIGs are published as tools to improve the security, outline requirements, and mitigate risk associated with DoD interconnected computer networks.

Although DSS is the Authorizing Official (AO) for all classified information systems for facilities cleared under the National Industrial Security Program (NISP) and leads many of the CCRI reviews, DISA is ultimately responsible for the management of all DISN circuits, i.e. SIPRNet systems. Therefore, SIPRNet systems must meet both technical and non-technical STIG requirements before an Authorization to Operate (ATO) or reaccreditation can be granted. This is where this job aid is most valuable, as reaccreditation includes meeting traditional security requirements as well as technical controls. And, this job aid can be valuable to both ISRs and ISSPs in helping contractors maintain a successful security readiness posture for SIPRNet assets as well as meeting reaccreditation requirements.

CCRI traditional security

If this past year has shown us anything, it is that the role of DSS is evolving and that the work required of industry is becoming more complex. In order for the field and industry to successfully navigate the current threat environment and mitigate risk, we will need to expand our knowledge beyond the current regulatory guidance, i.e. National Industrial Security Program Operating Manual (NISPOM), in order to mitigate risk, as well as educate the cleared contractor community.

Explaining the traditional security requirements applicable to the secure operation of SIPRNet systems to cleared industry personnel can be challenging, because many see this as a new discipline, when in fact, it mirrors much of what ISRs and CCs are already trained to do. Many of the traditional security requirements defined in the STIGs actually overlap.

However, there are some key differences that both ISRs, ISSPs and cleared industry must be aware of in order to provide accurate guidance and this job aid outlines those key differences. For example, a Continuity of Operations Plan, a SIPRNet specific risk assessment, local incident handling policies, IA Workforce-DoD 8570 training and tracking, etc., are not addressed in the NISPOM but are addressed and required according to the STIGs.

Why we need this job aid

First, the traditional security component continues to be a point of confusion for ISRs and ISSPs. While traditional security is a non-technical STIG requirement, it impacts all other technical aspects of a SIPRNet node. That is why it is equally important that ISSPs and ISRs have at least a working knowledge of traditional security (STIG) requirements. This job aid provides satisfactory working knowledge to the field in a quick and timesaving manner.

Second, it is neither possible nor necessary to train the entire workforce to be certified CCRI reviewers. Nevertheless, field personnel are expected to be able to provide some guidance for all NISP related activities under our cognizance. This job aid will not make a person a certified traditional security CCRI reviewer nor a traditional security subject matter expert, but it can serve as a great starting point and succinct reference for those in the field.

Third, cleared facilities with SIPRNet systems must be reviewed at every risk review. It has been my experience that (CCRI) traditional security concerns are noted at our risk reviews and are left unaddressed at times. This is not because we are not concerned about these STIG vulnerabilities, but rather it is a lack of understanding of what guidance to give. Absent proper guidance, the field will default to the NISPOM as we have been trained to do. However, this NISPOM guidance is often not compliant with STIG requirements. This can ultimately affect the security posture of the system and pose a risk to critical technology.

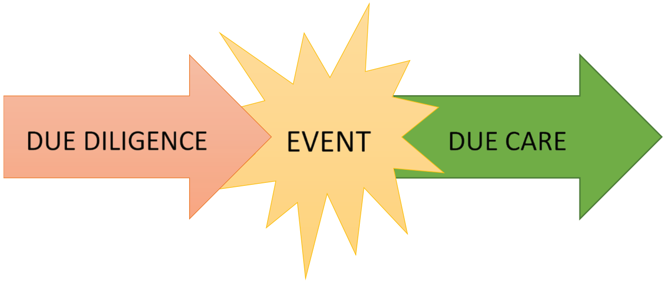
The goal of this job aid is not to increase the workload of our field personnel. In fact, it is the exact opposite. These SIPRNet systems are already in the field. Providing this type of guidance is not outside of our current job duties, but is a logical extension of DSS in Transition. We are all striving to understand and approach security in a more holistic manner that goes beyond our existing compliance-based assessments. This job aid is another tool for us to do our jobs more efficiently and effectively, while partnering to mitigate risk with our industry associates to protect our warfighter and most critical technical assets.

Applying due diligence and due care to information technology systems

by Dustin J. Sievers
Virginia Beach Field Office

Due diligence and due care. Many have heard of them and most have practiced them. But few understand what they mean or how they are applied to information security. Understanding the relevance of these concepts will become important as we move closer to realizing the risk-based approach to security. Opposite sides of the same coin, the terms were borrowed from the legal world to convey the ethical responsibilities surrounding certain events.

Due diligence describes the efforts taken to prepare for a given event while due care describes the actions taken after the event. Due diligence includes the training, forecasting, and planning in anticipation of a certain event done to protect the interests of the organization's mission. Due care encompasses all the relative actions taken after the event; the execution of plans, cleanup and mitigation, and damage control taken in the interest of the same organization. Whereas due diligence is proactive, due care is reactive.



Classified Information Spills

One of the most common examples of due diligence and due care in industrial security is how we prepare for and execute cleanup of classified information spills; i.e., government classified data on unclassified information systems (IS). If you've been around a while you know it's not a matter of 'if,' but rather a matter of 'when' this will happen. Organizations have little to no control over what is sent to them electronically; as a result, they may find themselves on the receiving end of a classified spill and are now responsible, ethically and legally, to clean and protect the classified data on their systems.

Due diligence in this scenario includes the formulation of Incident Response Plans, and if you have a Risk Management Framework (RMF) authorized information system, the RMF package will also include a classified information spill cleanup response plan. This plan will conform to the requirements outlined under security control IR-9 in Appendix A of the DSS Assessment and Authorization Process Manual (DAAPM). Pre-coordination with government customers and obtaining any required checklists to realize their expectation in the event of a spill is also needed. Training, running drills, and ensuring your information technology staff is properly resourced and knows how to run overwrite utilities are all activities included under due diligence.

Due care, in the case of a classified information spill includes performing and reporting of the associated administrative inquiry (AI) within appropriate timelines. Identification and cleanup of the affected systems is a given at this stage. Coordination with the information owner (IO) and their concurrence round out the expectations for due care in this case.

Classified Information Systems

Another common occurrence is obtaining an approved classified IS in the context of the RMF methodology. Receiving an Authorization to Operate (ATO) in Step 5 is the event or dividing point separating your efforts between due diligence and due care.

Due diligence in the RMF process starts with Step 1 (Categorization) and consists of identifying threat events, calculating their likelihood of exploitation and impact, and determining overall risk to the system and information. It also consists of all the control documentation and vulnerability mitigation in RMF Steps 2 (Selecting Controls) and 3 (Implementing Controls). Finally, we can see all of the testing, validation, and flaw remediation in RMF Step 4 (Assessing Controls) that make up the final portion of due diligence before the system is authorized.

DUE DILIGENCE	DUE CARE
Develop Incident Response Plan - **REF: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61v2: Computer Security Incident Handling Guide** **GCA Pre-Coordination** - **REF: Security Classification Guides (SCGs), Statement of Work (SOW), Checklists** **Source Overwrite Tools** - **REF: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88**	Administrative Inquiries (AI) - REF: DSS AI Job Aid For Industry Cleanup - REF: DAAPM Appendix I: Classified Spill Cleanup Procedures - REF: IO-provided Checklists/Actions

Table 1: Due Diligence & Due Care Actions and References for Classified Information Spills.

DUE DILIGENCE	DUE CARE
Risk Assessments - **REF: NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View** - **REF: NIST 800-30: Guide for Conducting Risk Assessments** **System Security Plans** - **REF: DAAPM V1.2 Section 6: RMF Six-Step Process** - **REF: NIST 800-53v4** **Control Implementation, Testing, and Validation** - **SCAP Compliance Checker** - **STIG Viewer**	Continuous Monitoring - Audit Trail Analysis - Patch Management - Changes IAW Configuration Management o REF: NIST 800-128: Guide for Security-Focused Configuration Management of Information Systems Violations: Administrative Inquiries - REF: DSS AI Job Aid For Industry Reaccreditations - -REF: DAAPM

Table 2: Due Diligence & Due Care Actions and References for Classified Information Systems.

DUE DILIGENCE	DUE CARE
Training **Self-Inspections** - **DSS Self-Inspection Handbook** **SOPs, Security Baselines, & Tailored Security Plans**	Plan Of Action and Milestones (POA&M) Vulnerability Closure Vulnerability Follow up Lessons Learned Continuous Evaluation

Table 3: Due Diligence & Due Care Actions and References for Security Vulnerability Assessments.

Due care, after the ATO is received, comprises all of the continuous monitoring actions that occur throughout the course of the system's life. Periodic audit trail analysis and patch management, as well as configuration management make up the due care aspects of an information system. In the event of a security violation, performing an AI and executing a graduated scale of discipline (as applicable) to individuals found culpable can also be seen as due care. Knowing when a security-relevant change is made that triggers a reauthorization action is another example, as is the retention, safeguarding, and/or sanitization of classified information upon the decommissioning of an information system.

Security Vulnerability Assessments

Many security programs rely on their Security Vulnerability Assessments (SVAs) as a gauge of effectiveness and opportunities for improvement, as feedback from the SVA is incorporated into business practices.

Due diligence for SVAs include all the training (received and given), self-inspections, and adherence to established standard operating procedures, baselines, and plans. Adherence to reporting and safeguarding requirements demonstrate the implementation of an effective security program prior to the SVA. Retention of artifacts from other due care efforts also fall under the due diligence and preparedness aspect of SVAs.

Due care for SVAs includes appropriate mitigation of identified vulnerabilities, the development of realistic plans of action, lessons learned, and process improvement that all feed back into the due diligence cycle for the next SVA.

The Economics of Due Diligence & Due Care

As DSS moves forward with risk-based security, the risk assessment becomes all too important to the effort. Whether it's the RMF-required Risk Assessment Report or the DSS in Transition security baseline transforming into a Tailored Security Plan, risk assessments drive the tailored controls that prepare us and encompass our due diligence efforts. Risk assessments have us identifying critical assets, threats to those assets along with their likelihood of exploitation and impact, then formulating risk mitigation as appropriate. Plans to implement mitigations are then prioritized based on importance to the organization and mission.

> “
>
> An ounce of prevention is worth a pound of cure.
>
> **- Benjamin Franklin**
>
> ”

There is indeed a challenge inherent to obtaining adequate resources for security functions; especially those due diligence functions that prepare for things that may or may not happen. Too many times, the security staff is in the shark tank competing for resources by stomping their boots shouting about the potential blood on the floor. Senior leadership only sees the boy who cried wolf; always pointing to a ‘what if’ scenario that may or may not materialize. This is how security programs are under-resourced, and ultimately wither and die. The solution to this challenge is to speak in a language senior leaders can understand; translate needs in terms of resources, such as dollars and cents. Instead of qualitative risk assessments, try using quantitative figures to secure those precious security resources.

Summary

Due diligence is what occurs before the fact; it's how you prepare for what you anticipate. Due care is execution after the fact -- the degree of completion you will attain to contain or put closure on whatever happened. In the world of information security, we have both ethical and legal obligations to perform both. We face a myriad of challenges every day in the shape of known (e.g., SVAs, RMF) and unknown (e.g., classified information spills) events. If due diligence and due care can be leveraged for these events, we minimize interruptions, deliver more confidently, and execute more effectively.

CLEARED CONTRACTORS
working abroad provide unique challenges

by Shawn Case, *San Diego Field Office*, and **Ann Marie Smith**, *San Francisco Field Office*

Cleared contractors living and working overseas operate in high threat environments, often with limited security support. These threats to overseas contractors pose a serious challenge to the National Industrial Security Program (NISP). To mitigate these threats, DSS personnel can provide countermeasures and execute risk mitigation actions. The focus is on two types of contractors:

Long-term visitors at foreign government or foreign contractor sites. Some cleared overseas contractors are long-term visitors embedded with a foreign entity under Direct Commercial Sales or Foreign Military Sales efforts. These employees often function as subject matter experts on an export-controlled technology. They are employed by stateside facilities, which have facility security clearances (FCLs), facility security officers (FSOs), and Insider Threat Program Senior Officials (ITPSOs). Since DSS provides verifications of personnel security clearances (PCLs) on these overseas contractors, metrics on them are institutionally available, including their identities, lengths and locations of assignments, and the technologies involved in their work.

Long-term visitors on U.S. installations or User Agency (UA) sites. The seemingly greater population of overseas cleared contractors are long-term visitors on U.S. installations or with U.S. operational entities. As codified by DoD Industrial Security Regulation and the NISP Operating Manual (NISPOM), they do not store or process classified information in a contractor facility; they operate as visitors under a UA's sponsorship. They are also employed by stateside facilities, which have FCLs, FSOs, and ITPSOs; however, DSS does not provide PCL verifications. Unlike contractor visitors at foreign entities, no metrics are institutionally available on this subset of the NISP contractor population. In this sense, DSS is blind to the size, location and activities of this type of overseas contractor operations.

SO WHAT'S THE RISK?

Cleared contractors working abroad face unique challenges which their coworkers in the U.S. do not face, and they elevate risk within the NISP. The concerns include:

Hiding in plain sight. Contractors who are working in overseas locations often live on the local economy, rent homes from foreign nationals, shop at foreign stores, engage in social activities with foreign nationals, use foreign internet and phone services, and may travel to other foreign countries on weekends or holidays. Thus, their interactions with foreign nationals become commonplace, and their sensitivity to the threat of foreign intelligence entities (FIE) can decrease over time. Unlike their stateside counterparts, contractors abroad are likely to have a larger number of, and more frequent communication with, foreign contacts. However, due to their circumstances, they are less likely to trip insider threat reporting triggers. They may continue suspicious behavior because their interactions appear as normal, not as an exception. Thus, in insider threat terms, they can easily hide in plain sight.

Ease of access by FIE. Foreign intelligence entities find it easier to operate in foreign countries when targeting U.S. citizens. Overseas, FIE can blend in and penetrate social circles of U.S. persons. Cleared contractors located overseas are attractive targets because they are more accessible, they may be experts in a desired technology, and they routinely socialize with non-U.S. persons. Additionally, U.S. citizens abroad may not be afforded the same privacy protections that they receive when they are in the United States.

Outside U.S. jurisdiction. Cleared contractors overseas are typically outside of U.S. jurisdiction when living in the host country, and U.S. law enforcement has limited ability to support them. For DoD-sponsored persons, the Status of Forces Agreement with the host nation dictates how offenses are handled and determines which law enforcement agency has jurisdiction. Local laws may increase the threat that overseas contractors face if they do not provide privacy protections commensurate with U.S. laws. A host country may even target U.S. contractors by monitoring their phone conversations, internet use and financial transactions.

Outside personnel security investigation (PSI) scoping. Unlike their U.S. counterparts, PSI subjects living overseas can have undetected records in the areas of credit, FBI, INTERPOL, and local law enforcement checks, as well as limited results from Treasury checks. This means that cleared contractors overseas may carry significant records that would otherwise cause concern for their continued access to classified information. However, because these individuals are living abroad, adverse criminal or financial records may not be discovered during normal PSI processing.

Security oversight challenges. By regulation, FSOs for overseas contractors are located stateside, making it difficult for companies to administer NISP requirements and maintain effective insider threat touchpoints with their worldwide workforce. Sometimes a company assigns a local security point of contact (POC), which may keep the stateside FSO informed. But the "dual-hatted" security POC is not usually trained as an FSO, and their performance in the duty is often ancillary to their full-time contract effort.

Likewise, overseas UA security managers may not be well-trained in the NISP and may not understand the need to routinely engage with cleared contractors or to contact FSOs when concerns arise. They may not even be aware of all of the contractors in their area of responsibility because of decentralized contracting processes. These organizational gaps can result in late, or unreported, notifications of suspicious incidents, and onsite reports made to the UA may not be communicated to the company FSO or ITPSO. Without this involvement, the company's Insider Threat Program does not engage to allow proper personnel security management.

TAKING A RISK MANAGEMENT APPROACH

DSS does not maintain an overseas presence. However, by taking an asset-focused, intelligence-led and threat-driven approach, DSS personnel may propose countermeasures or execute risk mitigation actions in response to the risks associated with overseas contractor operations.
The possibilities include:

Institutional responses. Blossoming DSS programs, including the DoD Insider Threat Management and Analysis Center, NISP Contract Classification System, the personnel security investigations mission, and Continuous Evaluation could all be leveraged to address the risks associated with overseas contractors. Each program may evaluate the assets, threats and vulnerabilities to calculate the risks associated with overseas contractor operations appropriate to their mission areas and determine risk mitigation possibilities against costs and benefits.

Field responses. After identifying contractors who have overseas employees and their specific locations, DSS personnel may research the various types and levels of threat which are prevalent in those areas and provide tailored briefings to the impacted facilities. This information may also be used to inform DSS field personnel in prioritizing facilities. A targeted education and training approach may be developed for the contractors living overseas and an engagement strategy with overseas UA security managers may help ensure reporting requirements are being met.

Partnering with industry is key in the effort to identify assets and vulnerabilities associated with contractor operations abroad and to cultivate cost effective mitigation measures. Although DSS personnel are not physically present at these overseas locations to provide security oversight, many risk mitigation options are available and may be developed with current resources to address the elevated risks associated with overseas contractors.

Delivering threat information to industry and the results of those efforts

by Patricia Bourgoyne
Albuquerque Resident Office

2017 was a milestone year for DSS as we began to transition to a risk-based methodology, and we saw many changes to the way DSS representatives had been trained and conditioned. All DSS field personnel, across disciplines, have SIPRNet accounts and have received threat information; but what is being done with that information?

The Albuquerque Resident Office team has been successful in working together to make sense of available threat information obtained in the form of Threat Assessment Reports (TAR), Threat Advisories (TA) and Threat Warnings (TW).   How do we do it? The answer is actually simple: Teamwork and partnership. Communication truly is the key ingredient in our team's success. The Albuquerque team integrates all disciplines into each other's day-to-day activities with the hope that through integration, a fuzzy picture becomes focused. As with any new project or process, we can all expect growing pains and hurdles. One suggestion to overcoming these hurdles is to take a leap of faith, just jump right in and learn as you go. Yes, we may fumble as we learn and grow, but this is normal. The important take away is to learn, grow and adjust. Being able to see the results of our efforts will be gratifying as we step back and see the big picture.

In preparation for scheduling facility visits, our team reviews assigned facilities under our purview and prioritizes them based on an intelligence-led, asset-focused, and threat-driven approach. DSS threat documents, in concert with outreach to industry, are used to identify technology and prioritize facilities based on updated profiles. The prioritized list is intended to be a living, fluid document updated as new and emerging threats are developed and identified. Once the list is complete, the next step in the process is to contact facility security officers (FSOs) and schedule visits to these facilities.

Before each visit, DSS representatives review threat documents that may apply to particular facilities. The industrial security representative, counterintelligence special agent (CISA) and information systems security professional have a roundtable discussion based on these documents to prepare to deliver threat information. This dialogue ensures everyone is on the same page with an understanding of why the facility is in the National Industrial Security Program and the risk to their programs. Ideally, the visit will include not only the FSO, but senior management officials, program managers, and subject matter experts. This is where partnership with industry becomes a key ingredient. Using this model, DSS representatives should be able to confidently leave the facility with an updated profile and a current list of classified programs and technologies that facility personnel support. Facility personnel will gain a better understanding of the threats to their facility and programs as well as receive suggested mitigation actions from DSS.

All DSS representatives have their unique approach to research and delivery of threat documents. Below are some helpful hints that have proven to work for the Albuquerque team:

- **Do your homework.** Prior to the visit, reviewing the facility's profile is key to getting an understanding of their mission. Discussing the TARs, TAs and TWs educates everyone on the threat. The CISA will also provide a history of suspicious contact reports (SCRs) or lack thereof.
- **Don't make assumptions**. Unfortunately, not all FSOs can identify their facility's assets. Inviting key management personnel and program managers to the visits can benefit both DSS and facility personnel.
- **Be patient**. Take your time in discussing the purpose and intent of the visit and the new DSS methodology.
- **Articulate**. Clearly discuss the need for the change. Adversaries are successfully attacking cleared industry at an unprecedented rate; how does this impact the facility, its mission and overall business revenue?
- **Provide examples**. The discussion should be personal with relevant case studies from both DSS and real events at the facility.
- **Ask questions**. What are the assets? How would the adversary attempt to solicit or elicit information/material from the company? What would be the impact of loss to facility assets? Do other contractors support similar programs and technologies?
- **Follow up**. Discuss the meeting takeaways and what actions can be taken towards developing a tailored security program as a result of the delivery.

The Albuquerque team believes that as we continue implementing the new DSS risk-based methodology, more success stories will become apparent. We must all remember to work in unity as teams and partners. We are, after all, on the same side with the same goals – defending our country and technology from adversaries and ultimately protecting our warfighters. Everyone's ultimate goal must be to protect national defense information, deliver uncompromised products and services and provide warfighters an advantage on the battlefield.

Here are some examples of the team's success to implementing the new approach:

A cleared contractor conducted an internal risk analysis after a threat delivery visit. The contractor reported they prepared detailed exit debriefings for departing personnel that includes information about who to contact after an employee departs the company, social media threats and types of information to report.

Another FSO took the initiative to educate herself and her staff with detailed information associated with each classified contract. She did this by creating a form that identifies the program manager for each contract as well as the technology associated with that contract. The FSO's intent was to share the form with DSS in order to provide the agency with clear insight of the technology associated with their facility.

Another New Mexico-based contractor, during a TAR delivery visit, became suspicious concerning a current business opportunity. The contractor reported they had recently been approached by a company who introduced themselves electronically to a representative of the contractor. The information was immediately provided to the CISA who referred the matter to the FBI. Due to the circumstances of the case, it was transferred from the FBI to New Mexico who proceeded with a federal case, ultimately leading to an arrest.

(Paul Godlewski, Albuquerque Resident Office, also contributed to this article.)

Open house strengthens partnership

In February, the Alexandria 3 Field Office held its second annual open house at a General Dynamics facility in Falls Church, Va. During the two-day event, 165 security professionals representing over 100 facilities from the National Capital Region attended.

The goal of the annual open house is to provide industry pertinent DSS updates, create mentoring and networking opportunities for industry partners, and provide an opportunity for facility security officers (FSOs) to meet their assigned DSS representatives.

The agenda and presentations were developed based on feedback the field office received from industry partners, and a desire to ensure the most up to date information was provided. Field office representatives and DSS staff presented information on a variety of topics which included an update on DSS in Transition (DiT), the National Industrial Security System, Counterintelligence initiatives and personnel security. Senior Industrial Security Specialists Dustin Dwyer, Katyna Sampson, Ryan Franklin, and Industrial Security Representatives Brandon Ester, Jamika Sanders, Shala Romandelvalle, and Scott Selchert collaborated in developing the agenda and provided the briefings.

Regional Director Justin Walsh and Field Office Chief Robin Nickel provided opening remarks focused on changes in the agency, region and field office. Counterintelligence Specialists Ryan Rivera and Luke Kuligoski, who support the field office team, provided an extensive overview of the 12x13 threat matrix developed as part of DiT, reporting updates, and cyber security products. Mike Clapp, Region Counterintelligence Chief, supported the effort as well and added various perspectives to the audience regarding threat information.

This year's open house included representatives from the Personnel Security Management Office for Industry (Larry Paxton, Lyn Akers, and Ivory Lawrence) who fielded a multitude of personnel security questions. Paxton further provided an in-depth presentation regarding Continuous Evaluation, clearance timelines, Federal Investigative Standards, and much more.

The presentations were very well received, with many attendees commenting they appreciated the amount of information provided on DiT. At the end of each presentation, a question-and-answer session fostered continued dialogue between DSS and the attendees. Additionally, time was allotted for FSOs to meet their assigned industrial security representative, ask specific questions regarding their facilities, and provide feedback.

Texas A&M achieves counterintelligence excellence

The Texas A&M University System is a recipient of the 2017 DSS Award for Excellence in Counterintelligence (CI). DSS Director Dan Payne presented the award to Texas A&M System Chancellor John Sharp and Texas A&M University System's Facility Security Officer Kevin Gamache at a ceremony on March 28.

DSS established the Excellence in CI Award to annually recognize those cleared companies exhibiting the most impressive CI results and cooperation supporting U.S. Government efforts to deter, detect, and disrupt the theft of sensitive or classified U.S. information and technology by foreign entities.

During the presentation, Payne said, "The need for change is clear. The U.S. is facing the most significant foreign intelligence threat it has ever encountered. Adversaries are using multiple methods of operation and methods of contact to target and steal U.S. technology from cleared industry."

He noted that Texas A&M is one of the nation's premier Tier 1 research universities, and many of the technologies listed on the Industrial Base Technology List are touched by Texas A&M research, development, and education programs. The university takes the protection of these technologies seriously, and has several initiatives to ensure this protection.

DSS employee supports military in Afghanistan

The Civilian Expeditionary Workforce (CEW) allows civilians to use their capabilities, experience, and knowledge as a crucial component of helping DoD accomplish its mission abroad. Current government civilians can volunteer for open positions supporting the U.S. military in foreign theaters.

"I was looking for training opportunities and read about the CEW program," said Sjnecca Maxwell, personnel security manager in the DSS Security Office, who recently returned from a deployment to Afghanistan. "I volunteered for many reasons—the chance to serve with the military, the chance to receive training in new fields that could benefit my career and to get out from behind a desk."

The DoD established the Civilian Expeditionary Workforce policy in January 2009, and since then, thousands of civilian volunteers, including DSS employees, have deployed to assist the military in a variety of locations abroad. The jobs performed by these volunteers have included administrative, engineering, safety, project management, operational support, education, intelligence, security, medical support—an enormous range of categories and job types.

Volunteers often work in high-pressure and austere operational environments, alongside military, contractor, federal civilian, and foreign national personnel.

"The deployment experience offers DoD civilians the opportunity to participate in what is often a life-altering experience, working in an environment where often they are the only ones who have the skills and expertise so greatly needed to accomplish a mission," said Larry Cunningham, Human Capital Management Office leadership development administrator.

Prior to deploying, Maxwell was required to complete specific training and physical requirements. After finishing 20 on-line training courses and a complete medical examination, she traveled to Camp Atterbury, Indiana, for two weeks of residential training, which included immersion training at Forward Operating Base Muscatatuck.

"During this phase of the training, we operated like we were in Afghanistan, to begin shifting our way of thinking," she said.

While undergoing classroom training, field training and simulated exercises, she experienced convoy attacks and simulated firing drills, and attended cultural classes.

"We learned how to escape from a disabled vehicle under fire while returning fire, how to respond if our facility is overrun, and most importantly, how to apply emergency lifesaving first aid," Maxwell explained.

"The program uses Afghan nationals in the training, and I met former teachers, military generals and shopkeepers. We were able to eat with them and listen to first-hand stories of life in Afghanistan," she continued. "Ultimately, the goal of training at Camp Atterbury is to mentally prepare you for life in a hostile combat zone."

> "Ultimately, **the goal of training ...** is to mentally prepare you for life in a hostile combat zone."

Upon completion of the training, Maxwell deployed to Forward Operating Base Fenty in Afghanistan. While Maxwell is a personnel security specialist at DSS, her duties in Afghanistan were that of a physical security specialist or so she thought. "The duties given to me were more emergency management/law enforcement," she said, noting among her duties were acting as the security liaison between contractors, military and civilians; maintaining the annual inspection requirements for several federal buildings; overseeing physical security and crime prevention; and coordinating security for events on base.

"Anytime we had mass gatherings, additional security was required," she explained. "My job was to build the security plan and coordinate the contract, military and K-9 security support teams for everything from 5K

> “
>
> I gained confidence in the abilities I now possess, and I gained new skills that will **allow me to be a better leader.**
>
> ”

base continue as planned,” she said. “Essentially, it’s their job to facilitate life on base to include billeting, finance and accounting, COR (contracting officer’s representative) duties for contracts, morale activities and construction.”

She also worked with the base commander on multi-million dollar projects that would affect the base for the next 10 years, as well as working with Afghanis in a Train-Advise-Assist role on power and water management. “While it may seem trivial, nothing can be accomplished without reliable power and water,” she noted.

Being in a combat zone, accommodations were austere and “there was no such thing as comfortable rooms and clean bathrooms. But I was lucky that I didn’t have to live in a tent,” Maxwell said. “I had a room in a hardened building, and shared four shower stalls and four toilets with about 40 women. My building was always hot and located 400 yards from the runway, so it always sounded like a helicopter or plane was about to land on you.

“The food was food,” she continued. “The dining facility did their best to keep us happy; however, the thought of chicken still makes me sad. I think I ate chicken every single way you could prepare it.”

Having served eight months on deployment, Maxwell noted that the most rewarding aspect of it was the accomplishments, whether big or small. “The logistics of the location, and coordination with our Afghan counterparts often made it difficult to get anything done,” she said. “I saw people spend their whole deployment working on a project, only to hand it over to their replacement. Never seeing the finished product of your labor is depressing and demotivating, so we learned to appreciate every accomplishment like it was a Super Bowl win.”

While it was a challenge to get used to a difficult environment without the comforts of home, Maxwell noted the hardest part of the deployment was accepting the reality of the situation.

“I carried a pistol to protect myself and others from people wanting to do us harm,” she said. “We had the threat of ‘incoming’ every minute of the day, and waking up to alarms, forcing you to scramble into a bomb bunker makes you wonder what you are doing over there. In the end, you are sitting with your battle buddy and someone cracks a joke to relieve the stress. Often, it was hard to go back to sleep but eventually, exhaustion wins.”

But in the end, with it all said and done, Maxwell would recommend a CEW deployment to any government civilian. She added that the experience qualifies as a Joint Duty Assignment which will further enhance her career opportunities.

“I would definitely recommend a deployment to others,” she said. “My tour made me appreciate all that I have, and I learned to do more with less, under circumstances that most people would never believe. I gained confidence in the abilities I now possess, and I gained new skills that will allow me to be a better leader.”

INTERESTED IN VOLUNTEERING?

Larry Cunningham advised that the Human Capital Management Office (HCMO) is in the process of establishing a formal structured DoD Expeditionary Civilian (DoD-EC) program at DSS and is currently in the design and development phase. He related that the DoD-EC program has a number of requirements that DoD components must implement in supporting this initiative, and must have them in place by Oct. 1, 2018.

Cunningham noted that the DoD-EC program has some strict screening requirements; including medical, dental, and physical examinations. He added, “Experience has shown that most agencies recruit three individuals for every one EC position due to ‘wash-outs’ who fail to meet all requirements and expectations. It’s not a program that every individual can apply for and if selected you can expect working seven-days-a-week with extended hours in austere environments.”

The DSS workforce can expect to see a communication campaign soliciting recruits for the fiscal year 2019 CBV pool, concluded Cunningham.

DEFENSE SECURITY SERVICE | PARTNERING WITH INDUSTRY TO PROTECT NATIONAL SECURITY