DSS ACCESS

Official Magazine of the Defense Security Service | Volume 5, Issue 4

Implementing Industry **INSIDER THREAT** Programs

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: Insider Threat

INSIDE

ASK THE LEADERSHIP

AROUND THE REGIONS

From the Director

As we close out the year, it's time to set our sights on the future. Looking ahead to 2017, it is clear - change is happening in DSS. We are undertaking a fundamental change in how we do business. Where we once focused on schedule-driven compliance, we are moving to an intelligence-led, threat-driven approach to security oversight.

This will require us to change how we think, act, and help cleared industry protect national security information. Change is always difficult; however, I'm confident we will thrive during this transition. We must begin by meeting the following four challenges.

First, we need to begin to change now. The United States is facing the most significant CI threat it has ever encountered. Our adversaries are successfully attacking cleared facilities at an unprecedented rate. Our new methodology will help us counter this threat, and included in this issue is an article that provides more details.

Second, we need to recognize that change presents a powerful opportunity for professional development and personal growth. The DSS transition will require everyone involved to sharpen their critical thinking skills, develop solutions to a changing environment, and be open to new ways of thinking.

Third, we need to share the same vision for DSS. Our vision is to help ensure contracted capabilities, technologies, and services are delivered uncompromised. This one sentence captures precisely what the future of DSS is all about. To achieve this vision, we are developing a new methodology based on:

- Knowing the assets at each cleared facility
- Analyzing and considering threats to those assets
- Understanding business processes related to assets
- Determining vulnerabilities to assets
- Implementing countermeasures to address the threats
- Developing tailored security programs
- Conducting continuous reviews of tailored security programs
- Comprehending and articulating to our partners the impact of compromise
- Remaining in frequent contact with facility security professionals and program managers.

Finally, we are looking at near term goals to build momentum. We formed an enterprise-wide integrated project team to best identify assets at cleared facilities, and maintain and continuously update the information. As we gain momentum, we will use the same approach to test the other steps in our new methodology.

I realize that change is challenging; however, I'm confident that together we will thrive through the transition. Thank you for your dedication to DSS and our important mission.

Dan Payne
Director

Resources available to industry for establishing, maintaining **INSIDER THREAT** programs

by Keith Minard
Industrial Security Integration and Application

The insider threat has long been a risk to security programs and the protection of classified national security information. The threat the insider poses ranges from the unwitting employee who fails to implement security procedures or inadvertently discloses sensitive information to an individual intent on committing acts to purposely harm national security.

President Barack Obama signed Executive Order (EO) 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing of Classified Information," in 2011 in order to address the growing concern of the insider threat. The EO directed U.S. government executive branch departments and agencies to establish, implement, monitor, and report on the effectiveness of insider threat programs to protect classified national security information. It also required the development of an executive branch program for the deterrence, detection, and mitigation of insider threats, including safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure.

While the EO applied to the federal workforce, additional guidance was required to direct cleared industry under the National Industrial Security Program (NISP) to implement the national minimum standards. On May 18, 2016, the Under Secretary of Defense for Intelligence (USD(I)) issued Change 2 to the National Industrial Security Program Operating Manual (NISPOM) which outlined the insider threat program requirements for cleared contractors consistent with those required for executive branch agencies.

Specifically, NISPOM Change 2 requires cleared industry to establish and maintain an insider threat program to detect, deter and mitigate insider threats. The program must gather, integrate, and report relevant and credible information covered by any of the 13 personnel security adjudicative guidelines that indicate a potential or actual insider threat. It must also be able to deter cleared employees from becoming insider threats, detect insiders who pose a risk to classified information, and mitigate the risk of an insider threat.

Rolling out the program to industry was a joint effort between

government and cleared industry. This partnership included the Defense Security Service, cleared industry, USD(I), the National Insider Threat Task Force, NISP Cognizant Security Agencies, and the National Industrial Security Program and Policy Advisory Committee (NISPPAC). The partnership enabled a collaborative effort leading to the development of the implementation guidance industrial security letter (ISL) that ensured industry had clear and accessible implementation guidance, and the right tools, resources, and training needed to successfully implement their company's insider threat program.

In order to support industry implementation DSS developed a wide-range of resources, and leveraged existing insider threat training to enable industry to establish and implement their programs. These resources included the ISL, which serves as DoD specific guidance; a single web page to enable insider threat information sharing with industry; an insider threat program job aid for industry; updates to the industry self-inspection handbook; an insider threat program plan template; and revisions to the certification and accreditation process manual, as well as a wide-range of training resources.

Cleared industry had until Nov. 30, 2016, to implement the minimum standards and meet the insider threat program requirements outlined in the NISPOM Change 2.

The cleared industry population consists of approximately 10,000 companies, 13,000 cleared facilities, 15,000 accredited classified information systems, and nearly 950,000 cleared employees. This makes contractors cleared under the NISP the largest single collective group of insider threat programs in the Federal government. Industry implementation of these requirements not only supports the protection of classified national security information at industry facilities but also integrates with programs at government locations where cleared employees are performing duties related to classified contract performance.

Now that the requirements of NISPOM Change 2 have been implemented across the NISP, DSS will continue to provide oversight, guidance, and direction to support program development implementation. DSS industrial security representatives will initially evaluate if the cleared contractor has implemented the minimum requirements, and follow-on vulnerability assessments will focus on evaluating program effectiveness.

DSS is committed to working with cleared industry to ensure that the programs now implemented continue to evolve, effectively deterring, detecting, and mitigating the insider threat, and supporting current and emerging threats posed by the insider.

DSS: An agency in TRANSITION

moving toward methodology consisting of four steps

by Kevin Jones
Change Management Officer

The world is rapidly changing and DSS is changing too. Where the agency once concentrated on schedule-driven National Industrial Security Program Operating Manual (NISPOM) compliance, DSS is now moving to an intelligence-led, asset-focused, and threat-driven approach to security oversight. The need for change is clear.

The United States is now facing the most significant counterintelligence threat it has ever encountered. Adversaries are successfully attacking cleared industry at an unprecedented rate. They are using multiple avenues of attack, varying their methods, and adjusting their priorities based on the targeted information they need. As a result, they are upgrading their military capabilities and competing against our economy using the very same information they stole from cleared industry.

In the past, DSS focused solely on the NISPOM to guide the agency's oversight compliance actions. As a static policy manual it does not identify what national security information needs the most protection; address the methods being used by adversaries; or consider the vulnerabilities inherent in business processes. DSS recognized this fact and is now moving forward to refine and pilot a multidimensional approach to security oversight using NISPOM compliance coupled with an asset-focused and threat-driven method of operation.

The agency's senior leaders met in September to build on the Risk-based Analysis and Mitigation (RBAM) efforts the agency conducted over the past year to identify, understand, and translate threat into action. Collaboratively, they designed and agreed upon a new methodology for implementing an asset-focused and threat-driven approach to helping cleared industry better protect national security information.

This new DSS methodology consists of four primary steps.

- The first step identifies the assets at each facility.
- The second step prioritizes assets based on national security information.
- The third step analyzes and applies threats to assets, identifies vulnerabilities, and captures NISPOM compliance requirements.
- The fourth step develops tailored security programs for each cleared facility by working collaboratively with program managers and cleared industry.

Nicoletta Giordani, DSS Industrial Security Integration and Application, leads a group through a session that identifies solutions to threat issues.

After the DSS Director approved the new methodology, a consortium of senior security practitioners from across the agency met in October at the Center for Development of Security Excellence. During this two-day session, the more than 40 participants identified gaps in the new methodology, proposed changes, and determined the benefits/challenges of each step in the approach.

With this foundation, DSS is now working to introduce the new methodology to cleared industry and government agency partners to integrate their feedback as well. In addition, DSS has formed an enterprise-wide integrated project team to validate Step 1 in the new methodology to determine how best to accomplish the three main tasks associated with it: Identify assets at each cleared facility, maintain this information, and update it on a continuous basis. Looking ahead, DSS will begin a series of pilots across the agency early next year to test the asset identification approach and gather lessons learned, best practices, and recommended changes. The focus will be on making continuous improvements and then applying the same approach to testing the other steps in the new methodology.

DSS Industry Day and Tech Expo draws large audience, more vendors

by Beth Alber
Office of Public and Legislative Affairs

Technological advances in cloud computing and mobile technology are continuously occurring, with businesses utilizing these applications on an increasing basis. Cloud computing allows DoD to leverage information technology functions, consolidate infrastructure and eliminate redundancies while improving continuity of operations. However, the overall success of utilizing the technology depends on well executed security requirements, defined and understood by DoD and industry. With this in mind, the theme for the second annual DSS Industry Day and Technology Exposition was "Streamlining and Managing Data through Cloud and Mobile Technologies." The event, hosted by the DSS Office of the Chief Information Officer (OCIO), was held in September, at the Gray Research Center on Marine Corps Base Quantico, Va. More than 200 government and military personnel attended the event, and more than 280 industry vendors were on hand to listen to speakers throughout the day. Approximately 29 companies participated in the technology exhibition.

The event provided an opportunity for industry to hear presentations from agency senior leaders on DSS current initiatives and emerging challenges in the context of the changing technology and security environment as they related to the event theme. In addition, DSS personnel briefed on the status of the DoD Insider Threat Management and Analysis Center, opportunities under the Small Business Program, and changes occurring in the NISP Authorization Office. A discussion group featured inputs from the Chief Information Officer Council comprised of CIOs from the Air Force Office of Special Investigations, U.S. Army Criminal Investigation Command, Naval Criminal Investigative Service, and DSS.

"The agency has changed in the 18 months since our last event," said Craig Kaucher, DSS Chief Information Officer, noting the facility was at capacity for these briefings. "The DSS briefers were talking about a whole different operations model, and the mission changes drove the conversations."

The event featured a panel discussion by chief information officers from the Air Force Office of Special Investigations, Naval Criminal Investigative Service, Army Criminal Investigation Command, and DSS. (Photo by Hollie Rawl, CDSE)

"After each presentation, there were lines of people linking up with the briefers to have follow on discussions," said Matt Kroelinger, DSS OCIO Business Relationship Manager and one of the Industry Day organizers. Kroelinger noted the DSS Small Business Program manager provided dates for follow up meetings. "In the future, we need to find a way to keep that communication going after the briefings."

"We brought our RKB (Russell-Knox Building) partners more prominently into the event this year," Kaucher said. "The CIO panel discussion was well received, and people enjoyed hearing the different perspectives and how each agency aligned its information systems in the building."

"We got some great feedback about including CIOs from the other agencies in the event," said Kroelinger. "With overlapping missions, collaboration and shared services, it was also beneficial for our government counterparts."

While attendees were participating in the Industry Day sessions, the Technology Exposition was open for people to visit, network, and view demonstrations of the latest products and services from the participating industry exhibitors. Topics highlighted at the expo included cloud capabilities, continuous monitoring, and virtual desktop infrastructure.

"People came up to me and said this was a much better venue," Kaucher said. "I got positive feedback on the switch, and the ability to roam and move about the campus. My commitment is to continue to do this event and continue to improve on the event.

"We are open for further feedback from attendees, and would love to hear from them," Kaucher concluded.

TOP: Matt Kroelinger, DSS OCIO Business Relationship Manager and one of the Industry Day organizers, provides administrative remarks at the event. (Photo by Hollie Rawl, CDSE) **BOTTOM:** James Kren (right), DSS Deputy Director, and other DSS senior leadership walk through the technology expo exhibits. (Photo by Beth Alber, OPLA)

Improving project performance is goal of new **integrated lifecycle management framework**

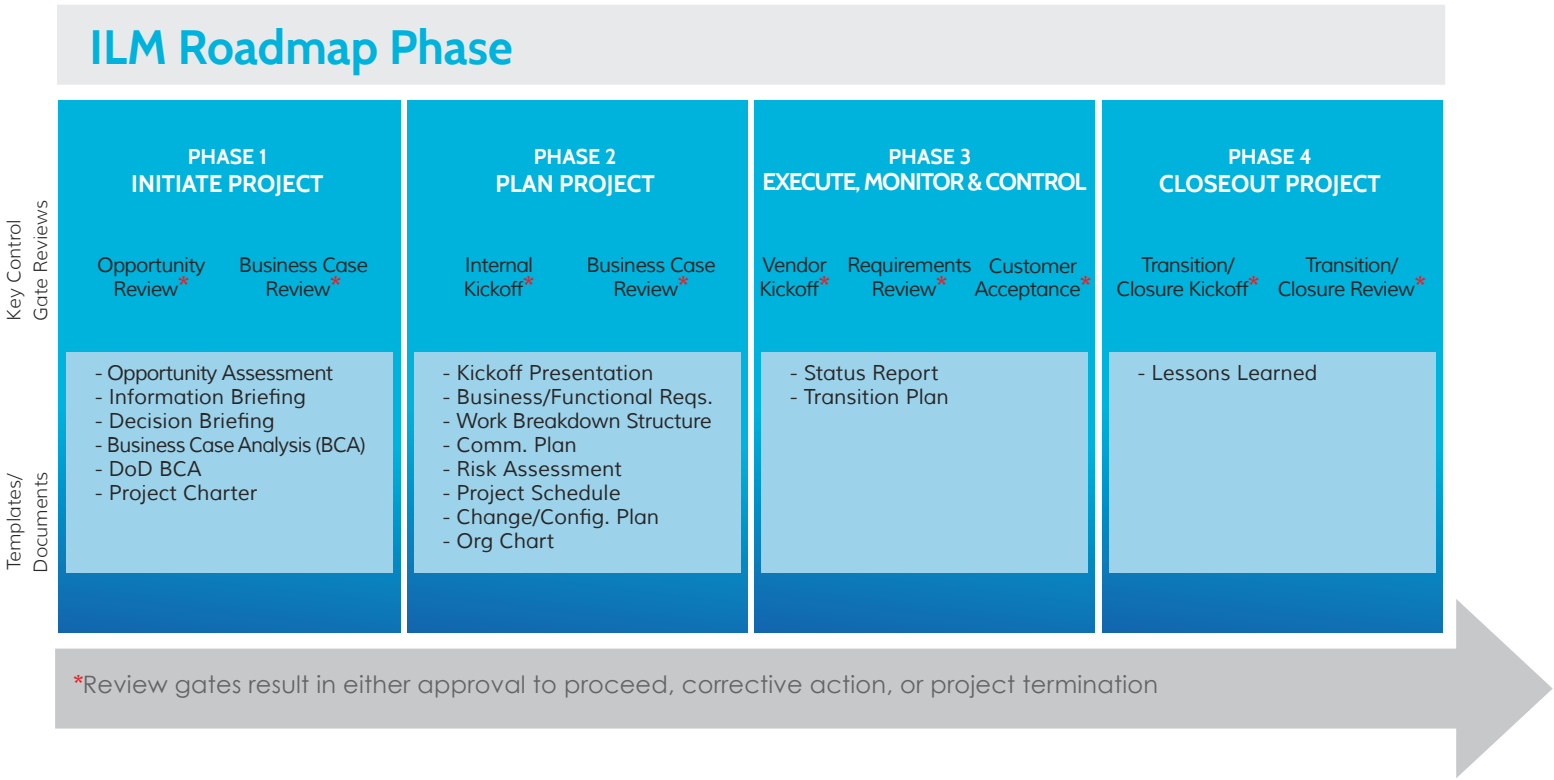
by Program Integration Office

The evolving threat landscape, combined with continued fiscal uncertainty, requires a new way of managing DSS enterprise projects and programs. DSS took aggressive action to improve project performance and launched a new organization dedicated to enterprise program management excellence.

The Program Integration Office (PIO) within the Business Enterprise Directorate was established to provide integration and project management services for enterprise-wide initiatives such as the National Industrial Security System, the DoD Insider Threat Mitigation and Analysis Center and the Vehicle Telematics Program. PIO developed a standardized project methodology that aligns with the DSS Strategic Plan 2020. It provides employees with the proper framework, processes, and tools to deliver exceptional program management support to DSS enterprise initiatives. The office streamlines disparate project management methods and provides guidance, assistance, oversight and control of program and project management to address current challenges in project planning and execution.

Before developing a new project management approach, DSS had to first understand its strengths and weaknesses within project and portfolio management. PIO led a team of subject matter experts, which included program managers from across the agency, in assessing the key concerns related to project management. Two themes emerged from the exercise: lack of accountability and risk management. Regarding accountability, the concern was ownership of activity status as results became increasingly difficult to determine and manage as the project proceeded. In some cases, gate or stage reviews did not exist, resulting in little visibility into project status. As for risk management, fully integrated risk assessment and mitigation planning did not exist, which had a negative impact on how project issues were identified, planned for and mitigated.

Based on the findings, DSS leaders and project stakeholders agreed that PIO should develop a standardized project management framework for the entire agency: the Integrated Lifecycle Management (ILM) Framework. ILM assists in the review and prioritization of new ideas and ends with the delivery of an agreed upon product or service, and transition to sustainment activities.



This framework was built with three key guiding principles in mind:

First, the framework aligns with the DoD Acquisition System (DoD Instruction 5000.02), the Project Management Institute Project Management Body of Knowledge, and DSS internal governance processes. It was essential for the ILM to comply with DoD guidance, be informed by industry standards, and remain tightly integrated with DSS governance policy.

Second, the processes within the ILM are designed to achieve very specific outcomes – not merely outputs. By implementing the ILM, DSS will strengthen its project and portfolio management processes. The framework and processes are clear, efficient, and documented well enough for even those individuals not familiar with project management industry standards to implement successfully.

Third, the framework facilitates substantial and ongoing customer engagement. This ensures customer requirements are met and project outcomes are achieved on schedule, within budget, and at the quality desired by the customer.

The ILM follows four key phases: Initiate; Plan; Execute, Monitor and Control; and Closeout. Each phase includes performance and deliverable reviews that are intended to drive transparency, accountability, ongoing collaboration, and ultimately the desired project results. The various reviews or stage gates throughout the process provide stakeholders the opportunity to validate any deliverables within that period of time and gain high-level insight into the project status.

Initiate

Because new customer requirements can emerge rapidly, often with little advance notice, DSS needed an organized and efficient way of capturing, vetting, and adjudicating new requirements. To balance the desire for new ideas and innovation with pragmatic business requirements, PIO established an Opportunity Assessment form. This form helps evaluate the merits of new ideas while providing visibility for the appropriate stakeholders to ensure alignment with agency priorities and mission goals.

Plan

Upon approval of the business case and formal assignment of the program manager via a signed charter, the project planning begins. The ILM calls for development of a comprehensive Program Management Plan that should clearly articulate the manner by which project risk, schedule, budget, and other key management processes are delivered.

Execute, Monitor and Control
The purpose of this phase is to develop the product or service that the project was approved to deliver. Typically, this is the longest phase of the ILM and where most resources are applied.

This phase uses all the plans, schedules, procedures and templates that were prepared and anticipated during prior phases. Active tracking and monitoring the progress of requirements is of the utmost importance to ensure business case objectives are being met.

Another major aspect of this phase is ensuring the outcome or product delivered via the project can be sustained. This entails developing the appropriate training, transition plans and other change management perspectives that will be needed before and after implementation.

The conclusion of the phase arrives when the product or the project is fully developed, tested, accepted, implemented and transitioned to the mission owner or sponsor.

Closeout
During this phase involves the project manager capture lessons learned throughout the project and ensures stakeholder sign-off, in addition to meeting any contractual obligations. The transition plan, developed early in the framework, is fully executed by the project team (such as knowledge transfer to the appropriate parties) to facilitate sustainment of the project outcome or product progress.

DSS used agile principles for ILM development and process rollout. While developing the ILM, PIO piloted each phase, managed toward desired outcomes, captured lessons learned, and updated and improved the framework and processes as needed.

Use of ILM has resulted in some immediate successes. In one case, senior leaders determined that a new emergency notification system was required to comply with DoD mandates. In the past, DSS would begin a rigorous business, functional and technical requirements development exercise, followed by acquisition planning for a new system. In this case, through the development of the Opportunity Assessment form and the business case, PIO recognized that an existing DoD system could be leveraged for the requirement. This dramatically reduced overall cost, risk to the agency, and time to implement, while highlighting and strengthening interagency information sharing, collaboration and joint initiatives.

In a second case, PIO worked with the ODAA Business Management System (OBMS) project team to pilot/test the ILM close phase. The project manager walked through the processes and completed templates to successfully closeout the project. Following the ILM framework, some of the activities completed were knowledge transfer sessions, lessons learned sessions with project stakeholders, and the development of a transition plan to assist the operations team with supportability and maintainability needs.

Through the use of the ILM, the PIO enables support of managed projects under a standardized framework, and coordinates integration of tools, activities and teams to meet successful delivery. PIO ensures projects are aligned with DSS-wide strategic goals and objectives. A project's success is no longer only defined by managing the schedule, budget, and quality, but also by enforcing accountability and fostering transparency and communication.

ON FIAR: DSS leads the way in Financial Improvement and **Audit Readiness** efforts

by Ahmed Nadeem and Shana Dittamo
Financial Management Office

With nearly two million employees and hundreds of installations across the globe, the Department of Defense (DoD) may be the largest and most complex organization in the world. Despite its size and complexity, DoD is committed to achieving financial statement audits by Sept. 30, 2017. DSS has been leading the Defense agency community in its Financial Improvement and Audit Readiness (FIAR) efforts and was one of four agencies, out of 26 total reporting entities, formally recognized by the DoD Deputy Chief Financial Officer with a certificate of achievement and excellence.

The Chief Financial Officer (CFO) Act of 1990 and the FY10 National Defense Authorization Act (NDAA) mandated that all federal entities receive financial statement audits. To date, DoD is the only federal agency that has not been able to receive a financial statement audit due to factors such as complexity of the mission, outdated systems, and missing or incomplete documentation. Aside from the legal requirements to receive a financial statement audit, audits also provide value through:

- Continuous improvement of business processes
- Efficiency and effectiveness of resources
- Increased public trust and stewardship of taxpayer dollars

The DSS Journey

DSS has been on the audit readiness journey for over four years and has emerged as a leader in the Defense agency community by viewing audit readiness as an integrated process improvement strategy enabling, and requiring, collaboration across all DSS operating and enabling elements through the annual Managers Internal Control Program (MICP). DSS asserted audit readiness over its major business processes and is planning to obtain its first-ever financial statement audit in FY17. Pending the results of the financial statement audit, DSS could be the first Defense agency to transition to a new accounting system (the Defense Agencies Initiative (DAI) system) and undergo a financial statement audit.

Audit readiness is not an administrative "check the box" exercise; it affects the mission and business processes of the entire agency, ensuring personnel are paid accurately and timely, contractors are not paid twice or inaccurately, system data is only accessible by authorized personnel. The entire workforce has engaged in this effort, making a more agile, integrated and transparent business environment.

DSS CFO Corey Beckett (right) receives a certificate of achievement and excellence from Mark Easton, DoD deputy chief financial officer at a Defense Agency FIAR Day.

DSS has partnered with an audit readiness team from PricewaterhouseCoopers (PwC) to increase efficiencies and at the same time prepare for a full financial audit. The DSS audit preparation can be broken into five areas:

- Leadership Support: DSS has established a system of governance that underpins the audit readiness effort. DSS uses the Enterprise Planning and Integration Council, the Deputies' Council, and the Executive Steering Committee as its Senior Management Council to lead the agency in the identification of systemic weaknesses and subsequent remediation. These groups are briefed quarterly on the status of the process improvement and audit sustainment program. Leadership buy-in has been instrumental in pushing the effort forward.

- Audit Readiness Human Capital: In an effort to achieve auditable financial statements and create a strong internal control environment over our business processes, DSS requires a well-trained financial workforce. In

early 2011, DoD Financial Management (FM) senior leadership developed a DoD FM Certification Program. The NDAA for FY12 provided the Secretary of Defense with the authority to prescribe professional certification and credentialing standards. The result is a course-based certification program to train personnel in audit readiness, decision support and analysis. Currently, DSS has a 100 percent compliance rate through the certification of 12 employees.

- Internal Controls: The FM staff has worked with process owners from across the agency to document key processes and produced standard operating procedures documentation for operations. In FY14, DSS documented 75 manual internal controls and examined 22 financially significant systems. Nine standard operating procedures or desktop guides were written and disseminated to DSS process owners to help implement new internal controls. Between FY14 and FY15, the pass rate for controls tested for the first time increased from 31 percent to 67 percent. As of the end of FY16, no material weaknesses remained open from the more than 50 weaknesses identified when the audit readiness journey began.

- Supporting Documentation: Financial auditors are required to obtain and analyze supporting documentation to use as evidence in order to draw reasonable conclusions. Much of the audit readiness effort has focused on collecting and analyzing supporting documents that verify the completeness, accuracy, and validity of DSS's underlying financial transactions and business events. The FM team worked with key stakeholders across the agency to collect documentation and stand-up processes for quick retrieval of documents in response to auditor requests. In 2016, DSS compiled complete and accurate documentation packages for asset costs, a challenging and critical effort that has plagued the Department for decades.

- Information Technology: DSS conducted a comprehensive gap analysis of its accounting technology and found room for improvement in the use of old legacy accounting system and adopted a new enterprise resource planning system, the Defense Agencies Initiative (DAI). DAI provides DSS with a fully integrated budgeting, accounting and mission capability that allow resource information to flow easily throughout the organization. DAI automated many business processes and internal controls that were previously performed manually. Through this deployment, approximately half of the original 50 plus audit readiness weaknesses were fully or partially remediated.

FY16 Mock Audit – An Important Test

In November 2015, DSS initiated the agency's first mock audit, which is tested DSS' ability to withstand a financial audit. The mock audit prepared DSS in three ways:

- Determined the framework of external auditors expectations;
- Prepared the DSS workforce for an actual financial statement audit; and,
- Identified major operational or compliance issues and develops corrective action plans to rectify those issues.

A financial statement audit consists of four distinct phases: Planning, internal control, documentation testing, and reporting. During the planning phase, the audit team establishes an understanding with DSS, gains an understanding of the agency's operations, and determines the scope in which the audit will be performed. The internal control phase focuses on risk assessments and tests the strength of the agency's internal controls. The results of this testing determine the nature, extent and timing of further procedures in the documentation phase. Finally, the reporting phase involves documenting any deficiencies identified during the audit testing, drafting statements, and developing corrective action plans to address any material issues.

DSS is currently in the testing phase of the mock audit and expects to complete the reporting phase in late 2016. This mock audit will conclude with PwC presenting a "mock" opinion to the DSS Chief Financial Officer on the agency's ability to withstand an audit in FY17 and identify those areas that require remediation.

Next Steps

DSS plans to engage an independent public accounting (IPA) firm for a full financial statement audit on its FY17 financial statements. The IPA examination will be more intensive than any other in-house testing thus far. The IPA will review the DSS business environment for compliance with applicable accounting standards and requirements. This audit will result in a signed report by the IPA stating that DSS's financial statements are fairly stated and key internal controls are in place and operating effectively. The reports may also identify areas of improvement. Such an effort will allow DSS leaders to revise or re-direct our audit readiness resources to key areas that impede our overall audit readiness goals.

This effort will be the culmination of years of hard work. Regardless of the outcome of the independent audit, DSS has improved its business processes and proven that it is a good steward of taxpayer dollars in executing its missions – safeguarding the nation's interests as the premier provider of industrial security risk management and security professional services.

A Q&A with **Corey Beckett**, DSS Chief Financial Officer

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

Corey A. Beckett a Defense Intelligence Senior Level executive, is the DSS Chief Financial Officer. In this capacity, he is the principal advisor to the Director, DSS, on all budgetary, accounting and fiscal matters, including the development and execution of the DSS budget.

Before joining DSS, Mr. Beckett was assigned to the Washington Headquarters Services, a DoD field activity, as the Director for Resource Management, where he was responsible for all aspects of budget formulation, justification, defense and execution of an estimated $1.5 billion annually, governing the acquisition and maintenance of construction and facilities programs.

Mr. Beckett began his federal service as a budget analyst intern within the Office of the Secretary of Navy, Comptroller, with assignments throughout the Department of the Navy, to include headquarters, Systems Command and fleet staffs. He held a number of positions with increasing responsibility at both the headquarters and field level of the Department of the Navy, and the Office of the Secretary of Defense, Comptroller, in which he was responsible for planning and programming, budget formulation, justification and execution for a variety of operating and investment programs.

Q: Tell us about your background and what led you to DSS.

I have 27 years of federal service as a government civilian. My entire career has been in the national security arena with the Department of Defense. While I have always been a financial manager, I've been fortunate to have an opportunity to work with many diverse programs, to include ship and aircraft platforms, weapons systems, information technology, intelligence, and construction programs and projects. I was drawn to DSS because of its unique and complex mission and opportunity to make a difference. I find the overall scope, mission and challenges very interesting and intellectually rewarding.

Q: DSS is preparing to get audit ready to meet the mandate set by the Congress. What steps have been taken? Why is this important for DSS?

DoD is one of two federal agencies that have never had a clean audit opinion on its financial statements. The department has reasonable controls over its budgets but there some critics who assert the contrary because we are unable to achieve a clean audit opinion. DSS needs to do its part to help change that. Most importantly, having auditable financial statements will reassure the public and Congress that DSS is a good steward of the public trust, demonstrates accountability, safeguards assets, and guard against fraud, waste, and abuse. I view audit readiness as a continuous, integrated process improvement framework across all DSS operating and enabling elements.

In preparation for audit, we followed a phased approach to gain a sustainable audit readiness state. In the early stages, we underwent a comprehensive review of our business environment and identified key areas of improvement, which included updates to our legacy financial system and the re-engineering of our antiquated business transaction processes for a sustainable, audit-ready internal control environment. After making these improvements, we established comprehensive testing, results evaluation and course correction strategies to improve our business processes. This allowed us to evolve our financial management practices into management best practices that were recognized by the Office of the Under Secretary of Defense (Comptroller) as best business practices for the department to emulate.

In the current fiscally constrained environment, DSS is bringing greater transparency to its financial and business operations which allow us to make a better and reliable case for new resources.

Q: A few years ago, FM implemented the Enterprise Resource Planning (ERP) system of the Defense Agencies Initiative (DAI). How has that assisted DSS in improving internal controls within the agency?

The successful implementation of the Defense Agencyies Initiative (DAI) was huge for the agency. DAI not only improved our financial transparency but also improved

DSS operations. One of the major challenges to improving the agency's financial information and audit readiness was replacing our legacy financial systems, which were old, dating back to the 1970s. The systems weren't designed to do what auditors expect from an audit-ready system, but rather were designed to track budgets, not to accommodate underlying transactions and business events. For example, auditors not only require review of obligation documents such as contracts but also require review of related execution documents, such as invoices or receiving reports and payment documents. We had that information, but it was not readily available and was scattered across multiple disjointed financial systems. DAI has not only integrated the financial systems but also has the capability to upload and store supporting documentation which greatly reduced the document retrieval and transmission timelines. DAI also allowed for the transition of many manual internal controls to automated platforms which effectively minimized the number of material weaknesses in our financial operations. Automated solutions, such as the time and labor module, have eliminated paper-based manual processes. As we move forward, we plan to further integrate our business systems with our ERP system. For example, currently the contract writing system and DAI do not interface with each other and thus require manual input of executed contracts into the DAI system. By integrating and automating these two systems, we will gain further synergies in the form of fewer human errors and savings in manual labor hours.

Q: We hear about the Budget Control Act, headquarters reductions and budget cuts. How difficult is the current budget environment and how is DSS faring in the fight for resources?

Today's budget environment is one of the most difficult I've been associated with in my career. The key challenge in this environment is to make sure that we acquire the necessary resources needed to meet our national security mission. This is extremely difficult when we are dealing with an economic crisis that has led to a strong downward pressure on all federal spending, to include defense, as a way to reduce the deficit. At the same time, the world is rapidly changing with new technologies, emerging threats, and increased complexity and uncertainty. The key challenge is striking the right balance -- getting the resources we need, while understanding that we need to make every dollar count by continually assessing our requirements, processes and operations to ensure we are operating as efficiently and economically as possible.

Q: The DoD recently implemented a course-based Certification Program for the Financial Management workforce. How will this help the DSS FM workforce?

As I look around at the financial managers we have at DSS, they are well trained and doing a great job in meeting the financial management needs of the agency. Most have more than 15 years of federal and DoD financial management experience. First, the DoD financial management certification program provides a framework on what type of training is best at a particular point in an employee's career. Second, the FM world is changing quickly and our training programs must adapt to shifting times. This calls for a multi-disciplined workforce with relevant skills, practical work experiences and up-to-date training. One example of this is achieving audit readiness. Many people think audit readiness is just the accountant's responsibility; however, all FM personnel must understand the audit environment.

To improve financial information and achieve readiness, we must train all of our personnel on audit issues. Some will need basic knowledge while some will require more advanced training. Analytical skills are another example of training required. As DSS utilizes the DAI ERP system, financial managers need to go beyond providing reports, and move toward analyzing and interpreting those reports. This requires more training in decision support skills. A course-based certification program provides a vehicle for ensuring that we provide the right training for decision support. As with most certification programs, the DoD FM Certification Program will require continued professional education or training on a periodic basis after certification is achieved.

Q: So what's next for DSS and audit readiness?

Over the past few years, DSS has dedicated significant time and resources to achieving audit readiness on an accelerated schedule. In FY16, we determined that we had made significant progress in executing the normal, repeatable auditable processes. DSS chose an innovative approach, whereby the audit readiness team performed a "mock audit" of DSS financial statements to identify any remaining weaknesses that we may not have uncovered and to stress test the audit infrastructure. "Mock" audits were planned and executed using most of the same procedures, tools and techniques that auditors would employ during an actual audit. Mock audit results have been encouraging to say the least. It confirmed our assessment of the state of audit readiness at DSS. In FY17, we plan to engage an independent public accounting firm in a full financial statement audit on our FY17 financial statements.

Acute CYBER THREATS persistent, adaptable; rapid reporting by industry imperative

by Mike Berry
Counterintelligence directorate

While the cyber threat is universal, the cyber threats that affect cleared contractor classified and unclassified information systems are particularly acute. This is illustrated in DSS's annual report "Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting." These threats come from foreign intelligence entities (FIE), criminal elements, insiders, and others seeking to exploit the systems.

The added security surrounding classified information systems lessens but does not eliminate their susceptibility to compromise. The cyber threat, particularly from FIE, recognizes this, and focuses substantial effort to compromise unclassified systems to acquire the information or control they seek. They also seek to further their ability to identify and exploit classified systems and people with access to classified information. Moving the information to another system, such as a cloud service provider, may complicate the threat efforts but it will not prevent them. Additionally, the provider becomes an extension of the contractor's network; and thus, also subject to cyber incident reporting.

The cyber threat also targets unclassified systems at cleared companies and facilities that may have no resident classified information. These non-possessing cleared contractors have access to information and resources valuable to the threat actor, e.g., unclassified sensitive technology, cleared personnel and the work they do, classified contract related information, and systems test/maintenance records. Whether or not the cleared contractor holds classified information, its unclassified systems are cyber threat targets and the contractor has the same cyber threat reporting requirements.

Cyber threats may also affect entities connected to a compromised network, including the network service provider.

The cyber threat is persistent and adaptable. It mounts continuing and prolific efforts to compromise cleared contractor systems and employees through the unclassified cyber domain, and quickly exploits the vulnerabilities and information it discovers.

Therefore, rapid and earliest identification and reporting of these threats and timely defensive responses are essential to ensure quick mitigation of the risks to classified contracts and information, the related sensitive technology, and cleared facilities and personnel. This reporting helps the cleared contractor and the government in curtail adversary success and preclude or minimize future occurrences at other locations. For example, DSS uses this information to project FIE activity and alert potential targets. When a cleared contractor applies the cyber threat alert notices it receives from DSS, it should immediately notify DSS when the indicator reveals suspected or known FIE activity. Such information has immense value to the government's tracking, disrupting and exploiting of the threat, and to enhancing and expanding the alert.

The reporting of cyber events on cleared contractor systems is done in accordance with paragraph 1-301 of the National Industrial Security Program Operating Manual for incidents that may indicate espionage. Paragraph 1-302 addresses additional reporting that was expanded upon with Industrial Security Letters from 2010 and 2013. Even though DSS receives and makes use of this reporting from unclassified systems, it does not have oversight of such systems, except where specified for companies under mitigation agreements for foreign ownership, control or influence.

More recently, DoD implemented two changes to the Defense Federal Acquisition Regulation Supplement (DFARS) that made cyber incident reporting a requirement in all subsequent DoD contracts under which the contractor would process or hold certain protected unclassified information on their unclassified systems. This requirement unifies defense contractor cyber incident reporting, addressing both contractual obligations for cyber incident reporting, and reporting of possible FIE activity through a computer/network action. It has the benefit of providing contractors a single reporting process and making the data immediately and fully available to DSS. It also gives DSS an added, valuable dimension in its counterintelligence coverage for cleared industry: the opportunity to correlate and analyze cyber adversary activity across cleared and uncleared contractors, and help DSS to better anticipate, identify

and warn or exploit developing or impending cyber threats to cleared contractors and contribute to those protecting against uncleared contractor exploitation.

Defense cleared contractors not under the DFARS clauses and all non-defense cleared contractors under DSS NISP cognizance, should continue to report cyber threat incidents on their classified and unclassified systems as directed by the NISPOM. If those cleared defense contractors voluntarily report incidents under their framework agreement with the Office of the DoD Chief Information Officer, they can meet the initial NISPOM reporting requirement by choosing the option on the Framework Agreement incident collection form to provide DSS a copy of their reporting.

DSS earns multiple CI and Security Awards

Five DSS employees captured 2016 National Counterintelligence and Security Awards, earning recognition from the National Counterintelligence and Security Center for significant contributions to the counterintelligence and security missions during the previous calendar year.

The DSS award winners were:

- Jonathan Cofer, Industrial Security Field Operations, Information Security, Individual Award
- Sara DeWitz-West, CI Northern Region - Industrial Security, Individual Award
- Adam Hauch, CI Headquarters - Supply Chain Protection, Individual Award
- Nick Luce, CI Western Region - CI Collection, Individual Award
- Rebecca Morgan, Center for Development of Security Excellence (CDSE) - Education and Training, Individual Award

Receiving honorable mention at the awards ceremony were:

- CI Collection and Requirements Branch (CACTUS VIPER), CI Headquarters - CI Analysis, Team Award
- CI Curriculum Program, CDSE - Education and Training, Team Award

The **Information Security Award** is given for the application of innovative policies, practices, or measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, security, and non-repudiation. Cofer, a senior information systems security professional, identified and customized a Security Content Automation Protocol tool. The tool allows DSS personnel to conduct a review of 100 percent of the system security settings in a fraction of the time thus allowing for evaluating the "whole picture" information system risk profile instead of manually reviewing a very small sampling of system security configurations. By adopting a standard automated tool, DSS greatly reduces the hours spent assessing information systems and brings the Defense Industrial Base classified information systems into alignment with current federal and DoD security standards.

The **Industrial Security Award** is given for the application of innovative policies, practices, and/or technology to protect classified information developed by, or entrusted to, U.S. industry. Counterintelligence Special Agent DeWitz-West used innovative practices to protect classified technology, which resulted in the identification of 665 potential foreign collection attempts within the Defense Industrial Base. By identifying these attempts as they were happening, DeWitz-West and other government agencies were able to work with cleared industry to impose countermeasures that allowed the U.S. to detect, deter, defend, and exploit subsequent foreign intelligence entities attempts. As a result, the intelligence community and law enforcement entities initiated investigations, operations, or operational sources on 48 subjects and sources.

The **Supply Protection Award** is presented for the application of innovative policies, practices, and/or technology to identify and mitigate attempts to compromise the U.S. supply chain, including efforts to collect information on, and develop access to, suppliers; sabotage of critical components; insertion of defective parts and components; transfer of technology; or acquisition of U.S. vendors. CI Analyst Hauch is an active proponent of protecting the U.S. supply chain, and his research and analytical findings led to the identification of suspect microelectronic parts within cleared industry. He conducts briefings at national-level microelectronics conferences, and provides training and guidance on supply chain assurance. Additionally, Hauch produced 11 intelligence information reports and authored two source directed requirements on supply chain-related issues, which contributed to the identification and mitigation of foreign entities' attempts to compromise the U.S. supply chain.

The **CI Collection Award** is given for substantial achievements in CI collection resulting in significant enhancements to U.S. national interests. CI Special Agent Luce identified 1,926 potential foreign collection attempts targeting DoD classified, export-controlled, and critical technologies protected by the International Traffic in Arms Regulation. His efforts resulted in federal intelligence and law enforcement agencies initiating investigations and/or operations on 94 subjects or operational sources in the Defense Industrial Base. In addition, Luce produced 256 suspicious contact

reports and 240 intelligence information reports which contributed directly to ensuring defense technologies are delivered to its customer without compromise.

The **Education and Training Award** is presented for superior efforts to ensure that the intelligence community has effective learning programs strategically designed to assist CI and security professionals in developing and refining their substantive and tradecraft skills, competencies, and expertise. Morgan, who serves as an instructor for the CDSE CI Awareness Curriculum Team, organized and hosted six webinars, developed three toolkits and four job aids, authored three insider threat case studies, revised three eLearning courses, and created a training CD. She drafted and expertly presented CI awareness briefs to multiple sessions of instructor-led training for seven different security disciplines. Morgan combined her management skills and professionalism to successfully conduct a highly effective marketing campaign that significantly increased CI Awareness training. Her integration of CI and threat awareness into the CDSE training programs effectively reached over 454,000 students who completed eLearning or instructor-led training during the last calendar year.

Goal of DSS Diversity Council to create culture of inclusion, increase awareness of initiatives





TOP TO BOTTOM: Denise Arel; Stephanie LaBeach; Betty Leach; Ahmed Nadeem; Miladys Ortiz.

President Barack Obama issued Executive Order 13583, "Establishing a Coordinated Government-Wide Initiative to Promote Diversity and Inclusion in the Federal Workforce" in 2011. In addition to establishing a government-wide initiative, the executive order directed individual agencies to develop diversity and inclusion strategic plans consistent with the government-wide plan, the agency's overall strategic plan, human capital plan, applicable laws and Merit System Principles. The government-wide plan identifies three strategic goals--workforce diversity, workplace inclusion, and sustainability--along with associated priorities. The guidance for agency-specific plans directs federal agencies to outline the actions they will take to achieve the priorities identified in the government-wide plan.

In accordance with the executive order, DSS established an Inclusion and Diversity Steering Committee which is championed by the Chief of Staff. The committee members are Denise Arel, Office of the Chief Financial Officer; Ahmed Nadeem, Financial Management; Betty Leach, DSS Front Office; Stephanie LaBeach, Atlanta Field Office; and Miladys Ortiz, Counterintelligence directorate. These members, who were selected for their diverse backgrounds, occupational series, years of government service and duty stations, will form the foundation of the Director's Council for Inclusion and Diversity (DCID).

The DCID will be established to align with the Director's priorities, and his commitment to the workforce and agency mission. The council will seek to create a culture of inclusion where individuals are drawn to serve, feel valued, and actively contribute to overall mission success. The DSS workforce varies with respect to gender, age, ethnicity, race, sexual orientation, education, religion, physical abilities, life experiences, family make-up and work experiences. This diversity has been key to the success of the agency. DSS must continue its emphasis on developing and sustaining an inclusive environment that values diversity to foster mutual respect and cooperation and therefore championed by all employees.

The steering committee created a draft charter for the DCID, which states the council's purpose:

- Promote and support inclusion and diversity initiatives by embracing the power of the workforce to foster an inclusive environment where all employees have the opportunity to achieve personal growth while contributing to the overall success of the mission of DSS.
- Provide leadership and advice while encouraging senior leaders to adopt new and innovative approaches to promote and increase diversity in the workforce.
- Serve as a liaison to senior leadership and a resource and advocate for staff and managers.
- Facilitate communication to improve awareness about inclusion and diversity issues and initiatives throughout the agency.

In today's fast moving world, DSS must possess agility, innovation, and a world view to meet the complex demands of unprecedented societal diversity. To be prepared for these changes, diversity must be embedded into the agency's DNA. Numerous studies have shown a positive correlation between workforce diversity and organizational performance. For instance, diverse teams are more creative, perform better at problem-solving, and foster better decision-making than homogeneous ones. The DSS leadership team has the primary responsibility

to ensure a diverse and inclusive workforce. They are responsible for the following initiatives in support of the executive order:

- Enhancing the agency's ability to recruit, hire, promote and retain a more diverse workforce.
- Creating a culture that encourages collaboration, flexibility, and fairness to enable individuals to participate to their full potential.
- Developing and implementing a more comprehensive, integrated, and strategic focus on diversity and inclusion as a key component of their human resource strategies.

Throughout the council development process, the steering committee will work with the DSS Office of Equal Employment Opportunity (EEO) on development of diversity strategies. The EEO will also collaborate on policies and mechanisms related to the formation of the DCID. Inclusion and diversity is an agency priority, and DSS is working to recruit, retain and develop a diverse, high-performing workforce that draws from all segments of society and values fairness, diversity, and inclusion.

"Our Nation derives strength from the diversity of its population and from its commitment to equal opportunity for all. We are at our best when we draw on the talents of all parts of our society, and our greatest accomplishments are achieved when diverse perspectives are brought to bear to overcome our greatest challenges."

- President Obama

Executive Order 13583

CHANTILLY OFFICE partners with Industry for Facility Security Officer Crash Course

by Diane Horan
Chantilly Field Office

For new facility security officers (FSO), the requirements and responsibilities of the National Industrial Security Program (NISP) can quickly become overwhelming. In an effort to assist new FSOs in understanding program requirements, the Chantilly Field Office instituted and hosted a one-day "FSO Crash Course" in August 2016.

The course was presented by the field office industrial security representatives (ISRs) and was intended for new FSOs or those who may benefit from a refresher course. The course encourages new FSOs to become comfortable with their role, and provides an overview of the resources available to establish and maintain a security program. The course exemplifies the DSS goal of partnering with industry and encourages meaningful relationships and trust between industry and their ISRs.

The event covered topics such as FSO responsibilities, required training, facility clearance documentation, classified contracts/subcontracts, personnel security clearances and JPAS. The ISRs also discussed how to present meaningful security education to the workforce and ensures that all employees understand the reporting requirements, how to conduct effective self-reviews, how to prepare for a DSS security vulnerability assessment and the benefits of becoming involved in a local industrial security area council. The FSOs also received instruction on the Industrial Security Facilities Database and e-FCL, which provided information on their functions and how to create an account.

The FSO Crash Course was also supported by DSS counterintelligence special agents who presented counterintelligence education and information, and delivered insight on Insider Threat program requirements resulting from NISPOM Change 2. Each FSO in attendance was provided security education materials, job aids, and a copy of the latest issue of "Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting."

The FSO Crash Course presented a unique opportunity for new FSOs to interact with one another and provided a great networking opportunity. The presentation of the course material by the ISRs conveyed their passion for the work and desire to help FSOs succeed. The FSOs and ISRs further interacted during a working lunch, which featured a question-and-answer session where FSOs asked questions in a more relaxed setting.

Feedback showed the FSOs found the course to be useful and the course material and manner it was presented to be extremely beneficial, contributing to rapid establishment of effective security programs. Additionally, the interactions led to more open communication between the FSOs and the ISRs on security matters.

"

Great initiative. Thanks for taking this on.

They were so specific with covering all areas that would relate to being an FSO. **Very helpful**.

The **CISA's information was amazing**! Her handouts were outstanding.

"

Huntsville Field Office comes together to support deployed warfighter, keep mission on track

More than 100 DSS employees serve in the military reserve, which requires fulfilling obligations away from the office. When that happens, DSS offices pitch in to ensure the mission continues. This summer, the Huntsville Field Office faced this scenario when an industrial security representative deployed to support a military exercise.

Senior Industrial Security Representative Dale Stephens serves in the United States Marine Corps Reserve and was recently selected for a promotion to the rank of Chief Warrant Officer Five. In June, Stephens participated in his fourth consecutive annual exercise in Africa, the Joint Multinational Exercise Central Accord 2016 in Libreville, Gabon. This exercise involved United Nations Multidimensional Integrated Stabilization Mission (MINUSCA) command post staff training and a UN Peacekeeping MINUSCA field training exercise for African military forces. Several branches of the U.S. military participated in the exercise, as well as many African and European state partners. Stephens served as the Director of Opposing Forces for the field training exercise with the African maneuver forces, simulating various scenarios for them to address and teaching participants different peacekeeping tactics, techniques, and procedures for future UN operations.

"This exercise and other exercises conducted across the African continent are good faith demonstrations of diplomatic and military partnerships between the United States and our partners," Stephens said.

While Stephens fulfilled his military obligations, the Huntsville Field Office came together to support his assigned facilities during his two-week absence, from routine correspondence and phone calls to assisting his facilities directly in person.

Senior ISR Jeremy Lamps conducted an Arms, Ammunition and Explosives survey out-of-state, and provided guidance and addressed pre-assessment issues to a large, complex facility.

"What he is doing is very important, and it's great he has the opportunity to continue his service," Lamps said.

Senior ISR Jeannie Russell also said she was "proud to have one of our own serving in the military and supporting DoD as a civilian." She described how evident Mr. Stephens' personal passion is for protecting the warfighter, and how fortunate the Huntsville Field Office is to support the military by both upholding the NISP and assisting a work colleague when he is called away to serve.

Field Office Chief Mark Schoenig said, "I'm proud the Huntsville team came together to give Mr. Stephens some peace of mind in knowing his facilities were being supported in his absence."

Senior Industrial Security Representative Dale Stephens (right), a chief warrant officer in the U.S. Marine Corps Reserve, stands with Gabonese Marine Sergeant in Ayeme, Gabon.

Virginia Beach Field Office partners with government contracting activities at local level

by Susie Miller
Virginia Beach Field Office

Since assuming the industrial security mission in 1980, the Defense Security Service has had cognizance over cleared contractor facilities and has conducted thousands of security vulnerability assessments, answered thousands of questions, and conducted numerous advise and assist visits. Yet a large number of government contracting activities (GCAs) have not been introduced to DSS.

During a field office meeting, a junior industrial security representative (ISR) asked why some GCAs aren't aware of DSS and its mission. This question planted a seed, which prompted a chain of events that would ultimately benefit DSS and hopefully the GCAs. If the GCAs don't know DSS, then let's introduce ourselves. Ultimately, this single idea would be transformed into a simple, yet informative one-day, two-session presentation for over 120 local GCAs. The goal of the presentation: Partnership with GCAs.

The originator of the idea worked with the office senior ISR to include the industrial security systems professionals, the counterintelligence special agent, and the entire office staff to pull off the event.

The field office team decided, as a collaborative group, that the presentations would cover the who, what, when, where, why, and how of DSS. Each presenter would cover a topic relative to DSS, e.g., elements covered in a security vulnerability assessment, certification and accreditation process, CI functions, SIPRNet, JPAS, acquisitions (DD 254s), Industrial Security Facilities Database, and the sponsorship process.

Initial GCA responses to the invitations were greater than anticipated, so a second session was added to accommodate the overwhelming interest in the event.

Putting this project together took months of planning and effort, to include gathering email addresses, sending out invitations, finding a facility large enough to hold the event. The presenters tweaked their presentations to ensure the information could be summed up in 10 minutes. One of the ISSPs gathered images and logos of the cleared contractor base in the Hampton Roads area, and created a video, which was shown at the beginning of each session.

As the GCAs entered the facility, field office staff greeted attendees and exchanged business cards. As each presenter hit the 10 minute mark, the next speaker began his/her presentation and the meeting went off without a hitch! After the first session was over, it was clear by the reactions of the GCA group that the event was a success. The second session was as successful as the first. Ultimately the entire day was a complete success – with over 120 GCAs in attendance. Each attendee left with a folder filled with DSS products and a contact sheet with the local DSS Virginia Beach office's personnel names, phone numbers, and email addresses.

Almost immediately, feedback came pouring in from attendees after the presentations, to include phone calls and emails requesting more events like this in the future. Queries included, "Can you come to our command/ installation and provide a more intimate presentation?," and "I'd like a one-on-one meeting/presentation." A survey was sent out to provide a more organized way to document feedback and requests to better gather and document the feedback

GCAs across the country could benefit from events such as this one. The Virginia Beach Field Office is formalizing the process, so other field offices can duplicate this effort. If you are interested in obtaining more information regarding the process, presentation, etc., please contact the Virginia Beach Field Office for more information. If you are interested in seeing the video that kicked off each session, visit **https://youtu.be/o8YPdStnKKM**.

Wounded Warrior chooses agency for its reputation, values

Robert Scott III, a United States Army veteran, was wounded during his last tour of duty supporting Operation Enduring Freedom in Iraq. During one of his many visits to the rehabilitation center at the Walter Reed National Military Medical Center, he saw a flyer for a "Warrior Back to Work" workshop. The workshop offered a great opportunity to do something that mattered and feel useful again.

The workshop provided an explanation on how to transition from military life to the civilian and corporate world. The workshop was a key factor in his decision to register for the Warrior Back to Work Program.

As a part of the program, he attended multiple job fairs and was interviewed by recruiters from various corporations and agencies. He received several job offers based on his background and experience, to include an offer from DSS. He chose DSS, not because they were new to the program, but for their commitment to wounded warriors.

"I valued DSS's reputation, stability, core values, and the fact that DSS offered to provide hands-on training and

Robert Scott III

growth within the agency," Scott said. After his selection, he became one of the first people to join DSS's Wounded Warrior program.

In his time with DSS, he has enjoyed the team-oriented atmosphere and the endless opportunities open to him. He has learned aspects of physical security, personnel security, and industrial (policy) security.

"I endeavor to become more educated and proficient in all areas of security," Scott said. "Doing so will allow me to contribute throughout different areas of security and become a well-rounded security professional."

Andover Field Office enhances threat awareness through outreach efforts

by Kathryn Kimball
Andover Field Office

In an effort to strengthen partnerships and provide industry insight into counterintelligence concerns, the Andover Field Office recently enacted a new outreach strategy.

During the inaugural event, 14 industry security professionals were invited to the field office and provided tailored counterintelligence briefings and products. The outreach specifically targeted the smaller cleared contractors with the goal of providing the latest threat information in a secure, yet informal setting while conserving DSS time and resources.

Attendees were provided with a classified "Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting" briefing to help them understand the technologies sought by the nation's adversaries, as well as the methods used to obtain those technologies. Also, attendees were provided an Insider Threat policy overview that included discussion of the National Industrial Security Program Operating Manual Change 2 requirements relating to the Insider Threat Program, along with an a briefing that elaborated on the insider threat, behavior and indicators.

To capture feedback, attendees were asked to complete a survey about the event and to voice interest in future outreach opportunities. Overwhelmingly, attendees expressed their gratitude for the informative presentations, the time spent ensuring they had an understanding of their requirements, and steps they can take to reduce risk at their own facilities. As a result of this outreach event, industry security professionals are better prepared to integrate CI awareness into their security programs which ultimately reduces risk to national security.

Management support vital to effective, proactive security program

For the first time, company key management personnel participated in the 9th annual Quantico Area Industrial Security Council (QAISC) kick-off meeting, held in August 2016, at the Stephens Ridge Event Center, Spotsylvania, Va.

The QAISC, founded in August 2007, is managed by a board of seven facility security officers (FSOs) and has over 500 security professionals representing various defense contractors in the Quantico and northern Virginia regions. The QAISC meets monthly to strengthen security professionals' knowledge and compliance with the National Industrial Security Program Operating Manual requirements and to learn more about industrial security.

The annual kick-off event was hosted by the Spotsylvania County Economic Development Council Authority and the event showcases the "hard work and trying environment" the FSO must work in today. The Council has hosted this event for several years.

DSS Director Dan Payne, one of the guest speakers at the event, provided insight into the changes occurring within the National Industrial Security Program. He discussed challenges in implementing risk management and the integration of the Insider Threat Program Senior Official into facility security programs. During the meeting, Payne presented a Cogswell Award to Diane Moulton, QAISC chairwoman and vice president of EIOR Technologies, Inc., a 2016 Cogswell winner.

Guest speaker Rep. Robert Wittman, first Congressional District of Virginia and a member of the House Armed Services Committee, provided information on the 2017 DoD budget process and his efforts to procure funding to protect the nation and its warfighters.

The final guest speaker Mark Rasch, principal client partner for Verizon, focused on evolving cyber challenges facing industry today. Rasch shared his past experiences working with the U.S. Department of Justice, Computer Crime Unit, which developed into the Computer Crime and Intellectual Property Section of the Criminal Division.

In his closing remarks, council founder Senior Industrial Security Specialist Randall Stacey of the Chantilly Field Office noted "that the culture has to change because security is all of our responsibilities. The hard work of the FSO must be an effective enhancement of the security program and not just putting a check in the box.

"These challenges could not be accomplished solely by the FSO," he continued, "but management and employees must support their efforts to build an effective, proactive security program."

DSS Director Dan Payne (second from right) presents a 2016 Cogswell Award to Diane Moulton, QAISC chairwoman and vice president of EIOR Technologies, Inc.

Director visits San Francisco Field Office

The San Francisco Field Office (formerly known as Sunnyvale Field Office) recently hosted DSS Director Dan Payne as part of a larger visit with the U.S. Army. During the visit, Lt. Col. Enrique Oti, U.S. Air Force, provided an overview of the new way DoD is attempting to tap into the Silicon Valley technology base through Defense Innovation Unit - Experimental (DIU-X) - Sunnyvale. He provided real examples of new innovations being considered by DoD through the DIU-X streamlined acquisition process. Then, Western Region personnel provided an overview of operations and successes realized through the risk-based approach being piloted by the San Diego Field Office. Lastly, Payne spoke and answered questions from the San Francisco Field Office personnel on the direction he intends to take DSS and the reason for this approach.