DSS ACCESS

Official Magazine of the Defense Security Service | **Volume 6, Issue 1**

DITMAC Achieves Initial Operating Capability

VOL 6 | ISSUE 1

Defense Security Service

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: DITMAC ACHIEVES INITIAL OPERATING CAPABILITY

INSIDE

ASK THE LEADERSHIP

AROUND THE REGIONS

From the Director

I am excited about the opportunities and change that come with a new year and a new administration. I will mark one year at DSS just as this issue is published and I want to briefly look at what we have accomplished in that time and look ahead to what awaits us.

In particular, I want to note the article in this issue on the DoD Insider Threat Management and Analysis Center. Achieving initial operational capability was a huge milestone, one all of DSS should be proud of. I am pleased that Marcel Lettre, Under Secretary of Defense for Intelligence (USD(I)), was able to participate in the ribbon-cutting ceremony and I look forward to Mike Seage's leadership of the office. I also want to note our DSS by the Numbers. This snapshot is an annual look at what we've accomplished as an agency. What it doesn't show, however, is the work behind the numbers. The hours of preparation, research and behind-the-scenes activity that was critical to achieving these numbers.

During my swearing-in ceremony, I said my first priority was the integration of counterintelligence and security at DSS and I think we have made substantial progress in this area. One of our first initiatives was the risk based analysis and mitigation model. We are continuing to build on that model and move to an asset-driven, threat-focused assessment methodology. As we move into 2017, we will be looking to pilot the new methodology and seek input from our government and industry partners. Successful implementation at DSS will require close collaboration and seamless integration of counterintelligence and security. Quite frankly, it's the only way the model will be successful.

Another of my goals was to have DSS Counterintelligence activities designated as an official member of the Intelligence Community (IC). Shortly before his departure, Mr. Lettre signed a memo officially designating me as the head of a Defense Intelligence Component. In essence, this memo announces to all of DoD that the counterintelligence element of DSS is now officially a part of the Defense Intelligence Community. For legal reasons, this designation does not apply to all parts of DSS, but the benefit to DSS CI is a benefit to all of DSS.

In addition to these changes, we must also focus our attention this year on the Continuous Evaluation and Unauthorized Disclosure missions, which were assigned to DSS in 2016. Both of these missions will require new thinking and new ways of doing business.

While we move out on these initiatives, we will do so with a new administration and new leadership. I look forward to sharing the DSS story with the next USD(I) and Director of National Intelligence.

Thank you for all you do to support national security.

Dan Payne
Director

DITMAC achieves initial operating capability, holds ribbon cutting for new facility

by Ariel Hill and Kristin Mattice
DITMAC

In recognition of achieving initial operating capability (IOC), the Department of Defense (DoD) Insider Threat Management and Analysis Center (DITMAC) held a ribbon cutting ceremony on Dec. 12, 2016, in Arlington, Va. Then-Under Secretary of Defense for Intelligence Marcel Lettre presided over the event.

IOC, achieved in October 2016, followed finalization of the DITMAC and DoD Component Insider Threat System of Records Notice and associated exemption rules. This means that the DITMAC has the legal and technical capability to receive and aggregate reporting from the 43 DoD components on potential insider threat incidents.

During opening remarks, Dan Payne, DSS Director, commended the DITMAC for accepting the challenge of establishing an enterprise-level capability for insider threat information management. He recognized the challenging goals DITMAC accomplished, noting that any startup is a difficult task. He also shared his vision for DITMAC becoming an example for agencies across the federal government to follow.

Lettre congratulated DSS and the DITMAC on achieving the milestone and said it was particularly gratifying for him to see the maturation of the DITMAC. Lettre had observed it from its initial concept, while serving as Special Assistant to then-Secretary of Defense Charles Hagel at the time of the Washington Navy Yard shooting, through watching it achieve IOC and operate as envisioned. Establishment

Under Secretary of Defense for Intelligence Marcel Lettre (left) and DSS Director Dan Payne prepare to cut the ribbon of the new DITMAC facility.

of the DITMAC was one of five major recommendations following independent and internal reviews of the Washington Navy Yard shooting. Secretary Hagel approved the recommendation to establish the DITMAC on Feb. 21, 2014.

Lettre championed the importance of the DITMAC mission, reminding those present to never forget that they are part of something bigger than themselves. He said the DITMAC still has a challenging road ahead, but noted that there is a unique opportunity to promote innovation and pursue technological advances to aid in insider threat detection across the DoD enterprise.

Following his remarks, Lettre presented 14 members of the DITMAC with Certificates of Excellence, and took a tour of the facility. The DITMAC staff also provided a demonstration of DITMAC capabilities and an overview of reporting metrics.

The Under Secretary of Defense for Intelligence Certificate for Excellence reads as follows:

"The DITMAC team is recognized for exceptional service from October 2015 through October 2016. In one year, the DITMAC team successfully led a high-priority effort, reaching across the Department's 43 components and collaborating with the Office of the Under Secretary of Defense for Intelligence and the National Insider Threat Task Force to establish the DITMAC and achieve initial operating capability. The DITMAC team developed and established an organization with a mission never previously attempted at the enterprise level. The team's unwavering determination, perseverance, and dedication to this mission were instrumental in promoting collaboration and information sharing on insider threats to DoD personnel, information, and facilities, and will have a positive and lasting impact on the DoD Insider Threat Enterprise. The team's outstanding contributions and support reflect great credit upon them, the Defense Security Service, and the Office of the Under Secretary of Defense for Intelligence."

Certificates were awarded to Jeannie Alnidawi; Delice-Nicole Bernhard; Joel Brush; Michael Buckley; Mark Burns; Sara Elligson; Adam Goglia; Matthew Guy; Betty Leach; Marie Marciniak; Mark Nehmer; Keysha Pearson; Michael Seage; and Sarah Sullivan.

TOP: DSS Director Dan Payne (center) and Bill Stephens (left), director of DSS Counterintelligence directorate, greet members of the DITMAC team. **BOTTOM:** Payne (left) talks with then Under Secretary of Defense for Intelligence Marcel Lettre prior to the ribbon cutting ceremony.

Two DSS senior leaders named as PRESIDENTIAL RANK AWARD winners for 2016

TOP: Bill Stephens **BOTTOM:** Denise Humphrey

Two DSS senior executives were named as Presidential Rank Award winners for 2016. Bill Stephens, a member of the Senior Executive Service (SES) and director of Counterintelligence directorate, was named a Meritorious Executive. Denise Humphrey, a Defense Intelligence Senior Level (DISL) and deputy director of the Center for Development of Security Excellence (CDSE) was named a Meritorious Senior Career Employee.

The Civil Service Reform Act of 1978 established the Presidential Rank Awards Program to recognize a select group of career members of the Senior Executive Service for exceptional performance over an extended period of time. Later, the Rank Award statute was amended to extend eligibility to senior career employees with a sustained record of exceptional professional, technical, and/or scientific achievement recognized on a national or international level. Two categories of Presidential Rank Award are available:

- Distinguished Rank recipients are recognized for sustained extraordinary accomplishment, and only one percent of the career SES or senior level may receive this rank.
- Meritorious Rank recipients are recognized for sustained accomplishment, and no more than five percent of career SES or senior level members may receive this award.

In announcing the award, Stephens was recognized for the following accomplishments:

- Recognized unexploited opportunities for the U.S. to strike back against foreign intelligence entities stealing sensitive U.S. information and technology in cleared industry; built a CI capability that is now the driving force in how the U.S. Intelligence Community, law enforcement, and security communities address this acute national challenge.
- Established the DoD Insider Threat Management and Analysis Center — the first of its kind in DoD — and orchestrated its initial operational capability within 10 months, while simultaneously providing guidance to other DoD Components in maturing their own insider threat programs.
- Established the DSS Operations Analysis Group (OAG) to detect and resolve vulnerabilities and improve cross-functional DSS operational execution. To date, the OAG has reviewed over 3,205 cases, identified 2,515 vulnerabilities, mitigated 2,262 of those vulnerabilities, and prompted cleared companies to act on 1,726 insider threats.
- Developed and implemented the DSS Insider Threat Identification and Mitigation Program. Stephens was instrumental in procuring an insider threat auditing and monitoring capability, ensuring DSS's compliance with Executive Order 13587 and White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Program. The National Counterintelligence Executive hailed the DSS Insider Threat Program as the most advanced program not directly supporting an official Intelligence Community organization.
- Uncovered an analytical gap in DoD Major Defense Acquisition Programs (MDAPs) and launched the "Bronze Dragon" program to provide key analysis of threats, vulnerabilities, and consequences. Stephens contemporaneously created a "commercial due diligence" process that markedly increased DoD awareness of risks associated with MDAPs that uniquely managed national security risks resulting from commercial exposure which was a transformational achievement.

- Soon after his arrival, Stephens also recognized a need for DSS CI to collaborate more closely with cleared industry, launching "Grey Torch" to support cleared companies. He built an engagement program, set timelines and generated strong relationships that continue to grow today. Stephens established heightened awareness in cleared industry for risk management, particularly as it concerns threat.
- Conceived and championed the Enterprise Planning Integration Council, a three-tiered formal decision-making process integrating operation and business requirements across the agency.
- Developed "Thwarting the Enemy," a computer-based course that annually trains 50,000 security professionals in cleared industry with minimal impact to agency resources.
- Established and leads the first-ever DSS Cybersecurity Operations Division that today is aggressively addressing threats within the cleared industry cyber domain.
- Since his arrival at DSS in August 2009, Stephens generated record-setting performance every year as measured in absolute performance and per-employee performance. The results are revealed in Federal action: individuals attempting to or successfully stealing sensitive information or technology were identified by DSS CI professionals and, as a result, became subjects of Federal law enforcement investigations or sources for intelligence operations. In less than six years, the number of subjects DSS identified has grown 2,200 percent and efficiency has improved 800 percent.
- Stephens is a pioneer in educating, training and developing CI talent supporting the NISP. His innovative concept to field a computer-based training capability to educate cleared industry generated immediate, real results when the CDSE began training 40,000 industry security professionals annually with essentially no drain on DSS CI manpower.

In announcing the award, Humphrey was recognized for the following accomplishments:

- Established and serves as chair of the DoD Security Training Council, a DoD interagency body that provides recommendations to the Office of the Under Secretary of Defense for Intelligence for security education, training, certification, and awareness for the Department and serves as the governance body for the Security Professional Education Development (SPēD) Certification Program.
- Developed and fielded the DoD Security Skills Standards, which serve as the foundational document to codify required skills for security professionals within the Defense Security Enterprise (DSE). She accomplished this through collaboration across the Military Components and Fourth Estate activities to specify the essential body of knowledge and essential body of work for DoD security personnel.
- Initiated the development of a CDSE Education Program designed to provide graduate-level security studies for the DSE to prepare security professionals for current and future security planning and leadership roles. The first of 17 graduate studies-equivalent courses was beta tested in June 2011 and presented in January 2012. After development of the courses, CDSE achieved graduate college credit recommendations from the American Council on Education, which enables students to use CDSE courses for college credit. There have been 663 course completions since the initiation of the advanced security studies curriculum.
- Designed, developed, and implemented the SPēD Certification Program, the first comprehensive, high stakes, legally defensible professional certification program within OUSD(I), which paved the way for later development of Intelligence Community certification programs. The first certification, Security Fundamentals Professional Certification (SFPC), launched in FY11 and there are now three core certifications and four specialty certifications. Since the inception of the SPēD Certification Program, over 5,000 certifications have been conferred upon security professionals throughout the Federal Government. This program achieved the first national accreditation of a U.S. Government-developed professional certification program (the SFPC accredited by the National Commission for Certifying Agencies), followed by accreditation of two additional SPēD certifications.
- Humphrey was singularly instrumental in the conversion of content for CDSE's instructor-led courses into foundational learning modules via eLearning. This enabled CDSE to develop topical security training that addresses the needs of both security professionals and all other personnel who require security training and awareness (such courses include Marking Classified Information, Active Shooter Awareness, Insider Threat Awareness, and Derivative Classification).
- Spearheaded the effort to integrate virtual environments into the curriculum at DSS. As a result, military service members, DoD civilian employees, and other government personnel are able to apply their knowledge in a realistic three-dimensional environment.

UPDATE ON THE NISP Contract Classification System (NCCS)

by Lisa Gearhart
Industrial Security Integration & Application

After testing several significant revisions, NISP Contract Classification System (NCCS) version v5.9.1 was released as full operating capability, which means that NCCS has met initial system and business requirements, and is ready for implementation as a production site.

This milestone was achieved when NCCS successfully tested a critical capability, which allowed cleared industry to see prime contract DD Form 254s, and to originate and certify subcontractor DD Form 254s.

The NCCS serves as more than just an automated DD Form 254 system. The system allows both government and vendors (industry) to originate a Facility Clearance Request, and vendors can originate a Request for Approval to Subcontract when they need to subcontract for COMSEC, CNWDI, TEMPEST, SCI and NATO. In spring 2017, the National Interest Determination process will be automated, and industry will be able to use their prime DD Form 254 to originate their subcontract 254s within NCCS.

In December 2016, system users included six government agencies and eight industry partners, who assisted in the implementation of NCCS. Over the next year, DSS will do a phased implementation with DoD Components, Federal executive branch agencies and cleared contractors to establish accounts for NCCS.

NCCS – System Implementation

- **Full Operating Capability (FOC)**: Reached Dec. 23, 2016
    - 6 agencies/8 industry implemented NCCS
- **Phase III:** January - April 2017
- **Phase IV:** May - August 2017
- **Phase V:** September - December 2017
- **Phase VI:** January - April 2018

What is a DD Form 254?

The DD Form 254 is a resource for providing security requirements and classification guidance to a contractor. The DD Form 254 is a U.S. publication referenced in the Defense Federal Acquisition Regulation (DFAR) and applied to contracts involving access to classified information by U.S. contractors.

NCCS registration is role-based and set up with location codes: DoD – DoDAACs; non-DoD - Agency Codes; Industry – CAGE Codes. A company or agency must have a General Account Manager (GAM) established with the company/agency Location Code(s) before user roles can be added. The GAM should be the person(s) who will register all the location codes. Based on the size of the agency or company, it may end up being a tiered hierarchy GAM level, similar to Joint Personnel Adjudication System (JPAS) or e-QIP.

- The GAM can edit user profile information for two levels: Their own level and the level below their level.
- The GAM has view-only access to user information for all other levels below their current level.
- Registration is based on location codes. A GAM can have user roles too.

The following are additional user roles:

NCCS GAM – Will have the ability to administer the groups, users and roles for the NCCS location codes and users.

Government Originator – This access allows Government support contractors and Government users to initiate, save, recall, resubmit and void the DD Form 254. Government users may create prime 254s.

Vendor Originator – Vendors/contractor users can initiate, save, recall, resubmit and void the DD Form 254. Vendors may create subcontracts at the Tier 1, Tier 2 and Tier 3 levels.

Government/Vendor Reviewer – This access allows vendors/contractors, Government support contractors and Government users to recommend certification, reject, hold or recall the DD254 depending on the status.

Government/Vendor Certifying Official – This access allows vendors/contractors and Government users to certify, reject, hold or recall the DD254 depending on the status.

Government Contracting Officer – This access allows a Government Contracting Officer to review and approve accesses with the Request for Approval to Subcontract that is submitted by the vendor.

If you are interested in testing NCCS or getting in to see the functionalities, go to the DSS website for more information: **http://www.dss.mil/diss/nccs.html**.

NCCS – Setup Requirements

There are specific NCCS machine setup requirements that include DoD certificates and JAVA that are required to digitally sign the DD Form 254s: **https://wawf.eb.mil/xhtml/unauth/web/homepage/machineSetup.xhtml**. The NCCS developer is responsible to provide training support to the NCCS application. These web-based training links are found on the WAWF production site. Users can find NCCS specific training as follows:

1. Navigate to the URL **https://wawf.eb.mil**
2. From the Login page, click the Help/Training button at the top of the page
3. Click the Web Based Training link located in the Training section
4. Click the NCCS icon
5. Click the NCCS Roles and Registration link under the Roles section

INSIDER THREAT
CDSE committed to providing timely security training, awareness products

by Rebecca Morgan
Center for Development of Security Excellence

The Center for Development of Security Excellence (CDSE) works to provide timely security training and awareness products and courses. In response to Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, and the national minimum standards on insider threat, CDSE rapidly produced two eLearning courses. These courses focused on the categories of training identified in the policy -- awareness training for the general workforce and tailored training for insider threat program team members.

With the subsequent release of the DoD insider threat policy and Change 2 to the National Industrial Security Program Operating Manual, CDSE launched an insider threat awareness campaign to include the virtual insider threat symposium, which was a four-hour live production attended by 987 security professionals. It was followed by an insider threat/counterintelligence speaker series, where the community leaders engaged over 1,800 insider threat professionals directly.

As the insider threat program continued to mature within the DoD and federal government, CDSE recognized a singular learning event would not adequately promote the desired culture shift in the DoD community, but a training continuum was required. CDSE conducted a Training Needs Analysis (TNA) with stakeholders to ensure future development aligned to current and emerging community needs.

The result of the TNA was a five-year plan for development of training for the DoD insider threat program workforce. For FY17, CDSE will launch four new eLearning courses to enhance the knowledge, skills, and abilities of insider threat program personnel on such topics as insider threat indicators in records checks; developing multi-disciplinary insider threat capability; insider threat mitigation response options; and preserving investigative and operational viability. Also in development is a "Short" for insider threat program senior officials and a webinar with an associated job aid on identifying anomalous activity in user activity monitoring. These materials are being developed in coordination with leadership and stakeholders across the community.

CDSE continues to work closely with the DoD Insider Threat Management and Analysis Center and Office of the Under Secretary of Defense for Intelligence to craft a strategic vision for DoD insider threat messaging, awareness, and communications materials. By providing the DoD components, industry partners, and other elements within the intelligence community and federal government a suite of resources from posters, videos, games, and messages, CDSE is providing the products and tools to enable general workforce readiness to respond to the insider threat.

More than 500,000 students completed insider threat awareness training during calendar year 2016. In recognition of CDSE's efforts in providing insider threat training and awareness, the then-USD(I) Marcel Lettre named CDSE as the center of Insider Threat Training for DoD in a Memorandum dated July 2016.

Questions on cyber reporting can be directed to your local DSS representative or field office.

What is unconscious bias, how could it affect workplace interactions?

by Raymond F. Campbell
Office of Diversity and Equal Opportunity

Equal employment opportunity training largely focuses on the rights and responsibilities of agency employees, the process for initiating and filing a complaint from start to finish, and laws/statutes related to equal employment opportunity.

Diversity and inclusion training focuses on cultural awareness/cultural competencies, recruitment and outreach strategies, generational differences, disability etiquette, and improving communication between differences – whether it is differences in thought, processing techniques, work habits, or some demographic variable between people, such as race, national origin, gender, age, etc.

One diversity topic studied and analyzed over the years is unconscious bias. Some writers also refer to it as implicit bias and nonconscious bias. The terms are used interchangeably with the same core meaning -- a bias that we are unaware of and which happens outside of our control. It is a bias that happens automatically and is triggered by our brain making quick judgments and assessments of people and situations, influenced by our background, cultural environment and personal experiences.

While most of us may believe we have no biases or can suspend our biases when it comes to workplace decisions or interactions, the fact is we all have unconscious biases. Naturally, our biases affect not only our worldview, but also our decision making -- sometimes without us even knowing.

The Office of Personnel Management has been trying to better understand the concept of unconscious bias and how it can affect the workplace. New training classes on the subject are being introduced to some agencies. While DSS hasn't incorporated a full training session on unconscious bias, senior leaders have taken initial training and the agency has plans to roll out complete training to all DSS employees starting in fiscal year 2017. DSS employees also have access to unconscious bias training through Skillport. A good start is the book, "Blind Spot – Hidden Biases of Good People," which helps understand the concepts associated with unconscious/implicit bias.

Interested in discovering your own unconscious bias? There's an effective tool available for testing one's own unconscious bias - the Implicit Association Test (IAT). The IAT was created and is maintained by Project Implicit, a consortium made up of researchers from Harvard University, the University of Virginia, and the University of Washington. The IAT was created more than 10 years ago and has been used by millions of people in over 20 countries.

> “
>
> **Unconscious bias** -- a bias that we are unaware of and which happens outside of our control.
>
> ”

The IAT is offered to interested individuals as a tool to gain greater awareness of their own unconscious preferences and beliefs. The IAT can be completed free of charge as self-administered demonstrations. After accessing the Web address, select "Project Implicit Social Attitudes." You can complete the activity as a guest by indicating your country and then proceeding.

Editor's Note: Campbell participated in an interagency policy group to develop a framework for the federal government on identifying and reducing the effects of implicit bias, and providing tools/training opportunities to address unconscious bias across the federal government. This Interagency Policy Group, led and coordinated by the Office of Science and Technology Policy, worked together on the White House Council for *Increasing Diversity in the STEM Workforce by Reducing the Impact of Bias*.

INTRODUCTION TO COUNTERINTELLIGENCE

New course seeks to increase field operations awareness of CI principles, techniques

by Ken Reuwer
Counterintelligence Directorate

DSS Director Dan Payne stated, “I want to see DSS as a more integrated part of the Intelligence Community … We formulate security policy based on the threat picture. CI brings us what that threat picture looks like. We can’t have one without the other.”

In response, the Counterintelligence (CI) and Industrial Security Field Operations (IO) directorates developed the “Introduction to Counterintelligence Course (ICIC),” that introduces DoD and federal government CI principals and techniques to security professionals in a one-week resident course. The inaugural course was held in November, 2016 at the Counterintelligence Training Center (CITC) in the FBI’s National Academy Building, Quantico, Va., as will be future iterations.

Supervisory Special Agent Doug Pulzone, a Defense Intelligence Agency employee on detail to DSS; CI Special Agent Paul Godlewski, from the Albuquerque Resident Office; and Ken Reuwer, CI advisor to the Operations Division were the core team members in developing the course and partnered with the FBI’s Counterintelligence Training Center to host the course. The team’s top priority was to educate

Attendees of the Introduction to Counterintelligence Course in front of the FBI National Academy Building.

and sensitize IO employees on CI theory and practice, and prepare them for tactical CI situations they could encounter while working with cleared industry. Students of the inaugural course were introduced to CI programs at other government agencies to include capabilities briefs, functional services, and case studies of operations based on DSS referrals. Now, the graduates of the course can recognize CI opportunities and concerns within cleared industry, and they can more readily address them or more promptly refer them to their respective CI special agent for a formal response.

Each block of instruction ended with a question and answer session with the presenters or subject matter experts. The discussions were engaging and detailed often sending the class into extra hours.

By happenstance, FBI Director James Comey made an impromptu guest appearance with the class and was pleased to learn his agency had been hosts for and supporters of this joint schooling with DSS.

The week ended with Mark Allen, CI deputy director, and Heather Sims, IO assistant deputy director for operations, making closing comments, and thanking the CITC for its logistical support. They also acknowledged the numerous government partners who contributed to the production of this course from across the federal CI and Law Enforcement community. FBI Supervisory Special Agent Mark Betten, CITC's acting Director, and SA Brian Weidner (FBI retired) represented the CITC.

After the course ended, the development team reviewed more than 50 pages of notes and comments, to include non-attribution course critiques submitted by the students. This review was done to ensure the course met all expectations, that viable recommendations are adopted in future courses, and that appropriate corrective actions address attendees' criticisms or suggestions.

Some examples of comments were:

- "Country specific threat briefings were fantastic. This is an area most industrial security representatives have little experience in, and more understanding of adversary methods is very helpful in seeing an accurate picture of the threat."
- "Many thanks to all who saw the need, approved and facilitated the course. I highly recommend it for all in DSS."
- "This course was phenomenally constructed and the impact to the field should be evident in the short term."
- "Professionally developed, organized and executed by (subject matter experts). The course structure and class discipline flowed nicely and led to an environment of increasing thought and evaluation."

Based on the favorable response from the attendees, who readily agreed the course improves their abilities to be more well-rounded security professionals with a working knowledge of the CI mission, the course has been renewed and will be continued three times per year with a goal of having all IO field personnel attend.

A Q&A with **Michael Seage**, Director, DoD Insider Threat Management and Analysis Center (DITMAC)

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

Michael P. Seage, a Defense Intelligence Senior Level Executive, is the Director of the DoD Insider Threat Management and Analysis Center (DITMAC). Seage assumed his current position in July 2016.

Q: Tell us about your background ?

I am third generation career military. My father served 35 years with the U.S. Marine Corps. I grew up traveling and moving, spending time in North Africa, Europe, Asia and Hawaii. His example inspired me to serve with law enforcement and then the U.S. Army.

I joined the U.S. Army in 1976 and served 30 years on active and reserve duty as a counterintelligence (CI) officer. I spent 27 years overseas and deployed 11 times, spending about 11 years away from my family. While in uniform, I deployed in support of Operation Desert Storm, to Somalia, and served as a United Nations military observer on two deployments in Sub-Saharan Africa. I ended my military career as the director, Intelligence Analysis and Production, U.S. Special Operations Command. I began my civil service career in 1995 with the U.S. Marine Corps as an analyst. I returned to the U.S. Army as a Special Agent with the Military Intelligence Civilian Excepted Career Program. I deployed seven times as a civilian, to Afghanistan with NATO and U.S. Forces Afghanistan, and Colombia.

Q: What led you to this position?

I am a CI special agent and have served in that role since 1979. CI focuses on the insider threat - espionage, terrorism, sedition, sabotage and subversion. Within CI, I served as an investigator, analyst, case officer, staff officer, and commander. I also studied information systems management in graduate school and developed a strong interest in cyber CI and cyber threats. Insider threat is an emerging discipline that fits well with my interests, education and training.

As to how I came here, I left Europe after 17 years overseas. My follow on assignment was with the U.S. Army Staff - G2. I served as the chief, Insider Threat, Intelligence Oversight and CI Policy. I focused on the CI and intelligence issues within insider threat. That changed when the Army G2 appointed me as the lead for the establishment of an Army insider threat program. Two years into the process, the Army funded and resourced its own insider threat program. During that time, I worked extensively with the DITMAC and the Under Secretary of Defense for Intelligence (USD(I) Insider Threat team. I became passionate about the insider threat mission. When the DITMAC leadership opportunity came, I left the Army, after 39 years, to work with the DITMAC team and DSS.

Q: What is the mission/vision for DITMAC for those who are unfamiliar with this new organization?

In 2014, the USD(I) assigned the Director of DSS, through the DITMAC, the mission of providing an enterprise insider threat capability for DoD. DITMAC's mission is to enhance the DoD's ability to mitigate insider threats to its people and assets by assessing risk, driving innovation, and promoting partnership.

The mission reflects a commitment to multiplying the Department's insider threat mitigation efforts in a coordinated manner. DITMAC will assess insider threat risk to aggregate, analyze, and contextualize information that components can use to take timely and appropriate mitigating actions. To drive innovation, DITMAC will leverage its expertise, track trends, identify leading ways to mitigate insider threat and continuously refine analytical and mitigation techniques. Lastly, DITMAC will promote partnership to establish collaboration and communication mechanisms that advance the enterprise's capability across the board.

DITMAC's vision is to protect the Department of Defense against insider threats.

While it has never been and will never be possible to defend against all insider threats, DITMAC looks to protect against insider threats through better risk identification and mitigation techniques, ongoing improvements, and collaboration. In protecting DoD, DITMAC must also balance critical ethical, privacy, and civil liberty considerations with the exigencies of its mission.

Q: It took two years to get DITMAC off the ground in terms of automation, policies, staffing, etc. What is the current status of the DITMAC?

DITMAC achieved initial operating capability on Oct. 17, 2016 and now can receive insider threat reports from the 43 DoD components via the DITMAC System of Systems SIPRnet portal. This system of systems provides an enterprise capability to centrally manage and analyze potential insider threat risk indicators submitted by the components and provides a single repository for DoD insider threat related information. A key element of achieving initial operating capability was the publication of the DITMAC and DoD Component Hub System of Records Notice and related privacy exemptions in the Federal Register. In addition DoD Directive 5240.16, change 1, Insider Threat established the DITMAC, defines our mission and assigns DSS the responsibility to manage our mission. We are fully integrated with our component stakeholders and report monthly to DSS and OUSD(I) leadership on our operational and enterprise status. We hired over 80 percent of the staff and will have the rest on board in early 2017. DITMAC spaces were completed and DITMAC now occupies two office spaces in Crystal City. We expect the remaining applicable DoD directives to be published soon. There is a lot going on with many good people helping us make it happen.

Q: DITMAC must rely on feedback and input from across DoD. How is DITMAC working with the rest of the Department to be effective? What are the challenges involved?

We brief the DSS and USD(I) leadership frequently. We have a strong outreach program at the senior and action officer level to train, assist and support our component stakeholders. We strive to personally meet with each of the components to better understand their needs and challenges so that we can better tailor our support to them. Our challenges are primarily policy and authority based. The issuance of critical insider threat policies and directives has enabled the component hubs to begin reporting to the DITMAC. Also, the component insider threat programs are in various stages of maturity which has a direct effect on their ability to report to the DITMAC. The DITMAC has endeavored to provide training and guidance to assist the hubs as they develop and will continue to do so.

Q: It seems that insider threat only gains people's attention when there is an incident, such as the Washington Navy Yard shooting. How do you maintain focus without losing people's interest or attention?

Communication with our stakeholders and training our supported members is working so far. We are developing a strategic communications plan to address this very issue. We have buy-in from the senior military and civilian leaders within the department today and we have to retain that into the future. We also have to retain the interest of our supported population. There is a lot of white noise out there that we have to compete with. Our goal is to help provide a secure operating environment for our workforce, from threats of physical violence, and by ensuring our sensitive and classified information and operations are protected. So far folks seem to be listening. Now we just have to stay focused and keep them all engaged and informed.

Q: The idea of being able to identify and then prevent an insider threat from taking action is very difficult. How does DITMAC try to accomplish that?

As our mission statement shows, we understand that it has never been and will never be possible to defend against all insider threats. DITMAC looks to protect against insider threat through risk identification and mitigation techniques, ongoing improvements, and robust collaboration across the enterprise. The 43 DoD components with insider threat programs have the lead in preventing and identifying such threats. The DITMAC is a resource for them to leverage to better enable them at achieving those goals. We assist in the assessment of the risk, provide subject matter expert support to guide their understanding of the risk and how to best respond, help them understand the environment they are working in and provide access to highly trained analysts who assist them through their research and analysis. In doing all of this our goal is to enable component decision makers to make informed choices when it comes to mitigating insider threat. And finally, we work closely with the Center for Development of Security Excellence on insider threat training and awareness

COMPREHENSIVE EFFORT UNDERWAY;
‘growing civilian leaders’ continues to be a priority

by Dr. Fred Bolton
Human Capital Management Office

DSS is engaged in a comprehensive effort to “grow civilian leaders.” This includes identifying leader development lines of effort, building a leader development model, and creating leader development materials to support core competencies and help prepare employees for the start of the 12-month Leadership Development Program (LDP) launching in the fourth quarter of fiscal year 2017. These efforts are being spearheaded by the Leadership Advisory Board and leader development advocates.

LEADER DEVELOPMENT LINES OF EFFORT

In supporting leader development, DSS is engaged in five primary lines of effort. These areas include policy and planning, programs, communication and outreach, integration, and support services. These efforts are synchronized to ensure that the leader development programs achieve the goal of providing DSS leaders with the knowledge, skills, and competencies to lead in the evolving and challenging 21st century security environment.

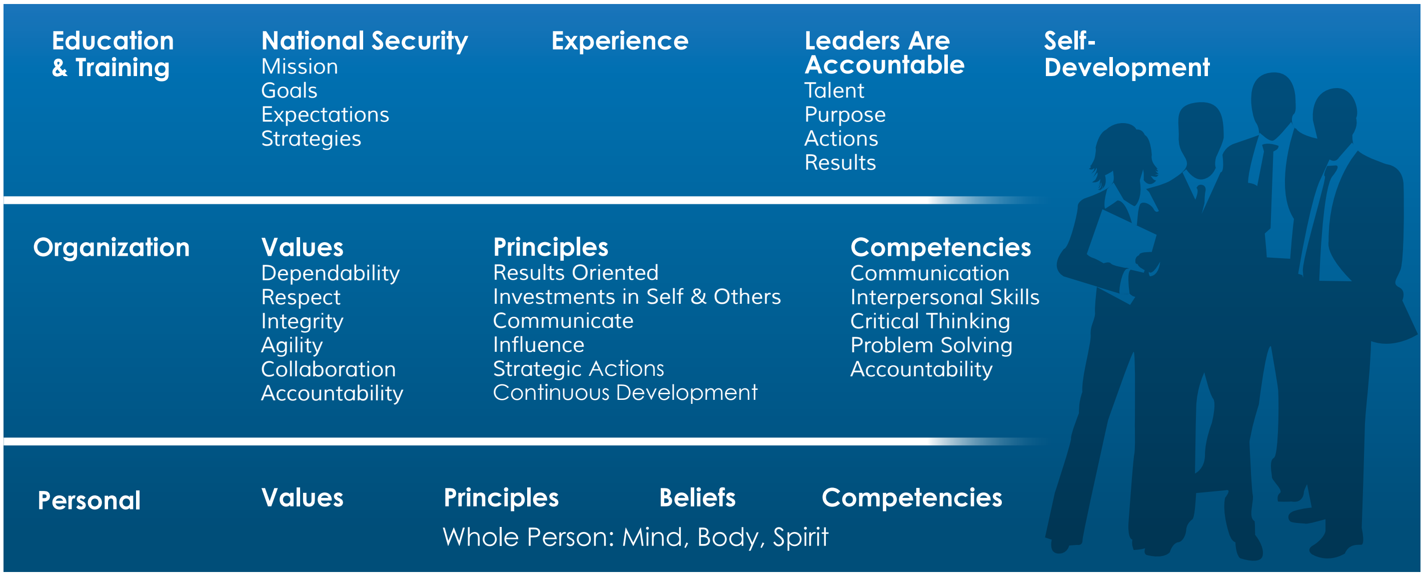
DSS Leader Development Lines of Effort
The main effort for the leader development team is in the programs area. Here the focus is on the development of learning activities that are immediately available to DSS employees as well as the development of the 12-month blended learning LDP. DSS employees don’t have to wait for the program to launch; online pre-requisite courses are available now for those interested. In addition, DSS employees have access to learning activities supporting several of the core leadership competencies with more being developed weekly.

Programs Policy and Planning Communications and Outreach Integration Support Services	**LEADER DEVELOPMENT END-STATE:** DSS leaders possess the knowledge, skills, and competencies to lead in the evolving and challenging 21st century security environment.

DSS LEADER DEVELOPMENT MODEL

The DSS leader development model emphasizes opportunities for individual growth through the pillars of education and training, experiences, and professional self-development. These pillars build on the foundation of personal beliefs, values, principles, and competencies, as well as the values, principles, and competencies of the organization. This model introduces a principle-based, value-centered, competency-focused, and mission-driven approach that drives all DSS leader development activities.

DSS Leader Development Model
Leader development activities also focus on opportunities that help develop the “whole person.” This ensures that leaders are people of character who are able to



Education & Training

National Security
Mission
Goals
Expectations
Strategies

Experience

Leaders Are Accountable
Talent
Purpose
Actions
Results

Self-Development

Organization

Values
Dependability
Respect
Integrity
Agility
Collaboration
Accountability

Principles
Results Oriented
Investments in Self & Others
Communicate
Influence
Strategic Actions
Continuous Development

Competencies
Communication
Interpersonal Skills
Critical Thinking
Problem Solving
Accountability

Personal

Values

Principles

Beliefs

Competencies

Whole Person: Mind, Body, Spirit

demonstrate DSS leadership principles and behaviors.

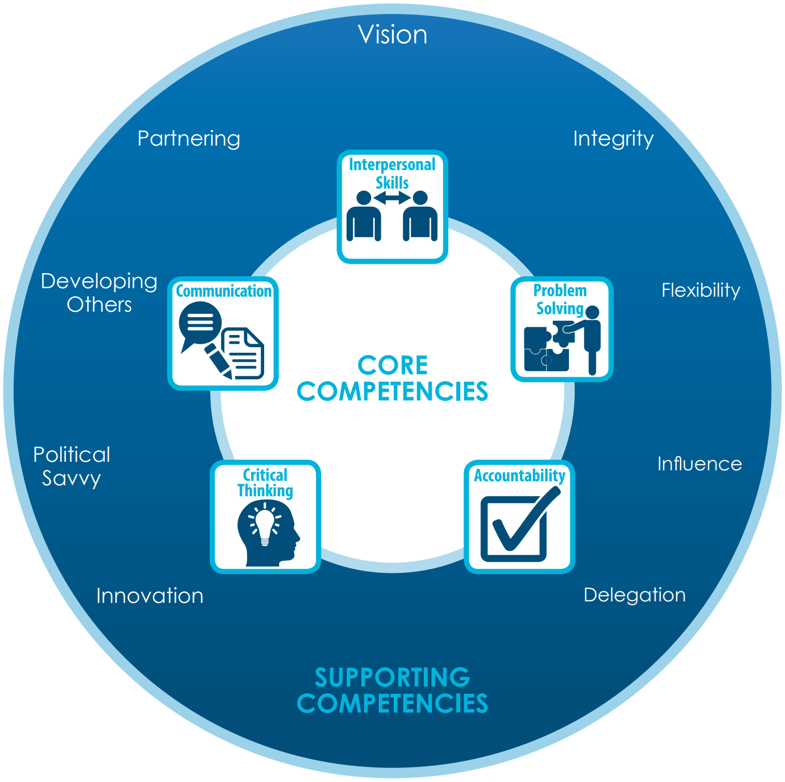
As one of the pillars of leader development, Education and Training focuses on formal opportunities to acquire knowledge and skills that when applied foster the creation and continued development of high performing leaders. Within DSS, leadership education occurs during a variety of organization-sponsored training beginning with New Employee Orientation. Formal leader education programs include the DSS LDP and participation in advanced and executive leader development activities.

DSS Core and Supporting Leadership Competencies

The majority of the leader development resources are provided through Skillport which offers employees access to a robust and high quality source of materials, to include online videos, eBooks, audio books, and courses. Learning resources can be accessed at home and work via desktop and mobile devices. The DSS team is also active in identifying and linking other resources internal and external to DSS and DoD that can enhance leader development at all levels of the organization.

A major effort supporting the communication and outreach line of effort has been the development of a comprehensive Leader Development intranet site. This site was recently launched and features links to information on activities and services related to leader development including short leadership lessons, announcements of leadership events, and access to reading lists, movie lists, and competency focused courses, as well as information on the internal DSS LDP and associated online pre-requisite courses.

The DSS leader development team is available to provide consultation and training activities focused on leader competencies and performance improvement at the individual, team, and work unit level. Regardless of your role in the organization or the extent of prior leadership education, there are always opportunities to engage in personal growth and development.



Director outlines vision for new way of doing business

In his initial remarks to the agency, DSS Director Dan Payne said, "Today the United States faces a counterintelligence threat that is unprecedented in the history of this nation. Advances in science and technology make the ability of our adversaries to steal our secrets and our technology far easier than ever before."

In October, Payne held an agency town hall to introduce his vision for transitioning the agency to a new method of operation to meet this threat. Payne again addressed the threat by citing recent examples of the theft of national security and sensitive information. "We know of front companies that are set up just to steal information," he said. He also cited examples of U.S. companies becoming involved in joint ventures with foreign companies who then have access to sensitive information.

"This isn't an effort to scare anyone or a call for more resources," Payne said. "This is real and it's happening at an alarming rate."

Payne said to meet this challenge, DSS must change its strategy and methodology and move from a schedule-driven, NISPOM-focused assessment to one that is threat-based and asset-driven.

DSS Director Dan Payne talks about the future of DSS at a recent town hall.

LEFT: DSS senior leaders listen to the director discuss ongoing initiatives. **RIGHT:** Payne talks about the future of DSS at a recent town hall. (Photos by Hollie Rawl, CDSE)

"The NISPOM provides a static set of guidelines," he said, "but it doesn't consider what needs protection and what methods are being deployed against it."

Instead, he said, DSS would take a threat-based approach with a global view. Such an approach would be based on knowing the critical assets at cleared facilities, analyzing the threats to the assets and developing measures to protect and defend the asset.

Payne said the Change Management Office, championed by Kevin Jones of the Center for Development of Security Excellence, was developing a standard operating procedure that, once completed, would be shared with industry and government stakeholders for discussions. Following that would be a series of pilots in 2017 designed to capture lessons learned and best practices.

"Change is difficult," said Payne. "But if we do not change, we will become irrelevant and not able to protect national security information as we should. Everything we do will be geared toward protecting national security information."

In closing, Payne asked for the support of agency personnel. "Work with us to make it better," he said. "We [the senior leadership team] don't have all the answers, but we are moving out. We will continue to fill in the blanks as we move forward."

DSS Chief of Staff Troy Littles discusses the results of the Federal Employee Viewpoint Survey at a recent town hall.

CHIEF OF STAFF holds town hall, provides update on ongoing initiatives

by Beth Alber
Office of Public and Legislative Affairs

In his first town hall as the DSS Chief of Staff, Troy Littles provided an update on ongoing initiatives, the results of the Federal Employee Viewpoint Survey (FEVS), and what the future holds for the agency.

"I've been the chief of staff for about 13 months," Littles said at the event on Dec. 7, 2016, which was streamed to DSS offices across the nation, "and I wanted to share where we're going as an agency, as well as update you on some initiatives. I want to hold these sessions semi-annually to share what we're doing, but also to recognize DSS employees and their accomplishments."

In discussing the creation of an agency leadership development program, Littles explained the impetus behind a formalized program, and the direction the program will take in the coming year. "The idea came from the field, who asked for a formal leadership development program," Littles explained. After reviewing programs of other government agencies, DSS gleaned best practices, and developed an advisory board.

> We know that we're asking employees to do a lot, with limited resources. ... We're looking at our options to **distinguish employees in a meaningful way**.

“Now, we’re soliciting ideas on how to run a program, changing the current model from employee driven to agency driven,” he said. He noted that once it’s established, it will be the primary leadership development training program for the agency. “You will be required to complete the program before being allowed to take any outside leadership development courses,” Littles noted.

Another initiative within the agency is the creation of the DSS Diversity and Inclusion Council (D&IC). “I was attending a senior leader seminar on diversity, and the question was raised, ‘what are you doing to increase diversity within your agency?’ And I couldn’t think of a good response,” Littles said.

Working with the DSS Office of Diversity and Equal Opportunity resulted in the establishment of an Inclusion and Diversity Steering Committee, whose members crafted a draft charter for the D&IC. Once established, the goals of the D&IC will be to cultivate a culture that encourages collaboration, flexibility and fairness to enable individuals to contribute to their full potential; recruit from a diverse, qualified group of potential applicants to secure a high-performing workforce drawn from all segments of American society; and develop structure and strategies to equip leaders with the ability to manage diversity, be accountable, measure results, refine approaches on the basis of such data, and institutionalize a culture of inclusion.

“This is an important initiative because any organization performs better with a diverse viewpoint,” he said, noting the council will be comprised of up to 20 people, with the steering committee members forming the foundation of it.

Feedback is vital for agency leaders to determine if they are providing a healthy environment for its workers, one that encourages collaboration and provides the resources necessary to accomplish the mission. To ensure the agency was on track, DSS senior leadership asked employees to complete the FEVS. The FEVS is a tool that measures employees’ perceptions of whether conditions characterizing successful organizations are present in their organization. The results of the survey provide senior leader insight on how well they are doing, and how they rank in comparison to other agencies.

“We had an outstanding response rate at 71 percent,” said Littles, noting that the overall DoD response rate was 26 percent. “Most input came from the field where the heavy lifting is being done,” which is consistent with the 2015 survey results.

Littles noted a few insights from the survey, the first being that employees understand the constraints of the agency and actively seek opportunities to work together to achieve objectives. “DSS has cultivated a strong team culture,” he said.

Additionally, employees understand the importance of their work and how it relates to the agency’s mission, yet only 42 percent said their workload is reasonable and 45 percent said they have sufficient resources to get the job done.

“We know that we’re asking employees to do a lot, with limited resources,” he said. “And we’re looking at our options to distinguish employees in a meaningful way.

“What you do is important and we know it’s important,” Littles said in his closing comments. “We know we ask you to do a lot of things, and know that the excellent work you do hasn’t gone unnoticed.”

> **What you do is important** and we know it's important ... We know we ask you to do a lot of things, and know that the **excellent work you do hasn't gone unnoticed**.

OFFSET STRATEGIES yield a decisive advantage; security vital to safekeeping of game changing innovations

by David Bauer
Director, Western Region
Industrial Security Field Operations

In 2014, then-Secretary of Defense Chuck Hagel announced the third offset strategy as a way for the Department of Defense to maintain military superiority in an environment of reduced military size and budget. An offset strategy is a competitive approach to maintain a military advantage over potential adversaries through the development of "game-changing" innovations that yield a decisive advantage.

The first offset strategy, the development of atomic and nuclear research and weaponry, played a crucial role in the ending of World War II, shaped military strategy, and provided the U.S. military a significant advantage for decades.

The second offset strategy included extended-range precision-guided munitions, stealth aircraft, and new intelligence, surveillance, and reconnaissance platforms. The lethality of the second offset and supporting strategy was unveiled during the first Gulf War with devastating effect.

Now, as the Defense Department seeks the third offset strategy, they are making investments in robotics, autonomous systems, miniaturization, big data, and advanced manufacturing.

What does this new challenge mean for the Defense Security Service and cleared industry? How can this "game changing innovation" be protected from compromise so the innovation provides the advantage needed? Maybe we should look back to consider the path forward.

A HISTORY LESSON:

In 1939, two German physicists in Nazi Germany split an atom and discovered fission. This action launched a race to further develop atomic research, investigate the possibility of creating an atomic chain reaction, and potentially create an atomic explosion.

THE MANHATTAN PROJECT:

In 1942, the U.S. Army took over the pursuit of atomic energy research in the United States largely because researchers felt the Army was the best-prepared organization to enforce a security system to protect the work from the Axis powers. The Army instituted policies to strictly compartmentalize all sensitive materials and to provide security clearances for all employees involved in the research. In spring 1942, the Office of Scientific Research and Development began letting "numerous contracts with industrial firms; the employment and interaction of ultimately tens of thousands of workers, scientists, and engineers; and the formation of complex organizations to construct and operate the large-scale production plants and their atomic communities." The Army moved to bring the entire project under one organization, known as the Manhattan District.

SECURITY AND COUNTERINTELLIGENCE WITHIN THE MANHATTAN DISTRICT:

In June 1942, the Army established the Protective Security Section responsible for the Manhattan District security program. The section was responsible for personnel, physical, and information security programs, and counterintelligence support. The Army recruited 25 officers and 137 enlisted personnel to perform security and counterintelligence missions, to include plant inspections and technical and undercover operations.

SECURITY CHALLENGES:

The industrial security program was "one of the most challenging and complex aspects" of the Manhattan Project security program. Security inspectors representing

Robert Oppenheimer (bending over) and General Leslie Groves (center right), director of Manhattan Project, at the Trinity test site. (Department of Energy photo)

the district observed contractor methods of handling classified materials, correspondence, and registration statements to the Securities and Exchange Commission, and other avenues of disclosure that posed a potential weakness. When a contractor terminated their contract, the Manhattan inspectors would ensure all classified materials were returned to government control or destroyed.

The District program had aggressive information security programs, teaching project personnel to be instinctively alert and security focused. Security personnel also practiced strict need-to-know, limited employees to specific work areas, and concocted cover stories for activities that gave employees plausible explanations for other activities within the project.

Censorship remained a large security effort throughout the life of the project. Security officials reviewed leading daily newspapers and periodicals for potential leaks related to the atomic program, eventually growing to over 370 newspapers and 70 magazines. The Army determined a single leak could attract attention of espionage agents and saboteurs and provide information that would compromise the program.

Early in the program, Army leaders weighed the national security risk caused by the need for qualified scientists and technicians with their potential contributions to the program. General Leslie Groves, director of the Manhattan Project, stated that decisions "had to be based on what was believed to be the overriding consideration -- completion of the bomb. Speed of accomplishment was paramount."

United States leaders realized knowledge of the Manhattan Project could compel Germany, Japan, and even the Soviet Union to use espionage to destroy America's military advantage. The Manhattan Project counterintelligence program attempted to provide "the shroud of secrecy necessary to forestall all attempts by the enemy not only to gain information....but also to sabotage it." The counterintelligence program used investigations to minimize the likelihood of breaches to security. Counterintelligence agents investigated all information leaks, mishandling of classified information, and performed more in depth background investigations into cleared employees who posed a potential security risk.

On July 16, 1945, a 19-kiloton explosion, codenamed Trinity, ushered in the atomic age. In the end, a decisive technology provided the United States the advantage on the battlefield that led to the end of World War II. The Army's effort to protect the first offset proved successful in delivering the technology to the battlefield, providing a significant advantage over the adversary.

This short essay provides a glimpse into the security effort surrounding the protection of the first offset. Without a doubt, the loss of the first offset would have had dramatic impact on the world we live in today. Cleared industry and academia will be at the forefront in the search for new technologies leading to the third offset. The effectiveness of the partnership between cleared industry, cleared academia, and DSS in protecting the third offset today will impact the world of tomorrow.

PERSONS WITH DISABILITIES

One individual's journey to becoming an industrial security representative

Editor's Note: The life of an industrial security representative (ISR) is challenging, as new hire Jason Jernigan, an ISR assigned to the Maryland Hanover 1 Field Office, is discovering. Below is a question-and-answer between Jernigan and Field Office Chief Pamela Pryor about his road to becoming an ISR, handling the responsibilities and getting settled in at DSS.

Jason Jernigan, the newest employee to the Maryland Hanover 1 Field Office, is a native of Florida and has been deaf since 14 months of age. Jernigan successfully competed for an entry-level ISR position and was hired under the Persons with Disabilities Program.

You interviewed for this job from Florida, rather than in person. How did the interview go?

Because I wasn't in the Capital Region when DSS interviews were being conducted, my interview was conducted by phone and with the assistance of interpreters. I was able to view the interpreters from my mobile device, and the interpreters served as conduits between me and the DSS selecting official.

What assistance did the field office provide prior to your arrival?

After being hired, through extensive collaboration, discussions with partnering agencies, and assistance from other directorates and offices in DSS, the field office was successful in ensuring a seamless transition for me into my new role as the first hearing-impaired industrial security representative in the Hanover field office. Prior to in-processing, my field office chief collaborated with the DSS Office of Diversity and Equal Opportunity (DEO) to determine what accommodations I would need to perform my duties. Almost daily discussions took place between a number of DSS offices -- the field office chief, the Office of the Chief Information Officer, DEO, Security, Logistics Management, DoD Computer/Electronic Accommodations Program, Industrial Security Field Operations, Center for Development of Security Excellence (CDSE) -- and me. The field office secured an interpreting agency for me, installed a VTC and Video Relay Service, and safety apparatuses within the office.

Did you have any issues with the training that helped prepare you for this job?

During the NISP Oversight Course in-person sessions, I was accompanied by an interpreter who communicated the instructions for my group training assignments. I was also able to take courses that are closed-caption capable. I retrieved my lessons through the online DSS training system and take part in the CDSE group discussions with the other trainees.

Has communication been an issue since you've come on board?

I communicate through writing, American Sign Language interpreters, mobile apps, video relay, closed caption services, instant messaging and a two-way device. The two-way device resembles two laptops that allows for instant messaging and exchange of text only. The device has been vetted and poses no security concerns for use in a secure environment.

I also supplied the members of the Hanover 1 team with pocket-sized sign language reference books, and I used this opportunity to teach basic sign language to team members in the field office on an as needed basis. The soul of a disability is only understood if we can embrace it with the willingness for each one to teach one.

Have you participated in any vulnerability assessments yet?

I'm excited to be on board and have been formally introduced to my assigned cleared defense contractors (CDCs). With the assistance of my lead advisor and support of the Hanover staff, I've supported several of my assigned CDCs. I've also participated in a complex CDC team Security Vulnerability Assessment, conducted employee interviews, and participated in Counterintelligence briefings.

What is your background?

I've got a Bachelor of Science degree in Public Safety and Security and Criminology, with a minor in Underwater Crime Scene Investigation, from Florida State University. While at FSU, I served as the representative and elections chair for student government. Prior to coming to DSS, I have held administrative positions at the Department of the Navy and Department of the Air Force.

What do you like to do in your free time?

I love to fly planes and I received my pilot license in 2012. I am one of 2,000 hearing-impaired pilots in the United States. When I fly, I use specialized equipment along with the use of light gun signals from the control tower to assist with communications, which allows me to fly. This technology is similar to what I use for driving a vehicle.

"Jason is quickly learning the ins and outs of being an industrial security representative through on-the-job training and staying focused on his assignments," said Michael Sibley, an ISR who acts as Jernigan's lead advisor in the Hanover FO and functions as his DSS mentor.

TRIBUTE TO A KING: The Defense Security Service held a "Tribute to a King," in honor of Martin Luther King, Jr., on Jan. 18, 2017. In discussing a tribute to a king, guest speaker Pastor Vincent Allen said, "We must reflect, we must respect, and we must reconnect." Allen, who works for the Office of the Deputy Chief Management Officer, Office of the Secretary of Defense, said, "We need to celebrate each other; we need to learn to disconnect and reconnect with people, reconnect to the humanity of it all. If we fail to engage with each other, then we fail the ideal of the tribute to Martin Luther King, Jr." During the event, the audience heard musical selections from guest singer Valerie Dawkins and the Voices of DSS. (Photos by Hollie Rawl, CDSE)

FY16: DSS by the Numbers

CENTER FOR DEVELOPMENT OF SECURITY EXCELLENCE

256	**Education course completions**
10,246	**Personnel** registered for **webinars**
270,222	**PDUs** [Professional Development Units] **Earned**
92,762	**Visits** to **Security Shorts**
386,791	**Visits** to **Toolkits**
1,283,190	**Course completions**
1,100	**Conferrals** in Security Professional Education Development Certification Program

INTERNATIONAL ACTIONS

4,108	**Visit** requests
13,784	**Travelers**/visitors
7,565	**Foreign sites** visited
256	**Transportation** plans
188	**Hand carry** plans
30	**Security Vulnerability Assessments**

NISP AUTHORIZATION OFFICE

31	**NISP Command Cyber Readiness Inspections** led by DSS
3,634	System security plans **(SSPs) accepted and reviewed**

Common deficiencies in SSPs:

1. SSP incomplete or missing attachments
2. SSP not tailored to the system
3. Inaccurate or incomplete configuration diagram or system description
4. Inadequate anti-virus procedures

2,246	Completed **system validation visits**

Common vulnerabilities found during system validations:

1. Security-relevant objects not protected
2. Improper Configuration Management
3. Improper Automated Audit Trail
4. SSP Does not reflect how system is actually configured

FOREIGN OWNERSHIP, CONTROL OR INFLUENCE (FOCI)

573	**FOCI facilities**
314	**Mitigation action plans** in place

Each year it's a tradition to look back and get a sense of what has been accomplished. DSS is no different. The following are the "by the numbers" accomplishments of the agency:

PERSONNEL SECURITY MANAGEMENT OFFICE FOR INDUSTRY (PSMO-I)

814,070	National Industrial Security Program (NISP) **contractors with clearance eligibility**
742,838	NISP contractors with **access to classified information**
150,115	**Requests for investigation** for security clearances processed
64,347	Interim **security clearance determinations** made
5,500	**Adverse information reports** triaged
33	Interim **clearance suspensions** in process

FY16

COUNTERINTELLIGENCE

46,382	**Reports of suspicious contact** from industry
5,560	**Referrals to law enforcement/** Intelligence Community
1,117	**Investigations/operations opened** due to DSS referrals
7,583	**Intelligence Information Reports**
3,600	**Personnel** attending seven **Counterintelligence Webinar** events
954	**Personnel** attending three secure **VTCs with Industry**

INDUSTRIAL SECURITY FIELD OPERATIONS

5,136	**Security Vulnerability Assessments** conducted *(including Excluded Parents)*
8,440	**Security vulnerabilities** identified
7,740	**Non acute/critical vulnerabilities** identified
700	**Acute/critical vulnerabilities** identified
915	**Facility security clearances** issued

Defense Security Service