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

DSS ACCESS

Technology expands message of **2015 DoD Security Conference**

WINTER 2015

Volume 4, Issue 4

DSS ACCESS

Published by the Defense Security Service Public Affairs Office

27130 Telegraph Rd. Quantico, VA 22134 dsspa@dss.mil (571) 305-6751/6752

DSS Leadership

Director Stanley L. Sims

Deputy Director James J. Kren

Chief of Staff Troy Littles

Chief, Public Affairs Cindy McGovern

Editor Elizabeth Alber

Graphics Steph Struthers

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

The views expressed by the authors are not necessarily the official views of, or endorsed by, the U.S. Government, the DoD or the Defense Security Service.

All pictures are Department of Defense photos, unless otherwise identified.

From the Director

In preparing for this column, I went back to our first issue in April 2012. In that column, I said the ACCESS would "demonstrate the scope and range of activities in which DSS is involved that make the agency a valued partner." I also introduced my motto for DSS, "People First, Mission Always." I had already shared that motto with our workforce, but I wanted to ensure that our partners and stakeholders understood my philosophy and vision for DSS.

I looked back at that column because this will be my last for the ACCESS magazine. I will leave federal service and the Defense Security Service at the end of 2015. Serving as the Director of DSS has been an honor and a privilege. I realize those words may be cliché and what you would expect from anyone in my position. But anyone who knows me knows that this is the only job I want in the government. Serving in this position — alongside you — has been the highlight of my 36-plus years of military and federal service!

It was the highlight of my career because I believe DSS is an outstanding organization, with outstanding people who every day execute a unique mission to ensure the security of the warfighter and the nation. As I've said many times, we are the only ones who do what we do. DSS is one of the smallest of the DoD agencies, yet executes a national-level mission on behalf of the federal government.

DSS is at its heart and soul a security organization, yet is aligned with other intelligence agencies (all of whom dwarf DSS) under the Under Secretary of Defense for Intelligence. DSS's expertise is industrial security, yet it is the executive agent for all security training and education across the Department. Managing these dichotomies every day was challenging and often frustrating. But leading DSS and its workforce through five years of budget uncertainly, furloughs, shut downs, leadership changes, reorganizations, and shifting priorities was extremely rewarding.

So getting back to that first column, I believe this magazine has done just what I wanted it to do and achieved every goal I set for it. It delivered DSS activities, personnel and mission to a wide audience. It demonstrated the agency's value in partnering with industry and government stakeholders. And by highlighting our people, we put them first on these pages in each and every issue.

I leave DSS with fond memories and pride in knowing I was able to contribute to the agency's success these past five years. Always remember, YOU — our people — matter, and what you do matters. DSS will remain "Our Agency, Our Mission, Our Responsibility!"

Thank you dearly for all you do to support our nation!

A Q&A with the Director

Editor's Note: Prior to his departure from the Defense Security Service, DSS Director Stan Sims sat down for an interview to share his thoughts on his tenure.

What do you see as your legacy at DSS?

I came to DSS from the Security Directorate (now the Security Policy and Oversight Division) at the Office of the Under Security of Defense for Intelligence (OUSD(I)). While I was there as the Director, I had the chance to watch DSS from afar but also engage with the staff up close on a number of issues.

So I knew quite a bit about the agency before I became the Director. And one of my top goals when I came to DSS was to change the culture. I believed at the time and continue to believe that a pure compliance-only view of the National Industrial Security Program (NISP) is off-base. So I wanted to instill a culture within the agency workforce that treats industry as national security partners.

DSS has a workforce of around 900 people with responsibility for over 13,000 cleared facilities. We have to encourage and empower industry to take responsibility for their security programs. Now DSS is here to advise, assist and support them, but we can't do that with a hammer. The better way is to work with industry as partners for the good of national security. And I think we have been pretty successful in changing that culture.

I also wanted to revive DSS in the NISP and bring it back to relevance. Again, from my view at OUSD(I), I knew there were and still are, senior leaders in DoD and across the government who did not know or understand what the NISP was, DSS's role in it, and why it was important.

I am a strong believer in the value and necessity of a single, cohesive national-level industrial security program. So I wanted to share that message and ensure it was relevant. I think we have made progress here, but it's a constant process of educating up and down and across the chain of command as leadership changes.

What accomplishments are you most proud of?

I think there are several things that I am proud of. One of my first priorities was to improve the organizational climate within DSS. I did that by focusing on the people (People First, Mission Always), programs and processes. I wanted to instill a shared feeling in the workforce of what it meant to work here and what life is like

A DIRECTOR IN ACTION; FROM LEFT: Stan Sims, DSS director, opens the 2015 Organization Day, held in June 2015. | Sims (right), settles the wreath at the 2015 Joint Police Week ceremony, held in May 2015. | Sims (left), welcomes James Clapper, Director of National Intelligence, to the Russell-Knox Building, Quantico, Va., in May 2013.

at DSS. A key component of that was to restore the workforce's confidence in leadership and to have a stable leadership team.

Second, I wanted to bring pride back to DSS. The agency had endured more than its share of negative publicity going all the way back to when it had the mission for personnel security investigations. I believe you have to have pride in your organization and in who you are. Without that, how do you have pride in your job and where is the motivation to do the best you can? I think we were able to do that by focusing on "Our Agency, Our Mission, Our Responsibility."

I also wanted to raise the credibility of DSS across the Department and the government. We know what we're doing here. In fact, we are the only ones who do what we do and we're good at it.

FOCI [foreign ownership, control or influence] is a good example. We now have other agencies asking for our advice because they recognize we are the FOCI experts in the federal government. We are now included in working groups and other discussions because of our expertise and our proven track record of success.

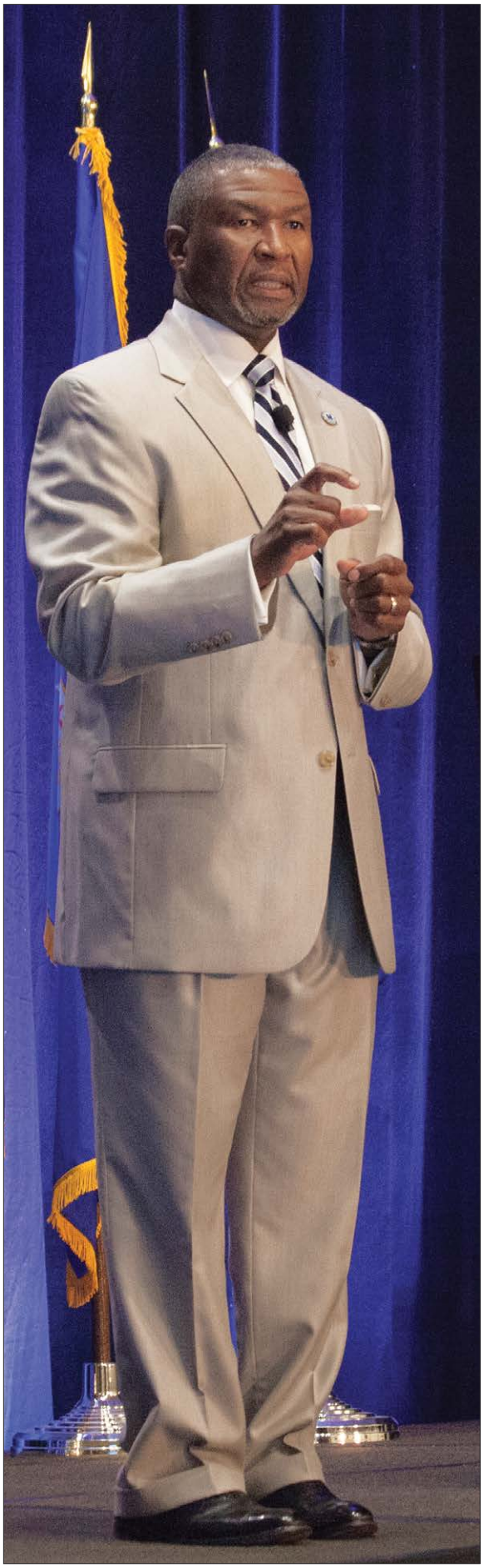
Finally, I am proud of our new Headquarters. Now, we were required to move to Quantico, but we have made the Russell-Knox Building our home and put our mark on it. We have embraced the building and the larger community and for the first time in its history, DSS truly has a place to call home and to be proud of!

What did you not accomplish that you wanted to? What is left "undone" in your estimation?

That's hard to answer because the agency's mission is evolving, but I think it has been manpower resources for DSS. I have not been able to convince the Department that a small resource investment in DSS is a huge investment in national security.

To quote a wise man, "a small investment in DSS would pay huge dividends to national security." Our field workforce is out every day in industry, where our nation's warfighting technology is produced. By not investing in DSS, it forces us to make priority decisions about our workload and ultimately forces us to accept more risk.

"To quote a wise man, **'a small investment in DSS would pay huge dividends to national security.'** Our field workforce is out every day in industry, where our nation's warfighting technology is produced."



Several months ago, DSS became a part of the Department's effort to reorganize the Defense Security Enterprise to support a "unity of effort" approach. The goal is to bring the Defense Security Enterprise more in line with how the Defense Intelligence Enterprise is organized.

A problem we have seen is that there are disparate pieces of the security puzzle spread across the Department. And while the USD(I) is the Principal Staff Assistant for security, the USD(I) doesn't have authority over all those pieces. This may not lead to an actual reorganization, but for security to be more effective, there has to be unity of effort and that can only be achieved through unity of command. So this is still a work in progress.

Finally, we started work on a Leadership Development Program at DSS, but it hasn't quite come to fruition yet. I think this program will serve our people and ultimately, our agency, our mission and our nation.

What advice do you have for your successor?

Roll up your sleeves, there's work to do and be prepared to work overtime! DSS is a small organization with more responsibility than any organization its size should have, and there is no one else to do the work. You have to get your hands dirty and work issues, even as the director.

I want to see the partnership with industry approach to the NISP continue. Don't revert back to a compliance-only mentality. I would also encourage him or her to be patient with the government and the bureaucracy. You have to stay focused and not let the slowness or the inertia of the bureaucracy take you off course.

And finally, I would remind them that the people of DSS are the most precious national security resource we have. Take care of them.

What was your biggest challenge as the Director?

Simple, it was making the case for more security manpower resources. We have one saying in the intelligence world, 'it's hard to prove a negative' and another one that says, 'there are only operational successes and intelligence failures.'

No one will ever attribute the fact that nothing bad happened today to having a great security program. It's only when something goes wrong that all of a sudden, security is broken. So there's this institutional thinking that security will never be seen as a preventive measure and you only invest it in when it fails. The challenge is in convincing the government to invest up front.

What do you see in the future for DSS?

I see a much more capable agency empowered to serve this nation as it is capable of doing and was meant to do. The security environment is constantly changing and I believe that will force change across the Department and at DSS. I see an agency with both the 'capacity' and 'capability' to do the mission. Today, we have the capability — the knowledge, the expertise. But we don't have the capacity to do everything that is being asked of us.

I also see DSS as a major player on the national security scene. I think we are in many ways today, but I also think there are many senior leaders who have not yet realized the value of DSS to national security. I think the changes in the security and threat environment may force them to see that value.

LEFT PAGE: Stan Sims, DSS director, speaks at the 2015 DoD Security Conference in September 2015.

RIGHT; CLOCKWISE FROM TOP: Sims enjoys the 2013 DSS Holiday Party with Becky Allen, former DSS chief of staff, (center), and Barry Sterling, director of Business Enterprise, in December 2013.

Sims greets members of the Montford Point Marines, who were guest speakers at the 2015 Black History Month celebration in February 2015.

Sims, then director of Security for the Department of Defense in the Office of the Under Secretary of Defense for Intelligence (OUSD(I)), discusses the conference schedule with Kathleen Roth, formerly of the Center for Development of Security Excellence, at the 2010 DoD Security Conference, August 2010.

What message would you like to leave for our industry partners? Agency employees?

To our industry partners, I would ask them not to give up on the government, we'll get there. I know it's a frustration for industry, which can move so quickly, to wait for the bureaucracy to respond. The government does not operate at the speed of business, but we will get there eventually and we will enable the success of the industrial base, not hinder it.

I also want to thank our industry partners for their commitment to national security and willingness to partner with DSS. I would encourage industry to continue that partnership because it truly does make a difference. Build security into your programs; it's cheaper in the long run, and it's the right thing to do for our men and women in uniform and for our national security.

To the men and women of DSS: You matter. What you do matters even if no one else in the Department or anywhere else realizes it. And because of that, you cannot give up. No one else does what you do, so you have to.

Thank you to each and every one of you for your support, commitment, patience and loyalty to the American people. And thank you for supporting me as your Director!

2015 DSC

Technology expands

by Adriene Brown
Center for Development of Security Excellence

Through the use of technology, more than 1,000 people participated in the 2015 DoD Security Conference, held Sept. 16-18, 2015, in Orlando, Fla.

Close to 300 DoD personnel were in attendance at the conference, which was hosted by the Defense Security Service, and over 700 personnel participated virtually from across the federal government, logging in from as far away as South Korea, Japan, and Rwanda.

"Combating National Security Challenges" was the theme of the three-day conference that was composed of 51 general and breakout sessions, and 43 speakers. The purpose of the conference was to provide an understanding of policy changes and initiatives taking place across the Department, and the sessions supported the theme by focusing on security concerns facing DoD today.

During his opening remarks, DSS Director Stan Sims noted that "the sessions are designed to leverage the collective experience of participants to better equip them to protect national security information, people, operations and resources," he said. "Our goal is to emphasize the DoD security's commitment to share the knowledge and tools needed to adapt to a constantly changing security landscape."

The general and breakout sessions covered a variety of security topics focusing on emerging security challenges and policy updates for each security discipline area. Specific session topics included:

- Updates and initiatives of interest from the Security Policy and Oversight Division
- DoD Insider Threat Management and Analysis Center
- Monitoring and Mitigating Insider Threat to Information Technology Systems
- Systems used by Security Professionals – JPAS, CATS, DISS
- Controlled Unclassified Information
- SPēD Certification Maintenance; and CDSE Advanced and Graduate Education

important message of
2015 DoD Security Conference

The keynote speaker, Daniel Payne, deputy director of the National Counterintelligence and Security Center, wrapped up the conference by inspiring and encouraging security professionals to continue to take up the charge of combating national security challenges.

The 2015 conference introduced two new features: Live streaming and a mobile application. For the first time in the history of the DoD Security Conference, sessions were live streamed simultaneously with the in-person event. Sixty-five percent of the sessions were broadcast, with 720 people online at peak participation.

This effort made it possible for more personnel to participate in the conference, including being able to ask questions during the presentations, without incurring any TDY costs.

In addition to the virtual sessions, a conference mobile application was developed, and close to 300 people downloaded the application to their mobile devices.

This app supplied the most up-to-date conference information and allowed participants to create their own schedules, take notes, download conference presentations, and send messages to other conference attendees.

Attendees assessed the conference and virtual sessions using electronic evaluation instruments offered onsite, through the mobile app, and through email after the event.

WHAT ATTENDEES SAID

"... my hat's off to you and team for the superlative work in pulling off the Security Conference. Absolutely top-drawer work!"

"... the conference was phenomenal."

"... for my part, the 2015 Security Conference was absolutely superb from beginning to end; the DSS CDSE team really outdid themselves. Congratulations."

"Virtually attending the 2015 Security Conference made it possible to gain valuable security information and training without expending our limited funds. Therefore a multitude of security professionals gained valuable insight into security happenings and program updates from our local work areas DoD-wide. Thank you for all your efforts and ingenuity in bringing the 2015 conference to everyone."

FROM TOP: Natalie Perkins (left), Center for Development of Security Excellence, shows a conference attendee the various courses listed on the CDSE website. | An attendee of the 2015 DoD Security Conference listens to a presentation. | DSS employee Mike Buckley explains the mission of the DSS Counterintelligence Directorate.


NETWORK SEARCH
WORLD

Establishing the DoD Insider Threat Management & Analysis Center

by Matt Guy
DoD Insider Threat Management & Analysis Center

In December 2014, DSS received a new mission — establishment of the DoD Insider Threat Management and Analysis Center (DITMAC) and development of its concept of operations. On Oct. 1, 2015, the DITMAC achieved a major milestone — provisional initial operational capability.

The mission of the DITMAC is to enable information sharing, collaboration, analysis, and risk mitigation across the DoD components to address the current and emerging threats trusted insiders pose to DoD personnel, assets and information.

The mission of the DITMAC is to enable information sharing, collaboration, analysis, and risk mitigation **across the DoD components**

The DITMAC fills a critical role within DoD by working with 43 DoD component insider threat programs to promote best practices, drive innovation, promulgate a fundamental set of standards and benchmarks, provide resource and policy advocacy to senior decision makers, and through an enterprise-level analytic function, close seams between components that may be exploited by insiders.

Following the Washington Navy Yard shooting on Sept. 16, 2013, the Secretary of Defense directed an internal review team to identify and recommend actions to address gaps and deficiencies in DoD programs, policies, and procedures related to the shooting.

One of the recommendations outlined was to establish a DITMAC to provide a centralized capability that could quickly analyze the results of automated records checks and reports of behaviors of concern, and recommend action as appropriate.

On Dec. 12, 2014, the Under Secretary of Defense for Intelligence (USD(I)) assigned responsibility for establishing the DITMAC to DSS. DSS Director Stan Sims subsequently assigned DITMAC establishment to the Counterintelligence Directorate.

To combat the increasingly complex insider threat, DITMAC will take advantage of the proliferation of data and significant advances in highly sophisticated analytics, and it will generate critical indications and warnings that will augment the individual capabilities of DoD component insider threat programs.

By exploring methods to analyze complex datasets from across the Department, the federal government, and publicly available commercial sources, and conducting trend analysis on insider threat risk data, the DITMAC will recommend methods for tracking, evaluating, and mitigating these risks. It will do so by using existing technologies, pioneering new analytic techniques and integrating innovative technologies.

Upon achievement of full operational capability (FOC), which is defined as the ability to fully execute all of the tasks assigned by the USD(I), the DITMAC will serve as the centralized hub for enterprise-level analysis of insider threats. Upon achieving FOC, DoD will have to determine if the mission stays with DSS or is transferred to another component.

Standing up the DITMAC was no small task and initially fell to just three DSS employees, who were supported by an internal working group made up of participants from agency support elements.

In less than one year's time, this team has:

- located and secured a lease on suitable office space
- developed position descriptions
- initiated hiring actions
- executed $48 million in funding
- developed and submitted a Program Objective Recommendation request for FY 17–21
- executed numerous contracting actions
- developed an IT infrastructure to support operations up to the Top Secret/Sensitive Compartmented Information level
- provided dozens of briefings across DoD, the Intelligence Community, and to multiple Congressional committees

While internal establishment activities continue to take place, the DITMAC team is also responsible for managing numerous external responsibilities, to include development of the DITMAC System of Systems, a concept of operations and standard operating procedures, drafting and publishing a System of Records Notice, identifying liaison officers, and managing four enterprise-wide working groups with more than 200 representatives.

GUS GREENE was selected as director, Industrial Security Field Operations (IO), in March 2015. He is a member of the Defense Intelligence Senior Executive Service, and a retired United States Army officer with over 37 years combined service as an intelligence professional.

Before joining DSS, Greene served as the Chief of Staff for the Director for Defense Intelligence (Intelligence & Security) within the Office of the Under Secretary of Defense for Intelligence (OUSD(I)). From September 2007 to July 2013, he served in several positions within OUSD(I), to include senior advisor to Warfighter Support Directorate; deputy director, Warfighter Support Directorate; director of Sensitive Activities Directorate; and assistant to the Deputy Under Secretary of Defense for Intelligence and Security.

His responsibilities included coordination and approval of DoD sensitive clandestine activities; managing quarterly reporting and presenting briefings of DoD clandestine activities to Congress and National Security staff; developing and promulgating policy for the Defense Cover Program, Defense HUMINT and Sensitive Special Operations Programs; overseeing DoD Cover and HUMINT resources; managing and overseeing selected special access programs, the Defense Sensitive Support Program, and National Program Offices; and representing the USD(I) in the development of related National Intelligence Policy.

A retired U.S. Army colonel with 27 years of distinguished uniformed military service, Greene also served in a variety of intelligence, operations, command, and staff positions from the tactical to the strategic levels including commanding a United States Army Intelligence and Security Command Brigade.

ASK THE LEADERSHIP

A Q&A with **Gus Greene**,

Director, Industrial Security Field Operations

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

Tell us about your background. What led you to this position?

I am an Army military intelligence officer who has served in a number of leadership positions, from the small platoon up to the brigade level. Probably more relevant to my current position is that I served as the senior intelligence officer or SIO several times and at multiple levels — which in military lingo is an S2 or G2 staff officer.

In each of these positions I was responsible for managing and overseeing the organization's physical, personnel, information, operations, and signals security programs, as well as the counterintelligence and force protection programs. The interesting thing I have found is that requirements and standards found in the NISPOM [National Industrial Security Program Operating Manual] are the same as those we had to conform to in the Army regulations.

My last 10 years were some of the most challenging and rewarding as I served in a series of sensitive positions on the staff of the Under Secretary of Defense for Intelligence. These positions served to broaden my experience and knowledge of the inter-agency, Congress and National Intelligence Community. Most importantly, they heightened my sensitivity to the significant security challenges that our nation faces ... especially as it relates to the Defense Industrial Base.

I also have a computer science background, which I leveraged throughout my time in the Army and served me well while at the Under Secretary of Defense where I was involved in the development and accreditation of a sensitive special access information system.

In my last assignment, as the Chief of Staff for the Director for Defense Intelligence (DDI) (Intelligence and Security), I had the opportunity to view first-hand the significant challenges and accomplishments of the Defense Security Service, and the efforts to partner with industry to better protect our classified information and technologies that are so vital to national security.

I also had the opportunity to represent the DDI at a DSS event last year where I saw a close knit group of professionals that had great pride in what they did. The camaraderie reminded me of my time in a brigade command. As a result, when this position was announced, I saw a wonderful opportunity to be a part of that team, in a challenging and rewarding position, where I might be able to bring some measure of value by applying my knowledge of the Intelligence Community, inter-agency, technology, and security to help solve the complex and challenging issues we face today.

Since arriving at DSS, you've spent quite a bit of time traveling to the various DSS field locations. What was your goal with these visits and what have you learned?

First of all, when I arrived, I was immediately asked by the Field Operations leaders and team about the changes I intended to make within the organization. I made it clear up front I didn't want to come in and make a lot of changes independently. Rather, I wanted to hear from those responsible for executing the mission first, then validate my findings with the IO leadership team and collaboratively build our way ahead together.

As I visited the field, I wanted to meet individually with every person present for duty and learn about them personally. I wanted to see what their work environment looked like, see what they do, how they do it, and the challenges they face in getting it done. There is a great TED talk by Simon Sinek entitled "Start with Why." One of my overall goals was to assess whether our people understood the "why", since understanding the "why" defines what we do and empowers the team to execute how we go about doing it.

I learned that we have a superb group of professionals who come from a wide range of backgrounds and demographics that are dedicated to the DSS mission. For the most part, our workforce knows and has embraced the DSS "why" and it defines what we do and how we do it. They are working hard every day to partner with industry to facilitate industry efforts in protecting the classified information and technology vital to national security. A number of issues have also been captured, discussed with the leadership team, and incorporated into the IO Strategic Plan, which will set the direction for fiscal year 2016.

Knowing in advance the scope and volume of work at DSS, I thought I would have to pull out all the stops to motivate people to work harder. Quite the contrary! I learned that our team is working amazingly hard. Frankly, there are too many things for our folks to do if we try to do it all. So we are putting a lot of time into thinking about how we can prioritize our work on the highest risk issues while ensuring a work life balance. That's why we will focus on implementing the risk based analysis and mitigation process in the coming year.

What do you see as the biggest challenge facing Field Operations?

The easy answer would be to say resources. But, every organization in the federal government today can say that they don't have enough manpower and dollars in this budget-constrained environment that we find ourselves in. I think the real challenge we face is how to use the resources we have in a more effective and efficient way. We need to change the way we do business and focus our efforts on the highest risks to the loss or compromise of classified information and technology.

Underlying this is effectively evaluating the risk and then ensuring that our efforts are focused on mitigating or "buying down" that risk. Right now, we have more questions than answers. Questions such as, "What risks are we trying to mitigate?"; "How should we be measuring risks?"; "What are the biggest factors contributing to those risks?"; "What can we be doing better to reduce those risks?"; and "How do we more effectively use our resources to reduce risks?"

One of the areas where I think we have a lot of work to do is in our information systems security side of the house. As I told our information systems security professionals, or ISSPs, we are still essentially using a carbon-based life-form to overlook another carbon-based life form to assess a speed-of-light silicon-based system that is so complex, it almost defies understanding.

We need more and better automated tools to assist us in this area, which is why it is one of our highest priorities for fiscal year 2016. Moving to more of a risk-based analysis and mitigation approach is also one of our top five priorities for this fiscal year.

What do you see as the greatest strength of Field Operations? And conversely, what most concerns you about Field Operations?

I will talk about my concerns first because I want to end on a positive note by talking about our greatest strength. Regarding my concerns, it is really about the things that we have already talked about. The threats to our cleared contracting community are unrelenting. To meet this challenge, the Department of Defense is taking steps to update policy and put new practices in place.

For example, we have several major policy efforts underway such as the NISPOM update, Conforming Change 2 for the insider threat, and the transition to a Risk Management Framework or RMF. Each of these policy changes will impact our field operations. Internally, we are working with our industry partners to pivot to more of a risk-based analysis and mitigation approach in everything we do.

These changes are happening right now and in the near-term; and they will fundamentally alter the way we do business over time. I get concerned that folks will get overloaded, frustrated or overcome by the uncertainty of the future. The good news is that those that I have spoken to so far have embraced the need for change. They see it as an opportunity to get better at what we do and provide even more value to our nation's defense.

And, that will bring me to our greatest strength. I have said it before, but I will reiterate here — I think our greatest strength is our people. We hear every day about some great service or effort that one of our folks in the field or here at headquarters is doing. Part of that great work is because of the great leadership we have in place.

I have been totally impressed with the quality of our folks and their leadership. I know that each and every one of our folks takes our mission and their piece of performing our mission very seriously, so I want to take this opportunity to say thank you to every one of them. I am very excited about the future, and I am honored to be a part of this great organization.

New director, new focus highlight annual Field Operations training

"Transforming Process to Mitigate Risk" was the theme for the annual Industrial Security Representative's Training Meeting, held by Industrial Security Field Operations (IO) in July and August at DSS headquarters in Quantico, Va.

Representatives from all four regions attended the two sets of three-day training meetings, featuring an agenda packed with updates on policies, initiatives and programs.

The training also included an agency update and overview by DSS Director Stan Sims, who shared the issues affecting DSS and his way forward for the agency in 2016. He also fielded questions from each group that ranged from his philosophy of partnering with industry to what the agency's budget and manpower look like in the new fiscal year.

NEW DIRECTOR

Gus Greene, IO director since March, provided his leadership philosophy, an introduction to the directorate, and requested feedback on the directorate's top five priorities going forward.

In an effort to introduce himself, Greene visited the various regions because, "you don't get an appreciation for what people do until you get out and see them," he said. "I spoke to many of you and learned a great deal."

Mr. Greene also shared his focus on asking "why" DSS and IO exist as a way of understanding how IO does things and what the organization produces.

Greene noted that he's reached out to industry partners, and "had some interesting discussions about their challenges and concerns."

NEW FOCUS

Greene outlined the proposed top five priorities for the directorate and field for 2016, noting that all were tied to goals outlined within the DSS Strategic Plan. These goals — workforce planning, policy implementation, mission automation, risk-based approach, and collaboration — are intended to change how IO identifies risk and then manages that risk, explained Greene.

When talking about incorporating a risk-based approach to current IO procedures, Greene said a checklist approach wasn't the most efficient method to determine risk. "We need to understand the threat and vulnerability of each facility for the agency to be better at assessing risk," he said.

> "You don't get an appreciation for what people do until you get out and see them," [**Gus Greene**] said. "I spoke to many of you and learned a great deal."

"Our risk-based process is very nascent, and we need to get the process started. While doing so, we need to better understand how the outcome of the new process will change the way you do business in the field. And that's where I need your input."

The three day agenda included a number of updates and new initiatives that will have a direct impact on field operations. Perhaps the most significant were the current state of the security vulnerability assessment (SVA) and the direction SVAs will transition to in the near future and the Triage Outreach Program and how the field would continue to implement it.

Other presentations included facility security officer effectiveness, peer review of SVAs, adjudicating security violations, training and certification for Arms Ammunition and Explosives, data quality initiatives and the DoD Insider Threat Management Analysis Center.

PHOTO BOX

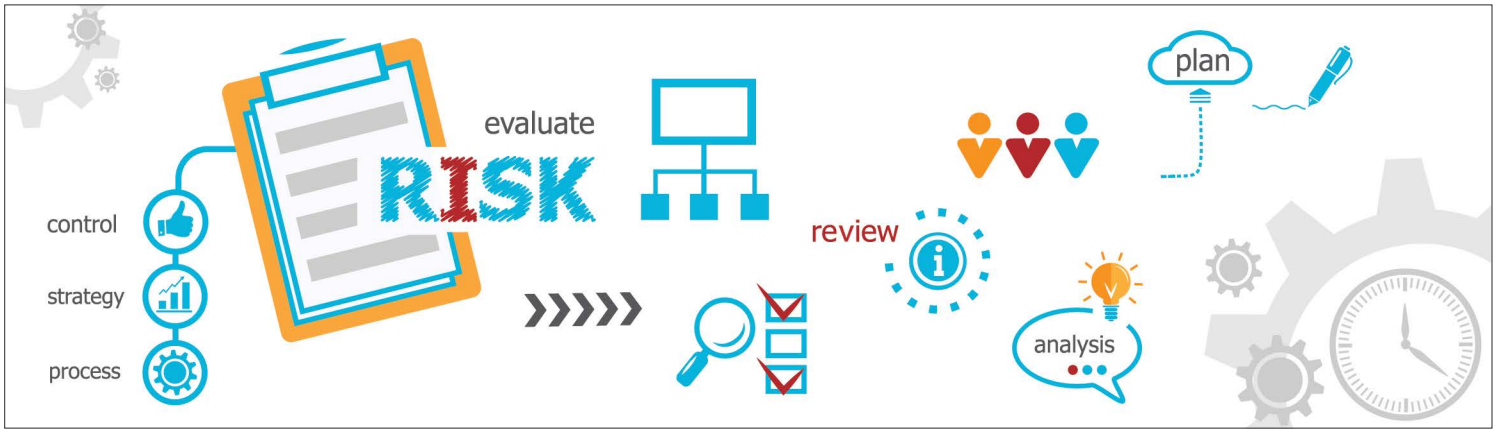
FAR LEFT: Chuck Tench, Personnel Security Management Office for Industry, provides an update on PSMO-I initiatives at the annual Industrial Security Representative training meeting in July and August.

TOP: Gus Greene, director of Industrial Security Field Operations since March, explains his leadership philosophy at the three-day training event.

MIDDLE & BOTTOM: Industrial security representatives listen to presentations at the annual training meeting in August 2015. Representatives from all four regions attended the two sets of three-day training meetings, featuring an agenda packed with updates on policies, initiatives and programs.

" TRANSFORMING PROCESS TO MITIGATE RISK "

Two sets of three-day training meetings featured an agenda packed with updates on **policies**, **initiatives** and **programs**.



Applying risk management principles in the National Industrial Security Program

by Tim Barnes
San Diego Field Office Chief

In line with the DSS Strategic Plan goal of strengthening capabilities to mitigate risk to the national industrial base, the San Diego Field Office is working hard to create efficiencies that facilitate better prioritization and make a positive impact on the National Industrial Security Program.

At the beginning of this fiscal year, the San Diego Field Office developed a Risk Management Model that would take into account threat, vulnerabilities, and defense industry assets. The criteria related to items that were synonymous with the area; for instance, San Diego-area companies work extensively on unmanned aerial vehicles and maritime-related technology, thus much of the criteria relate to those technology assets.

The entire office — industrial security representatives, information systems security professionals, counterintelligence special agents, and field office chief — collaborated to create these Risk Management Criteria. With the aim of developing the criteria and managing risk, the field office used a Venn diagram, depicting three spheres: Asset, Threat, and Vulnerability.

It should be noted that the vulnerabilities listed weren't always typical NISPOM-referenced vulnerabilities, and those items sharing spheres potentially indicate a higher degree of risk. In addition, the field office looked at unique threats to the companies and technologies in their local area, and countries 1 through 4 are the most active collectors in San Diego.

Once the risk model was developed, the San Diego team developed a scoring process (using one point per criterion) and used the equation **"Risk = Asset + Threat + Vulnerabilities"** to determine the overall risk score. Those facilities with the highest total risk score became the new priority for the office. Eventually, this risk methodology was used to drive operations/actions, and therefore prioritization in San Diego.

Nine facilities that were previously identified as a priority 3 or 4 or who were not overdue for a security vulnerability assessment now became a top priority. The nine assessments were conducted, and the results were a bit surprising.

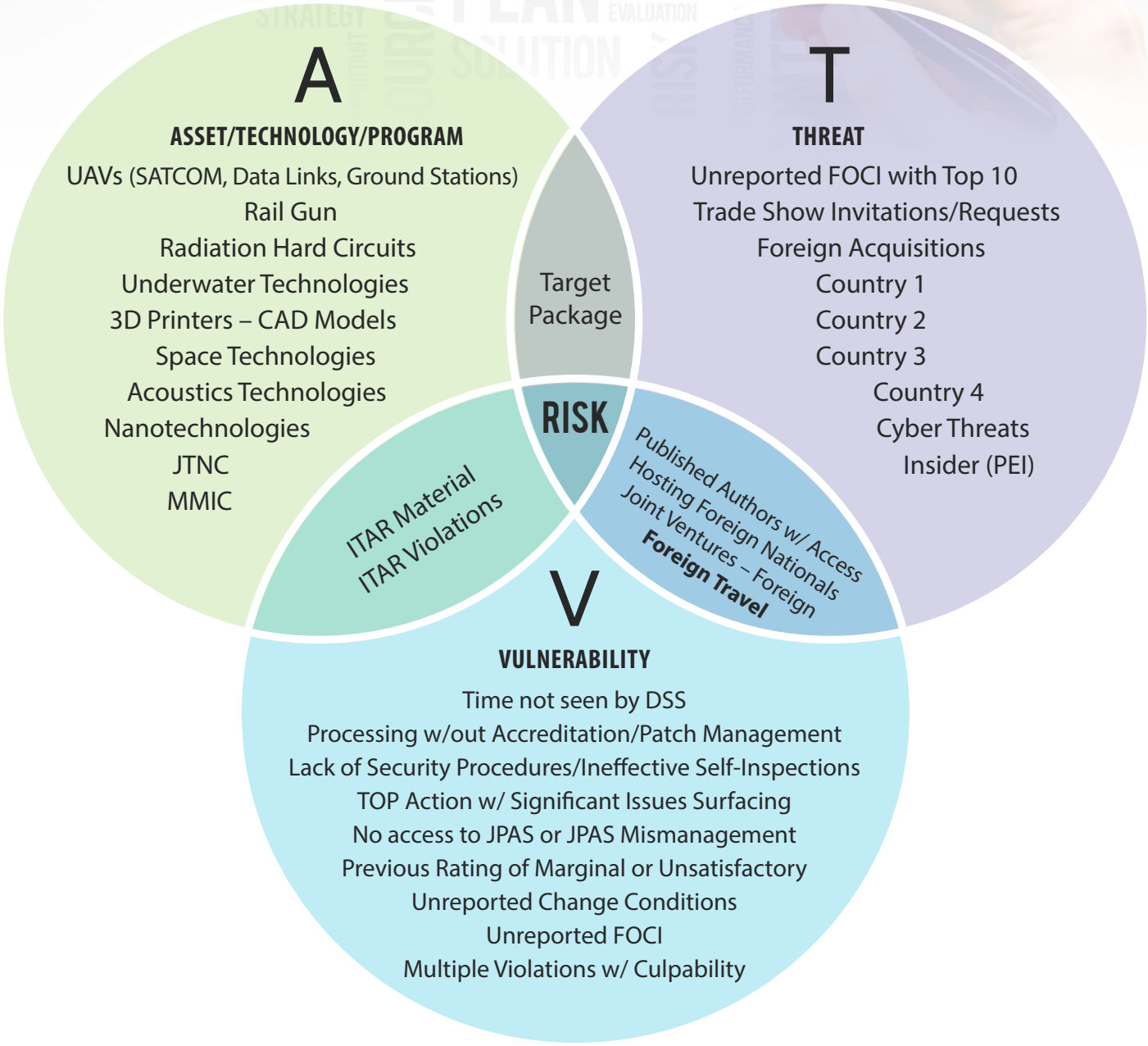
The San Diego team identified five substandard security programs, numerous critical vulnerabilities, security violations, adverse information, and suspicious contacts, all of which would have been unidentified for some time due to previous prioritization procedures. Eight of the nine assessments contributed to these findings.

More alarming in this process was the identification of poor security programs that often ran parallel with the threat or vice versa.

LESSONS LEARNED:

- Although the San Diego team believes the risk-based methodology is sound, it is imperative that the criterion developed are not standardized. In order to effectively manage risk, every location/team will have unique assets, threat, and vulnerability trends.
- The risk-based approach drove field office operations to be at the right facility at the right time based on the operational impact these actions had for DSS.
- Criteria for local risk models should be developed by a multi-disciplined team for not only a shared prioritization but also for adding valuable insights that could be missed by only one discipline.
- Although this process was initially developed to manage risk for prioritizing security vulnerability assessments, it can actually be used for prioritizing all actions or for all teams.
- This methodology allows a team to easily change criteria to meet the dynamic changes to vulnerabilities, threats, and assets.
- The Counterintelligence Requirements Branch was instrumental in aiding the San Diego Field Office in prioritization. They helped narrow the intelligence gaps that the field office initially experienced due to its limited knowledge of the facilities not seen for some time.
- The assessments or actions conducted based on risk were mutually beneficial to all the disciplines that make up a field office. In fact, it appears that any security team with multi-disciplined members would benefit from similar practices.

Since its creation, the risk-based approach has been influential in driving San Diego Field Office operations. By including all disciplines in the office while developing this risk-based approach the team has been able to integrate priorities and find greater efficiencies that had not been realized in the past.


A
ASSET/TECHNOLOGY/PROGRAM
UAVs (SATCOM, Data Links, Ground Stations)
Rail Gun
Radiation Hard Circuits
Underwater Technologies
3D Printers – CAD Models
Space Technologies
Acoustics Technologies
Nanotechnologies
JTNC
MMIC
T
THREAT
Unreported FOCI with Top 10
Trade Show Invitations/Requests
Foreign Acquisitions
Country 1
Country 2
Country 3
Country 4
Cyber Threats
Insider (PEI)
V
VULNERABILITY
Time not seen by DSS
Processing w/out Accreditation/Patch Management
Lack of Security Procedures/Ineffective Self-Inspections
TOP Action w/ Significant Issues Surfacing
No access to JPAS or JPAS Mismanagement
Previous Rating of Marginal or Unsatisfactory
Unreported Change Conditions
Unreported FOCI
Multiple Violations w/ Culpability
Target Package
RISK
ITAR Material
ITAR Violations
Published Authors w/ Access
Hosting Foreign Nationals
Joint Ventures – Foreign
Foreign Travel

Annual training provides insight into a rapidly

Professionals from all four DSS regions attended the 10th annual ISSP training event

by Jonathan Cofer
Industrial Security Field Operations

With the steady increase in frequency and severity of attacks on information technology, today's information assurance (IA) professional must be able to adapt quickly and leverage cutting-edge skills in the interest of national security.

To keep abreast of the latest issues in cybersecurity and further enhance collaboration, the Office of the Designated Approving Authority (ODAA) hosted the Annual Information Systems Security Professional (ISSP) training at the Russell-Knox building in Quantico, Va., in August.

The 10th annual ISSP training event was attended by over 80 information assurance professionals from all four DSS regions, as well as the Office of the Chief Information Officer and the Center for Development of Security Excellence, and featured presentations by subject matter experts covering a variety of information security topics.

ISSPs face the challenge of keeping their technical skill sets current and applicable, while maintaining the agility to respond to new and emerging threats to information systems in contractor facilities. The annual training meeting provides them a forum to receive guidance and insight into the changing needs of industry from the perspective of senior leadership, as well as to learn collectively from their peers' unique experiences in the field.

Dr. Allan Paller, founder and research director at the SANS Institute, a worldwide cybersecurity training organization, delivered a presentation outlining risk management and risk reduction strategies across the Department of Defense.

> ISSPs are "among the most highly qualified and experienced IA personnel [I have] encountered within DoD,"
> – **Dr. Allan Paller**, founder, SANS Institute

He provided specific examples of the need for collaboration between and within agencies to help thwart adversaries and praised the ISSPs collectively stating they are "among the most highly qualified and experienced IA personnel he has encountered within DoD," who are well-equipped to handle the changing information security threat landscape.

SANS Principal Instructor Dr. James Tarala provided an in-depth presentation of the 20 critical security controls, whose implementation is necessary to reduce the attack surface of information systems processing classified data.

Additional presenters represented key partners and stakeholders such as the Defense Information Systems Agency and Army Research Laboratory. These experts provided updates regarding collaborative programs with DSS such as the Command Cyber Readiness Inspection program and emerging technologies like the move to cloud service providers.

DSS Director Stan Sims and Industrial Security Field Operations (IO) Director Gus Greene both highlighted the strategic objectives and operational challenges facing the agency. Greene outlined his vision for IO and how attendees would contribute to the mission.

Karl Hellmann, the new ODAA assistant deputy director, outlined major initiatives within the division that align with the DSS Strategic Plan 2020, as well as the government transition toward the Risk Management Framework.

Hellmann outlined how these initiatives would affect ISSPs and the facilities and stakeholders whom they support. He further detailed the need to move away from a pure compliance stance to one that targets the higher-risk systems most susceptible to exploitation by our adversaries.

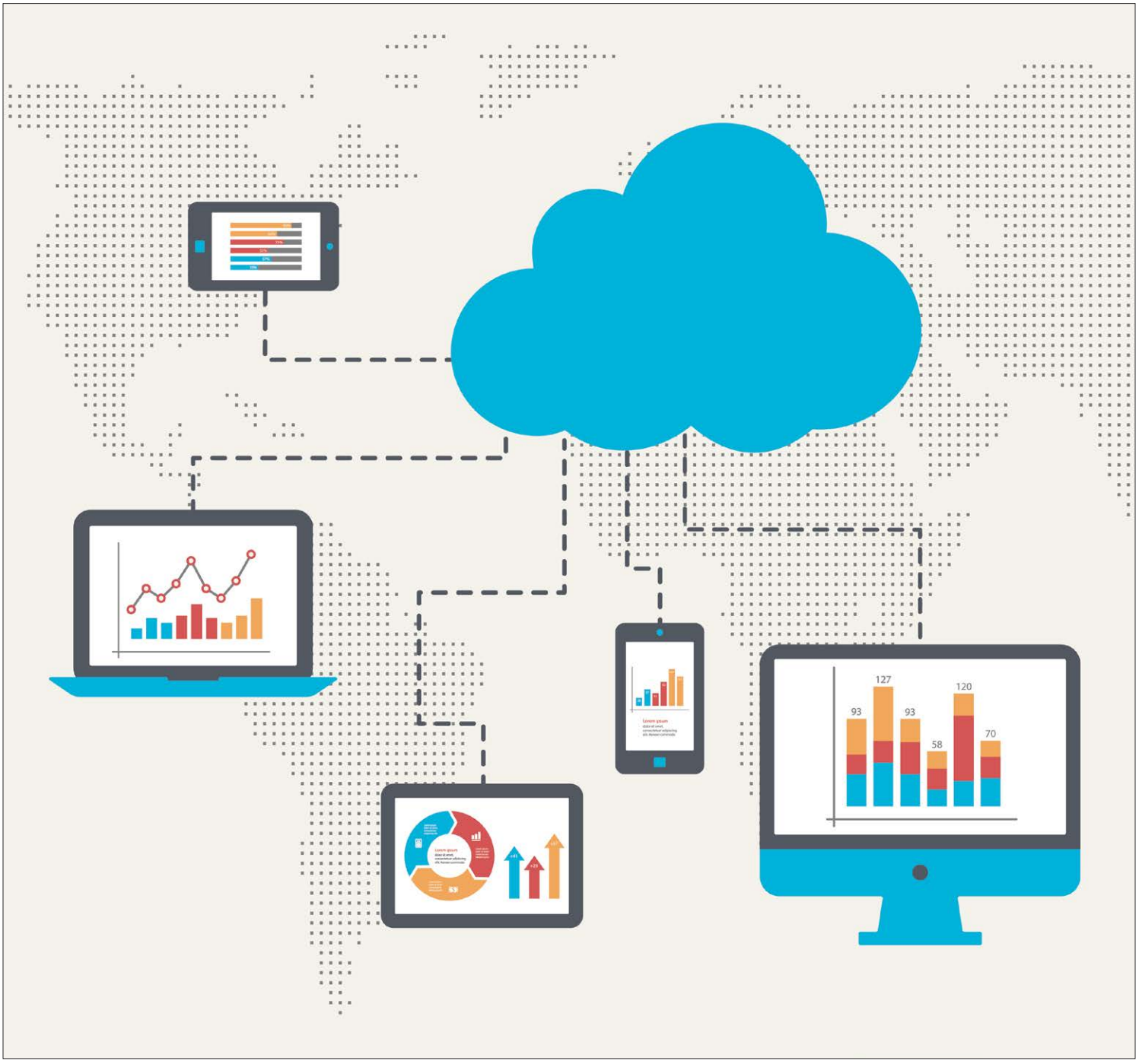
The annual training meeting also included knowledge-sharing sessions, which exposed participants to various techniques and technologies, such as quality assurance, mobile device security, cloud security and the introduction of the cloud-based Virtual Development Environment and Toolkit.

The four Regional Designated Approving Authorities conducted break-out sessions aimed at addressing issues specific to their geographic region and teams in order to enhance communication and collaboration at the regional level.

The national security threat picture evolves quickly, and a highly trained and well-equipped cybersecurity workforce is a must. Changes in technology such as cloud computing, mobility, applications and software as a service, and unconventional threat vectors as well as highly-skilled and tenacious adversaries require an IA force with the training and experience to respond and defend.

The annual ISSP training event provides an environment to enhance the skills and capabilities of our information security professionals, further preparing them to face threats.

changing information technology environment



Changes in technology such as cloud computing, mobility, applications and software as a service, and unconventional threat vectors ... **require an IA force with the training and experience** to respond and defend.

NEW & IMPROVED

Automating the DD Form 254 process through development of the NISP Contract Classification System

by Lisa Gearhart and Booker Bland
Industrial Policy and Programs

The Federal Acquisition Regulation Section 4.404, Contracting Officer's Responsibility and clause 52.204-2, Security requirements, requires that classification guidance be provided when contract performance requires access to classified information. This guidance is provided on the Department of Defense Form 254, Contract Security Classification Specification.

The DD Form 254 provides a cleared contractor, or subcontractor, with the security requirements, classification guidance and relevant security provisions required to perform on the classified contract.

Until recently, this process was managed by fillable, electronic versions of the form, and forms were emailed, faxed, or sent through the postal service to cleared contractors, other government activities, and the Defense Security Service.

The process did not provide for a centralized repository of information, allow for the inclusion of business rules, or provide for the use of other data sources in the completion of the DD Form 254. The National Industrial Security Program Contracts Classification System (NCCS) will change that.

The initial operational capability of NCCS began on June 8, 2015, and established a centralized repository for the collection of classified contract security requirements and supporting data, and also provided a venue to automate the DD Form 254 process, workflow, and delivery.

The goal of NCCS is to establish an enterprise Federal information system application that supports DoD and other Federal Agencies in the NISP by facilitating the processing and distribution of contract security classification specifications for contracts requiring access to classified information.

DSS, in partnership with the Office of Defense Procurement and Acquisition Policy within the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, expedited the deployment of NCCS as an application within the existing Wide Area Workflow (WAWF) E-Business Suite. WAWF is a secure, web-based system for electronic processing of procurement and contractual documents.

Development of the NCCS started in June 2014, with the expectation of additional system functionality to be released in November 2015. Incremental modular releases are planned for every six-to-10 months to allow for additional functionality.

DSS developed the application's business functionality requirements based on input from DoD, other Federal agencies and industry, and it will be responsible for developing future NCCS requirements. The NCCS application can be accessed on the DSS external website: www.dss.mil.

BIG WINNERS: The Western Region CI Team receives the NCSC Director's Award of Excellence. Shown from left are Director of National Intelligence James Clapper, Western Region CI Chief Tom Montero, Western Region Deputy CI Chief Jeff Boick, and Director of the National Counterintelligence and Security Center William Evanina.

DSS recognized at the 2015 National Counterintelligence & Security Awards

The DSS received recognition in three categories of the 2015 National Counterintelligence (CI) and Security Awards at an August ceremony hosted by the Director of the National Counterintelligence and Security Center (NCSC). The NCSC recognizes CI and security practitioners for exceptional performance in 19 categories.

Jonathan Laahs, CI special agent in the Phoenix Field Office, received the individual award for industrial security. The Western Region CI Team received the NCSC Director's Award of Excellence. Frank Carapezza, CI Headquarters intelligence analyst, and Brian Medley, DSS liaison to FBI Headquarters, were recognized as part of the Defense Intelligence Agency's Dormant Wraith Task Force, which also received the Director's Award of Excellence.

Laahs was recognized for his "unswerving dedication to the Defense Security Service counterintelligence mission." His exceptional performance "demonstrated excellence by identifying 522 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 operations on 52 identified subjects or operational sources in the National Industrial Base." The Western Region CI Team, one of three special recipients of the NCSC Director's Award of Excellence, were recognized for "exemplary counterintelligence support to the National Industrial Base, federal law enforcement, and the Intelligence Community." In 2014, the Western Region identified 242 investigative subjects and operational sources and disseminated 1,162 intelligence information reports. Region CI Chief Tom Montero and Deputy CI Chief Jeff Boick represented the team at the ceremony.

Medley and Carapezza were involved in the disruption of illegal foreign acquisition of Department of Defense sensitive technologies as part of the Dormant Wraith Task Force. The task force provided evidence leading to the arrest of a foreign hacker, initiated several counterintelligence investigations, and caused extreme financial distress to at least one key foreign intelligence entity front company.

The award ceremony was attended by over 200 people, to include the Director of National Intelligence James Clapper, who gave the keynote address. He praised the awardees for their exceptional work and also recognized their family and friends for their support.

Clapper acknowledged counterintelligence and security successes go unnoticed because of necessary secrecy of the discipline, but the award presentation provided a unique opportunity for family members to get a glimpse into the dedicated work of their awardee.


IDGH
EJ+EO
EFF
-WEF

CASE STUDY

Successful mitigation of FOCI involves entire agency

by Will Cooper
Industrial Policy and Programs

DSS is charged with mitigating foreign ownership, control or influence (FOCI) in companies performing on classified contracts under the National Industrial Security Program. This is done through FOCI mitigation agreements implemented and overseen by the FOCI Operations Division (FOD).

A recent case, however, illustrates that FOCI mitigation requires the effort and talents of multiple DSS stakeholders, working together to safeguard classified information and protect the warfighter.

A U.S. company, Alpha, was sponsored for a facility clearance (FCL) to perform on classified contracts. DSS determined that Alpha was owned by Charlie Corporation, a foreign company based overseas. DSS also learned that Charlie had purchased Alpha with money loaned by a financial institution located in the same foreign country as Charlie, Bravo Bank, using Alpha as collateral to secure the loan.

Alpha = U.S. Company

Bravo = Foreign Bank

Charlie = Foreign Owner

Based on this information, the FOD implemented a Special Security Agreement (SSA) with Alpha to mitigate the FOCI resulting from Charlie's ownership and the indebtedness to Bravo. A requirement of the SSA was that Alpha nominate new directors to its board who had no prior affiliation with Alpha and who were eligible for a personnel security clearance. The FOD approved two such "outside directors", and the company received its FCL.

A short time later, Alpha notified its industrial security representative (ISR) that Charlie had defaulted on its loan to Bravo and was declaring bankruptcy. Since Alpha was used as collateral for that loan, Bravo assumed control of Alpha.

Bravo promptly fired all directors except one of the outside directors, installed several new officers, and asserted all rights of ownership of the cleared company notwithstanding the SSA. In effect, Bravo was taking steps to nullify the SSA. The FSO remained on staff but was ordered to report to Bravo personnel.

As a result of these actions, a foreign entity controlled a cleared company without recognizing any limits on its ability to access classified information, thereby compromising the security of that information and impairing the cleared company's ability to perform on its active, classified contracts.

As soon as the ISR learned of the situation, she notified her field office chief, regional senior action officer, and FOD action officer. This was the first case of its kind any of them had encountered.

The FOD action officer and ISR coordinated with the DSS Office of General Counsel, Facility Clearance Branch, and senior leadership in both the Industrial Security Field Operations and Industrial Policy and Programs directorates to devise a path forward.

This early teamwork ensured that actions were taken swiftly. Within two days, the General Counsel reached out to Bravo's attorneys to explain its obligations under the SSA and outline the legal consequences of failing to abide by it, while field and regional personnel coordinated a local response with the ISR and a counterintelligence special agent to monitor Alpha on a day-to-day basis, to ensure that classified information remained protected.

The action officer worked with the remaining outside director to update government customers and push back against inappropriate demands from the new directors and other Bravo personnel. The Facility Clearance Branch worked concurrently with senior leadership on contingency plans to terminate Alpha's FCL in the event that classified information was deemed to be at risk.

DSS personnel remained in constant contact, ensuring new developments were communicated quickly and all pertinent information was leveraged to resolve the situation. Within three days of being contacted by the ISR, Bravo rescinded all appointments of new directors and withdrew all questions respecting Alpha's operations and work, confirming that it understood the rules of the SSA and would abide by it.

Within two weeks, Alpha reconstituted its board to include the previously approved outside directors and executed resolutions excluding the affiliates from access to classified information, with Bravo acknowledging that it had been so excluded. Alpha continued to use its SSA and perform on its contracts.

Acting in concert, multiple DSS offices successfully resolved a novel case by preventing an unmitigated foreign financial institution from potentially accessing classified information or impairing a cleared company's performance on classified contracts.

DSS staff leveraged their subject matter expertise in different fields to fulfill the agency's mission, and their work with industry stakeholders, from the outside directors to outside counsel, illustrates the effectiveness of partnering with industry to solve national security problems.

FOCI is seldom easy, but when DSS personnel work closely together while leveraging industry resources, it can be mitigated effectively and completely.

Developing emerging leaders through mentoring initiatives

by Laura Szadvari
Human Capital Management Office

Recognizing the importance of employee retention within a rapidly changing and increasingly competitive work environment, DSS has spearheaded a mentoring program that aims to engage both mentors and mentees in a mutually beneficial relationship that meets the collective needs of both parties.

To start this initiative, the DSS Human Capital Management Office (HCMO) held two mentoring events that brought the workforce together to share information, trade stories, and impart career-related guidance and advice.

The first event was "speed mentoring" where senior leaders and employees had the opportunity to circulate around the room and talk, round-robin style, about career goals, concerns, and challenges. Each conversation lasted for approximately three minutes to allow mentees to meet with as many mentors as possible within the allotted time.

The unique format of the event allowed mentees to have multiple conversations on personal and professional issues while, simultaneously, providing the opportunity to network with senior leaders in the hopes of establishing future connections.

Feedback from the speed mentoring event was extremely positive. Participants liked the opportunity to openly discuss career plans and movement/changes both in government and industry. Mentees were also pleased with the variety of mentors chosen to participate. As a result of the event, at least three mentor/mentee partnerships were formed.

HCMO also sponsored a Mentoring Desserts Panel in which seven senior leaders shared their thoughts on leadership, challenge and conflict, and professional development and career advancement.

The session provided an open and honest exchange of information as leaders shared their accomplishments and their disappointments, as well as their concerns. Both panel participants and audience members found the informal dialogue refreshing.

"I enjoyed the opportunity to engage with our workforce and share thoughts and experiences about leadership," said Gus Greene, director, Industrial Security Field Operations (IO). "I also enjoyed hearing the thoughts and experiences of the other panel members. There was a good cross section of people of various backgrounds, which enriched the overall event."

> "I enjoyed the opportunity to engage with our workforce ..."
> – **Gus Greene**, director, IO

Michael Halter, IO deputy director and a panel member, not only shared his perspectives on leadership, but also used the event as an opportunity to learn from other panelists and "enjoyed being 'mentored' by other seniors."

During her introduction, La Shawn Kelley, chief, HCMO and acting DSS Chief of Staff, said, "Every leader needs a mentor or someone he or she trusts to be open, honest, and candid when it really counts."

PHOTO ARRAY

LEFT: Laura Hickman, chief, Personnel Security Management Office for Industry, discusses past career opportunities with a participant of the speed mentoring event.

MIDDLE: Julie McGovern (right), acting chief of the Human Capital Management Office, outlines her career goals during the speed mentoring event

RIGHT: Fred Gortler (right), director of Industrial Policy and Programs, provides his leadership philosophy to Franklin Caul, HCMO, at the speed mentoring event.

Feds Feed Families:

DSS brings tons to the table

by Dahlia Thomas
Office of Public and Legislative Affairs

The 2015 DSS Feds Feed Families campaign was a huge success, as DSS employees contributed 8,126 pounds of food and $775 in monetary contributions, more than doubling last year's donation of 3,360 pounds.

The goal of the 7th annual government-wide Feds Feed Families, sponsored by the U.S. Department of Agriculture, is to help food banks and pantries stay stocked during summer months, when they traditionally see a decrease in donations and an increase in need.

Launched in 2009 as a part of President Obama's United We Serve campaign, the food drive has collected nearly 39 million pounds of food since its inception. This year's event ran from July 15 to Oct. 1, 2015.

DSS offices nationwide (Headquarters, Center for Development of Security Excellence, and the Capital, Northern, Southern, and Western Regions) participated and worked locally with 27 food banks and non-profit organizations in their communities.

They gave through virtual donations (purchasing food online and having them deliver it directly to the food bank of choice), monetary donations, gleaning at local farms (crops collected from local farms that would normally go to waste), and participating in numerous office food drive promotions.

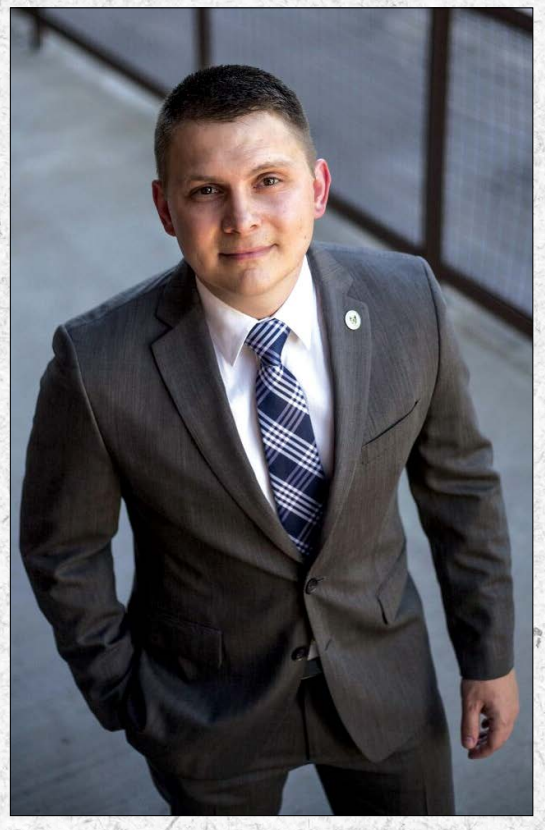
The agency's collective efforts were recognized in the DoD Hall of Fame 2015, with special recognition going to the National Capital Region offices at Mill Road, which donated 2,399 pounds (largest donation); the Charleston Resident Office, which donated 1,000 pounds (largest donation relative to number of employees); and the Western Region, with the largest monetary donation of $775.

As a key participant, the Department of Defense played a vital role in coordinating a nationwide effort, with its agencies and components donating close to 3.3 million pounds of food and goods to local food banks around the country. This includes 100,000 pounds of perishable food that was gleaned in the National Capital Region.

ABOVE: The National Capital Region offices at Mill Road donated 2,399 pounds during the Feds Feed Families program.

BELOW: The Andover Field Office participated in the campaign, donating goods to a local food bank in Massachusetts.

Counterintelligence special agent recognized by alma mater



Justin Shanken was recognized by the University of Georgia Alumni Association as one of its 2015 "40 Under 40" recipients.

by Morgan Hammonds
Deputy Chief, Counterintelligence Division, Southern Region

Justin Shanken, counterintelligence special agent (CISA) in the Atlanta Field Office, was recently recognized by the University of Georgia (UGA) Alumni Association as one of its 2015 "40 Under 40" recipients.

Each year, the UGA Alumni Association recognizes 40 exceptional alumni, under the age of 40, who are achieving great success in their professional and personal endeavors. Other winners in 2015 included a congressional chief of staff, agency and company executives and vice presidents, a news producer, a surgeon, a senior congressional policy advisor, and a professional golfer.

Shanken was nominated by a former university advisor for his work in establishing an internship between the UGA's School of Public and International Affairs and DSS. Shanken spoke at the school on multiple occasions, informing students about pursuing careers in the intelligence community, the security clearance process, his military service, and the benefits of serving in the military. Additionally, he is currently mentoring a small group of UGA students who are considering a career in intelligence after they graduate.

The alumni association recognized Shanken for his professional accomplishments, to include serving his country during a time of war, being selected as the 2014 Southern Region CISA of the Year, and for performing his current national security duties and responsibilities with DSS. In September, he and the other 39 winners were recognized at an award ceremony in downtown Atlanta.

Shanken honorably served as a CI special agent in the United States Army for over six years, was assigned in Europe and deployed to the Middle East, and received several military decorations, to include the Global War on Terrorism Expeditionary Medal for his service during Operation IRAQI FREEDOM. Shanken joined DSS in July 2009 as a CISA.

DSS hosts Women's Equality Day event

Three of DSS's four regional directors participated in a Women's Equality Day Panel Discussion at the Russell-Knox Building on Aug. 25, 2015. The event was held to commemorate the 1920 passage of the 19th Amendment to the Constitution, granting women the right to vote.

The DSS panel of senior leaders, who happened to be women, focused their remarks on their motivation in applying for their current position, their biggest challenge, how they measured success, and advice they would offer to others looking to achieve similar leadership positions.

Heather Green, Capital Region, said she was motivated to apply for the position because of her love of the mission, "I love being in the field," she said. "Loving what you do is important."

Regina Johnson, Southern Region, said her motivation was the opportunity to lead and to infuse the region with a female perspective. Cheryl Matthew, Northern Region, said the biggest challenge to her career was finding the right home-life balance.

Each of the panel members challenged the audience to step outside their comfort zones and take advantage of new opportunities. "You have to learn from every experience you have," said Green. Johnson encouraged the audience to find a mentor and "learn all you can from them."

Cruising the Chesapeake Bay

In August, DSS Counterintelligence Special Agent Craig Beck, Capital Region, participated in a Wounded Warriors of Maryland on the Chesapeake Bay event, to honor the contributions of wounded warriors and their families. Beck, who is also current Commodore of Galloway Yacht club and retired U.S. Army Chief Warrant Officer 4, along with 40 other boat owners, volunteered to provide a cruise around the Chesapeake Bay for the servicemen and women and their families.

The event included stops at the Francis Scott Key Memorial Buoy, where the Star Spangled Banner was written, past Fort McHenry and into the Baltimore harbor. Afterward, participants dined on a crab and shrimp feast. More than 175 wounded warriors and their families participated in the event which was the vision of current Commodore of North Point Yacht Club Jim Diven, who is a retired U.S. Army sergeant major.

Defense Security Service