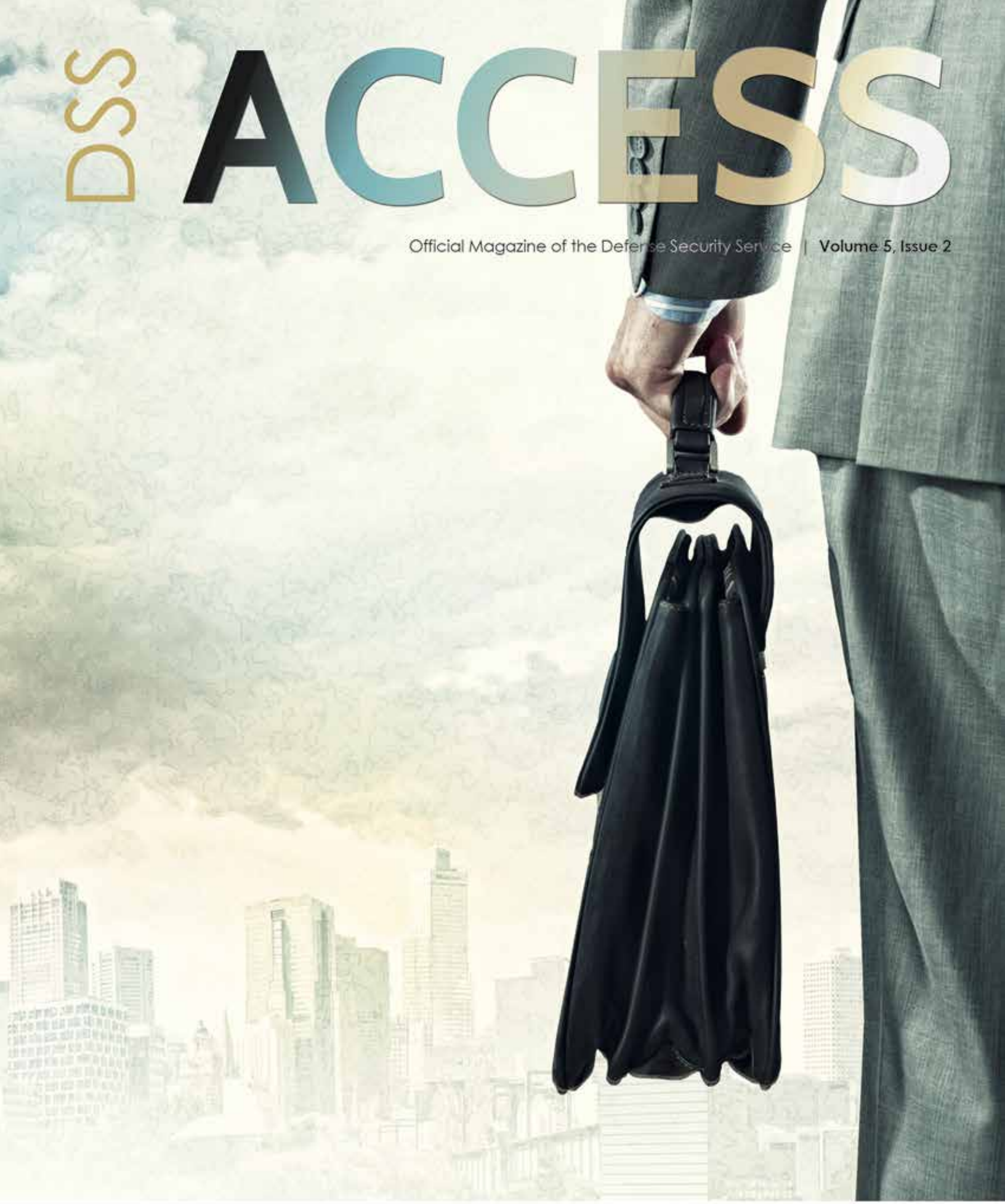
# DSS ACCESS

Official Magazine of the Defense Security Service | Volume 5, Issue 2



## DSS welcomes **new director**

**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 | Dan Payne

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 Department of Defense, or DSS.

All pictures are DoD photos, unless otherwise identified.

## COVER STORY



## INSIDE



## DIRECTOR AWARDS



## ASK THE LEADERSHIP



# From the Director

This is my first column for the DSS ACCESS, and I can't tell you how excited I am to be at DSS and contributing to this publication. I have found the ACCESS to be a great mixture of mission-oriented information and human interest stories that appeal to a wide readership. I want to continue in that same vein and am looking forward to using this venue to share my priorities and direction for DSS.

On my first day at DSS, I sent an email to the workforce introducing myself and briefly sharing my perception of the current security and counterintelligence (CI) environment. I wanted to share some of that message here.

By way of introduction, I have spent my entire career in counterintelligence and security. I believe the CI threat to the United States is more significant now than at any other point in our history. To meet these challenges, DSS must be flexible and nimble. That may require DSS to adjust the way we traditionally do business. I know change can be uncomfortable, but I believe it is necessary to thwart the new risks posed by our adversaries. Adding a risk-based methodology to our business processes is a significant step in the right direction.

I also believe we need greater integration between CI and security. The first line of defense in any good counterintelligence program is a strong security program. Security policies and activities are driven by the CI threats that we face. Being on the front line, security is also in a prime position to identify some of the CI threats and filter that information back into the intelligence cycle so that it may be factored into the assessment of the overall threat creating a feedback loop.

Now all that said, I find myself the director of a well-run organization that has had significant achievements over the past several years and possesses a very talented workforce that on a daily basis 'punches well above its weight class.' My responsibility as the leader of this high performing organization is to take what has already been created, build upon those successes, and take DSS to an even higher level.

I am very proud and honored to serve as the Director of DSS and look forward to a challenging and exciting term.

Dan Payne
Director

# DSS welcomes new director

On April 8, DSS held a swearing-in ceremony to officially welcome Dan Payne as the 13th Director of the agency. Presiding was the Honorable Marcel Lettre, Under Secretary of Defense for Intelligence. The ceremony included passing the DSS colors, a military tradition signifying the transfer of authority and functions to the incoming director.

Lettre said he wanted to officially welcome Payne to DSS and continue to celebrate the outstanding team at DSS. He also personally thanked Jim Kren, deputy director, who served as acting director on an interim basis. "His willingness to serve is a testament to his integrity and I appreciate his efforts to ensure a smooth transition to a new permanent director," Lettre said.

"DSS is clearly a unique organization," Lettre continued. "It's the smallest agency in my portfolio, but its level of responsibility is unmatched in government. Our government's faith in DSS is a testament to the passion, commitment, and expertise of all DSS employees." In Payne, Lettre said, the agency was getting a dedicated and capable leader who had earned a reputation as an innovator.

Lettre briefly highlighted Payne's career with the Central Intelligence Agency and his more than 30 years in the field of counterintelligence. Prior to joining DSS, Payne served as the Deputy Director of the National Counterintelligence and Security Center. Payne's previous senior assignments at CIA include Deputy Chief of South Asia Division; Deputy Chief, Counterintelligence Center; Assistant Inspector General for Investigations; Deputy Director, Counterterrorism Center for Counterintelligence; and Deputy Chief, Counterespionage Group.

Lettre noted Payne's efforts in forensic accounting which led to the identification, arrest, and conviction of Aldrich Ames and his spouse for espionage. Payne subsequently established a unit at the Central Intelligence Agency that specialized in this work and personally trained others in the financial forensics techniques.

In closing, Lettre said, "We have the right leader in the right position at the right time ... a time when rapid technological change is a given. Dan is a no-nonsense man from the south side of Chicago with the depth and breadth of experience needed to steer the DSS ship through our dynamic and complex national security environment. I am confident that he will surpass all expectations in this new capacity, that he will look out for this fabulous workforce and that he will ensure the continued success of the Defense Security Service."

In his remarks, Payne noted he began his federal career as a 22 year-old GS-5 with the Defense Investigative Service, the forerunner to DSS. "Never did I imagine that I would be standing at this podium today, being sworn in as the 13th Director of the Defense Security Service. So thank you Mr. Lettre for your trust and confidence."

Payne also recognized former Director Stan Sims and Deputy Jim Kren for the many very positive changes that have taken place at DSS over the past several years. "Much of the credit goes to the leadership of Mr. Sims and Mr. Kren," he said. "Credit is also due to the workforce that has embraced change in the past to reshape DSS into what it is today."

Payne then addressed how he sees the current counterintelligence environment. "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."

He also said cyber-thieves are stealing our technology and personal information at an alarming rate. The government now measures our losses of information not in terms of documents, but in terms of petabytes. (One petabyte is equivalent to 100 times all of the printed material in the Library of Congress.)

"The danger to our national security information is greater now than ever before," Payne said. "Globalization has put our national security supply chain at risk in ways we never imagined. Keeping our supply chain safe from our adversaries requires constant vigilance."

Payne said the only way we can successfully confront these challenges is by partnering on several different levels and eliminating stovepipes. He then cited his priorities for DSS and the role he expects to play as Director:

- "Counterintelligence and security must work in unison. Security policies and procedures are developed to

**THE WELCOMING; FROM LEFT:** The Marine Corps Base Color Guard moves the colors during the swearing-in ceremony for DSS Director Dan Payne. | Under Secretary of Defense for Intelligence Marcel Lettre provides opening remarks at the ceremony. | DSS Chief of Staff Troy Littles accepts the flag from DSS Director Dan Payne. *(Photos by Marc Pulliam, CDSE)*

---

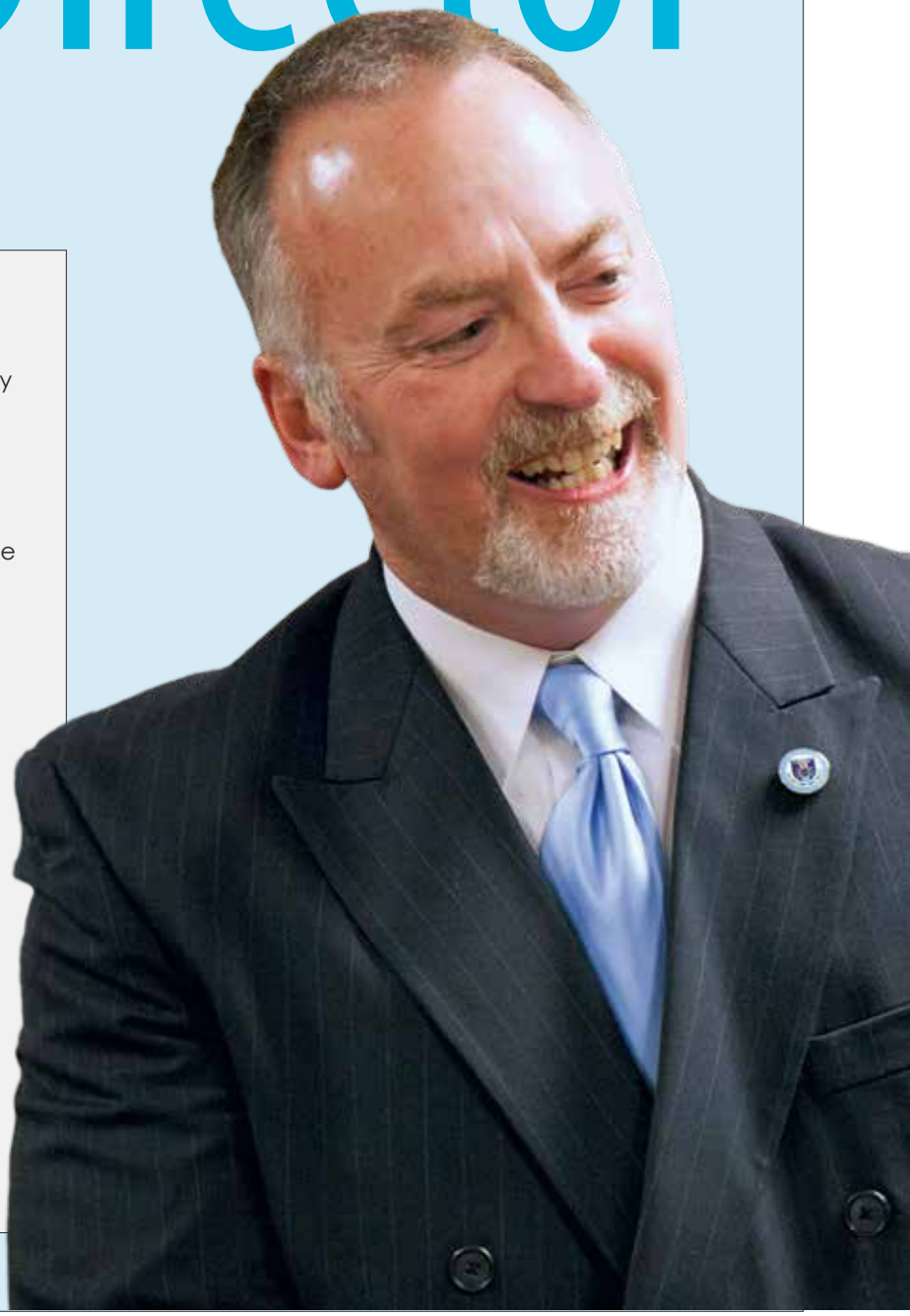
thwart the counterintelligence threat and a good security program is the first line of defense in any good counterintelligence program. The information about our adversaries that is developed in the security process must filter its way back into the intelligence cycle so that we can understand the full extent of the threat and work collectively to thwart it. As Director of DSS, I will strive for greater integration of CI and Security in protecting our national security information.

- "Second, we need better integration and collaboration at the federal level. While great strides have been made to better integrate and share information, more can be done. It will take all of us, using our individual strengths and expertise, to fully confront the counterintelligence threats we face. As Director of DSS, I will strive to forge stronger links with other agencies within the Department of Defense, the Intelligence Community, and our federal partners to protect our national security information.
- "Third, it is important that we have a collegial and collaborative working relationship with industry. The United States government doesn't build anything. Government may envision it, government may plan it, government may fund it, but everything that is produced, is produced by industry. As Director of DSS, I will build upon our existing partnership with industry to jointly combat the threats we face.
- "Lastly, America has many allies. But there are some allies that stand apart from others. For more than 100 years we have stood shoulder to shoulder in confronting the threats that face our countries. I can say confidently that we are all battling the same issues and independently we are developing many of the same solutions. But it is in the small differences where we learn from each other and where we spark innovation. I believe there is much more our countries can do together to combat the counterintelligence threats that face our national security industries. As Director of DSS I will work closely with our allies to seek out opportunities to do so."

Payne concluded his remarks with the following message to the DSS workforce, "To the talented workforce of DSS, to our industry partners whose products have kept America safe, and to all others who join us in this noble cause, I look forward to working with you to keep America safe and strong."

LOOKING AHEAD

# A Q&A with the Director



**Editor's Note:** Mr. Daniel E. Payne, a member of the Senior Intelligence Service, was appointed by the Secretary of Defense as Director of the Defense Security Service, on March 21, 2016. He is the agency's 13th director.

Mr. Payne is a career counterintelligence (CI) officer with the Central Intelligence Agency who has spent more than 30 years in the field of counterintelligence.

Prior to joining DSS, Mr. Payne served as the Deputy Director of the National Counterintelligence and Security Center.

Mr. Payne's previous senior assignments at CIA include Deputy Chief of South Asia Division; Deputy Chief, Counterintelligence Center; Assistant Inspector General for Investigations; Deputy Director, Counterterrorism Center for Counterintelligence; and Deputy Chief, Counterespionage Group.

## How did your background prepare you for this job?

I have been involved in counterintelligence for about 34 years. On a daily basis for the past 34 years I have seen how foreign intelligence services have tried to steal and have successfully stolen our secrets.

Additionally, I have worked on the other side of the coin; I have worked to steal the secrets of our adversaries. As a result, I have a thorough understanding of the threat to cleared industry, not just from a theoretical standpoint, but from a no-nonsense, here-is-how-it-is-done perspective.

When you don't have hands-on experience with espionage or intelligence collection, there is a tendency to view espionage much like a violent act you hear about on the news. It's always an event that happens somewhere else. You never think it will happen to you or happen in your backyard.

But I'm here to tell you, it happens all the time and it happens in your backyard. I know this, because I have seen it, and I have done it. Also, in my previous job, I had the opportunity to see counterintelligence and security programs throughout the U.S. Government and industry.

There are a few government agencies that have very solid CI and security programs. Most do not, and it's the same in industry. Some of the larger companies have very robust CI/security programs. Most do not.

Our country is being drained of national security information, and in many cases, proprietary information as a result. Few people can relate to the importance of the work being done by DSS and our industrial security partners like I can.

## As an outsider to DoD, you bring a different perspective of the CI and security landscape. How do you see the new risk-based approach at DSS fitting in with that perspective?

I think the risk-based approach DSS is developing is the way of the future. We are the smallest agency in the Department of Defense and have one of the most critical tasks.

We are responsible for the protection of national security information at approximately 12,500 facilities nationwide. We cannot afford to give the same level of attention to each facility. We must take a look at the technologies that are most critical to protect and also the technologies our adversaries are trying to steal. That is where we need to put the bulk of our attention.

I think the risk-based approach DSS is developing is the way of the future. **We are the smallest agency** in the Department of Defense and have **one of the most critical tasks.**

Additionally, we need to look at tailoring the manner in which we protect the information at these facilities according to the changing methods of operation of our adversaries. We have to be current, we have to be flexible, and industry has to be a partner every step of the way.

## What was your perception of DSS before you arrived and has it changed?

I remember DSS when the personnel security mission transferred to the Office of Personnel Management. At that point, it seemed like DSS was on the decline, and I think there were concerns as to whether or not it would survive. You saw that in the series of acting directors DSS had.

But I think, starting with Kathy Watson [previous director], DSS began to carve out its niche and focus in on its core mission. I think that continued under Stan Sims, and DSS really began to come into its own and develop its unique expertise. I also think DSS has greatly improved its relationship with industry.

There is one thing that has been a significant and pleasant surprise to me and that is the quality of DSS personnel and leadership. First, I want to talk about the workforce. There isn't a day that passes that I am not impressed by the quality of DSS personnel. They know their business, they're experts at it, they have great attitudes, and they are highly motivated. I am impressed every single day.

Leadership is also very strong. DSS has experienced leaders who are also highly motivated and very open to innovation. You have to be willing to innovate and

you have to be willing to change. The world and our adversaries are changing constantly. We must adapt. If we do not adapt, we will die (literally and figuratively.)

### At one point, early in your career, you were an Investigator with the Defense Investigative Service. What do you remember about that position and the agency?

The primary mission in 1982 was personnel security, and I was an investigator. Industrial security was a relatively new mission for the Defense Investigative Service. I was assigned to Edwards Air Force Base in California.

I had a great passion for investigation and frankly, I believe personnel security is a great place to start as an investigator. There is no investigative position where you can interview as many people as you can doing background investigations.

You are interviewing people all day long, day after day. You really develop your interviewing skills. You can experiment; you can try out new interviewing techniques or tactics and see if they work for you. You learn to read people and size people up very quickly. You learn to adjust your approach within just a few seconds of contact based on your assessment of their behavior. I loved the job and frankly it gave me the skills to be successful very quickly when I moved to the CIA.

Additionally, Edwards and the surrounding area was a very unique place. It did give me my first taste of the defense industry. Back then, the Space Shuttles were being built in Palmdale, Calif., as was the SR-71, and I spent a lot of time at those facilities. Although the first stealth planes were not being built at Edwards, the majority of the workforce came from there. It was a very, very interesting place.

### What are your priorities during your tenure?

Adopting the risk-based approach to everything we do is probably my top priority. I think it can be applied in many different forms at DSS, whether it's in field operations, counterintelligence or FOCI [Foreign Ownership, Control or Influence]. But I think it is where we need to go.

I also want a stronger link to the Intelligence Community

Intelligence that we collect on the activities of foreign intelligence entities who are trying to steal our secrets drives security policies that we put in place to protect our secrets. **So, CI drives security.**

(IC). The IC has a lot of information that would help inform the risks industry faces. They also have unique insights on collection. The more we can interact with them and get wired into their information sources, the better informed we will be. That is critical in assessing risk and looking at ways to mitigate it.

Additionally, DSS has a unique information resource: Industry! Nobody has the contact with industry that DSS has, and we can help inform the IC on the full threat picture. You will hear me say this a thousand times. Intelligence that we collect on the activities of foreign intelligence entities who are trying to steal our secrets drives security policies that we put in place to protect our secrets. So, CI drives security.

At the same time, information collected during the security process has to be filtered back into the intelligence cycle to help inform the threat picture. CI and security are two sides of the same coin.

I also think we can benefit by a closer working relationship with some of our foreign allies. My experience has been that we are all battling the same issues. It is comforting that most often we are all coming up with same solutions independently. But it is in those differences where we can develop some very innovative ideas.

DSS has a strong partnership with industry, but it can always be stronger. I think there's a natural tension in industry between spending money on security and making a profit. Our job is to protect national security information. So, we can listen to industry and be flexible where we can, but there will be times where we will have to stand firm.

Ultimately, the model should be that DSS sits down with the security personnel of a company and jointly develop a security plan that is unique to that particular company and facility taking into consideration the product they are producing, the manner in which they are producing it, a realistic threat picture for that particular piece of

technology, company, and facility. We have to tailor security according to the threat, the vulnerability, and the potential impact of compromise. That's my vision.

## You are here on a two-year detail. How does that inform your decision making and priorities?

I don't think it affects my decisions or priorities at all. I'm all in. That said, it's very common in the Intelligence Community to rotate every few years, particularly at the senior level. It's also the military model and one that increasingly applies to DoD civilian leaders. So I don't think this is unusual for senior positions.

## You have already started visiting field locations. What are you learning?

I'm looking at how the offices are running their programs, first and foremost. How are they doing their jobs? What are the challenges they're facing? And I'm already learning and thinking about what we can do better.

For instance, I think our field counterintelligence personnel are hampered by not having access to JWICS. This inability to get top secret information, particularly signals intelligence (SIGINT) and cyber reporting, means the field is not getting the total threat picture. And it's the people in the field who are working with industry everyday who are in the best position to determine what's useful and how to use it.

So we will work on that, and it may be that we have to partner with other government agencies to obtain access in the short term. It's not ideal, but if we can get JWICS to Iraq and Afghanistan, we should be able to get it in Philadelphia.

## What do you see as the biggest challenges facing DSS?

I think our biggest challenge is breaking down stove pipes in the Department. DoD is the largest bureaucracy in the government. There are a lot of players and some cross-jurisdictional concerns inherent in that bureaucracy. I think that can sometimes limit our access to information we need, or at least delay getting the information. So it complicates our role.

I am not hesitant to take on these issues. I understand that other parts of the Department have different mission sets and sometimes different goals. Security and counterintelligence aren't everyone's top priority in DoD. That is, until something goes wrong, of course. But that is not unique to DoD. I think every organization has this tension, but we have to do what we can to be efficient and effective.

## What message would you like to share with the men and women of DSS?

I think it's very easy to get caught up in the day-to-day business, the nitty gritty details of our jobs and not take time to step back and look at the bigger picture. The "why we do what we do."

For instance, you may be providing a threat brief to someone who is traveling. You may have done that brief a thousand times, and you look at it as just another threat brief. Well, let me tell you something, there are foreign intelligence officers who have collection requirements. And they are looking for people who work for certain companies or have access to certain technologies. And they are waiting for them to travel. And they find out about the travel through Facebook, through SIGINT, through e-mail monitoring, through intercepted text messages.

They will dispatch an intelligence officer who has a very good assessment of the traveler based on social media, e-mails, and internet activity. And that intelligence officer is going to be highly skilled in "bumping" into people and establishing a very non-threatening relationship based on common traits. You're a stamp collector? That's funny, so is he! He will be able to discuss that topic at length. You will be amazed by how much you have in common.

Over time, when the two are really good friends, he will manipulate that relationship to get exactly what he wants and that entire project that person is working on will be compromised. But then again, that threat briefing you gave him, may prevent all of that from happening.

Trust me, that's how it works. I've done it, and I've seen it done over and over. That single threat brief that you gave, can save an entire program. So my message is, don't just focus on the task. Remember why we are doing our jobs. Don't forget the big picture. Every employee in DSS has some role in protecting our nation's secrets. Never forget that.

DIRECTOR AWARDS

# Annual award ceremony

The fifth annual Director Awards ceremony was held in late March and coincided with the Industrial Security Field Operations Supervisor's Training.

The standing-room-only crowd witnessed the inaugural presentation of the 2015 Humanitarian Award, as well as recognition of the 2015 Excellence in Innovation Award, and Team and Employee of the Year for 2015.

In his opening remarks, James Kren, DSS Deputy Director, said the Director Awards program has continued to evolve each year, noting the addition of the Humanitarian of the Year Award. "This program showcases the very talented workforce in the agency," he said. "During this time when budgeting is tight, recognition can decline leaving employees wondering whether or not their efforts are truly noticed and appreciated. This program is a way of recognizing you, your work and the value of your risk-based decisions."

He noted that the agency will continue to incorporate changes that will enhance the success of the program and in turn, support the recognition of those employees who go above and beyond the call of duty. "Whether you are an award recipient or an award nominee, you competed among a group of highly talented employees and teams across DSS, and this program is a win-win for us all," he said.

There are two factors for which an employee or team is nominated for the Director Awards: Business results and agency core values. Business results include such factors as building partnerships, innovation, customer focus, and process improvement. Agency core values are dependability, respect, integrity, agility, collaboration and accountability.

In his closing remarks, DSS Director Dan Payne noted, "The threats we face grow daily due to the improvements in technology," Payne said. "DSS is on the front line to face those threats. Every little thing you do is one step closer in confronting the threats we face.

"In listening to the awards and narratives, I am struck by the diversity of the teams, and the breadth and scope of the mission that we have at DSS," he continued. "Today is about you; the nominees and the winners we recognized, as well as the larger DSS workforce. My job as director is to build upon this foundation of achievement and excellence."

## EMPLOYEE OF THE YEAR

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

The winner of Employee of the Year for 2015 was Heather Mardaga, Center for Development of Security Excellence. Mardaga was nominated for her efforts in establishing new industrial security training.

Mardaga developed the first comprehensive training path for industrial security representatives. She formalized a three-tiered training program which replaced training that only concentrated on developing new employees, thus neglecting the mid- and senior-level industrial security representatives.

# recognizes the '*best of the best*'

Employee of the Year Heather Mardaga (right), Center for Development of Security Excellence, stands with DSS Deputy Director James Kren.

*(Photos by Hollie Rawl, CDSE)*

> "There's a saying, **'the team is only as strong as its members;** and the members are only as strong as the team.' I'd like to share this award with all of these people."

She did not merely define a training path; rather she revolutionized the traditional training methodology by incorporating critical thinking and risk analysis into a progressive training venue interspersed with synchronous and asynchronous training.

In accepting the award, Mardaga said, "I started with DSS in 2002 as an investigator, and the agency has always given me opportunities for growth and potential. I transitioned from Field Operations to CDSE, and on the first day as curriculum manager, I was handed a contract for the development in just nine months of a brand new training program."

Mardaga continued, "Over 60 people helped support this initiative, from DSS leadership down to the employees in the field, who provided feedback and made it worthwhile. There's a saying, 'the team is only as strong as its members; and the members are only as strong as the team.' I'd like to share this award with all of these people."

## TEAM OF THE YEAR

The Team of the Year award recognizes teams who, as a group, exhibit the highest standards of excellence, dedication, and accomplishment in support of the DSS mission. The 2015 Team of the Year is the Defense Insider Threat Management and Analysis Center (DITMAC) team.

The DITMAC team reached across 43 Department of Defense components, the National Insider Threat Task Force and DSS to develop and execute pioneering initiatives in the establishment of the DITMAC organization — notably excelling in building partnerships and accountability.

On Jan. 1, 2015, the DITMAC was only words on the December 2014 Under Secretary of Defense

Members of the 2015 Team of the Year, the Defense Insider Threat Management and Analysis Center, stand with DSS Deputy Director James Kren (center).

for Intelligence memo. It had no organizational structure, no permanent staff, no budget, no concept of operations, no standard operating procedures, no identity, no office space or infrastructure, no Systems of Record Notice, no DoD instruction or directive, no strategic communications plan, and no case management system.

In just 12 months, with only three initial core members, all of these items were achieved and DITMAC reached provisional initial operating capability on Oct. 1, 2015.

In accepting the award on behalf of the team, Matt Guy said, "This was a challenging and rewarding year; we built something from nothing, and learned a lot. We discovered that the supporting and enabling elements are very important, but didn't realize how important until you're sitting in the dark with just pencil and paper.

"This is a long haul effort and there's still a lot of work to do," Guy continued. "We push for a reason. Two-and-a-half years ago, 12 people in the Washington Navy Yard went to work with a reasonable expectation of safety and security. We owe nothing less than our best to the families affected by the Washington Navy Yard, Fort Hood, and WikiLeaks incidents.

"A lot of activities have taken place, but we are doing it for a reason," he concluded.

**Defense Insider Threat Management and Analysis Center Team Members:**

Andy Branigan, *Business Enterprise*

Michael Buckley, *DITMAC*

Matthew Guy, *DITMAC*

Matthew King, *Business Enterprise*

Mark Nehmer, *DITMAC*

Miladys Ortiz, *Counterintelligence*

Anique Tores, *Human Capital Management Office*

Cherry Wilcoxon, *Business Enterprise*

## EXCELLENCE IN INNOVATION OF THE YEAR

The Excellence in Innovation of the Year is awarded to an individual or team that develops and implements innovative products, services, processes, or technologies to meet new or existing requirements, articulate needs, and improve the way government operates.

The purpose of this award is to develop new solutions that go beyond marginal improvements in existing products, services, processes or technologies. It is designed to encourage dialogue across the community, challenge peers to think and work differently, and take calculated risks to move government in a new direction.

The 2015 Excellence in Innovation of the Year was presented to Team San Diego, Industrial Security Field Operations, for their creative implementation of risk management principles.

The San Diego team pioneered the implementation of risk management principles designed to buy down risk and increase DSS effectiveness in protecting classified information entrusted to cleared industry.

The multi-disciplined team, involving local, regional, and headquarters personnel, leveraged the institutional knowledge of all levels within DSS to better attack foreign targeting of U.S. classified and sensitive technologies.

With their synchronized approach to operations, they established criterion for each element of risk to better align resources against where risk thrives. The team developed new data streams and identified intelligence gaps to further refine their risk identification.

In accepting the award on behalf of the team, Tim Barnes, Field Office Chief, thanked all who supported the implementation of the risk management principles, especially the members of Team San Diego. "This wasn't created in a vacuum," he said. "It was an integrated environment, which had an impact on multiple echelons and the various directorates."

Representing the 2015 Excellence in Innovation of the Year winners, Team San Diego, Jeff Boick (left) and Tim Barnes (right) stand with DSS Deputy Director James Kren.

"This wasn't created in a vacuum. **It was an integrated environment**, which had an impact on multiple echelons and the various directorates."

## HUMANITARIAN OF THE YEAR

The Humanitarian of the Year award is presented to the employee or team who contributes to human welfare, and improving the quality of life and health of a group of individuals in the United States or abroad.

The employee or team nominated has demonstrated significant leadership and outstanding volunteer service accomplishments and through the scope

Humanitarian of the Year Randy Staples (right), Logistics Management Division, stands with DSS Deputy Director James Kren.

of work undertaken a commitment to humanity and selflessness, without regard to personal or organizational gain or profit. The employee or team established or furthered a legacy and/or sustainable program that is of ongoing value and benefit to others.

The 2015 Humanitarian of the Year award was awarded to Randy Staples, Business Enterprise.

Thanksgiving is a holiday for people to be thankful for what they have. Staples is thankful for many things but foremost is his family. Staples wanted to create a tradition for his family and also teach his children what it truly means to be thankful.

So Staples and his family provide meals to the homeless on Thanksgiving Day through an effort that he and his wife oversee themselves. They begin the process in September to start recruiting and training volunteers, coordinate for food delivery to ensure the food is hot, and coordinate with the local D.C./Maryland governments for the necessary permits.

> “We started this initiative 20 years ago with our first child, **to teach our children values, teach commitment to service,** and to gain an appreciation for what they have.”

In accepting the award, Staples said, “We started this initiative 20 years ago with our first child, to teach our children values, teach commitment to service, and to gain an appreciation for what they have.”

## EMPLOYEE OF THE QUARTER

Also recognized during the ceremony were the Employees of the Quarter for 2015:

**Employee of the First Quarter:** Adam Lawson, *Counterintelligence*

**Employee of the Second Quarter:** Gary Layne, *Industrial Security Field Operations*

**Employee of the Third Quarter:** Matt Guy, *Defense Insider Threat Management and Analysis Center*

**Employee of the Fourth Quarter:** Jeremy Hargis, *Industrial Security Field Operations*

# And the nominees were ...

## Nominated for Employee of the Year

Matthew Guy, *Defense Insider Threat Management and Analysis Center*,
for his work in establishing the new DITMAC office.

Bill Huebner, *Business Enterprise*, for his efforts to automate the supply business.

Peter Jackson, *Industrial Policy and Programs*,
for his analytic approach to companies under foreign ownership, control or influence.

Edwin Kobeski, *Counterintelligence*, for his efforts in identifying bad cyber actors.

Stefan Rodrigues, *Industrial Security Field Operations*,
for his efforts in implementing risk management principles.

## Nominated for Team of the Year

Counterintelligence Operations Division for their highly effective methods
in countering foreign intelligence threats to industry.

Industrial Security Training Initiative Team, Center for Development of Security Excellence,
for establishing a comprehensive training path for industrial security representatives.

Team Albuquerque, Industrial Security Field Operations,
for their innovative approach to supporting cleared industry.

## Nominated for Excellence in Innovation

Counterintelligence Operations Division for successes that contributed to the
protection of U.S. and foreign classified information and technologies.

## Nominated for Humanitarian of the Year

Counterintelligence Western Region for its support to the Operation Warfighter Program.

Juaquita Gray, *Industrial Security Field Operations*,
for her support to the Palo Alto Veterans Administration Hospital.

# A Q&A with **Fred Gortler**, Director, Industrial Policy & Programs

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

**Fred W. Gortler III**, a Defense Intelligence Senior Level executive, is the Director, Industrial Policy and Programs.

In this capacity, Mr. Gortler oversees efforts in industrial security policy, mitigation of foreign ownership, control or influence (FOCI), implementation of FOCI mitigation measures, and administration of international programs.

Gortler has served in the national security arena since entering active duty in the U.S. Air Force in 1980. The Director of National Intelligence appointed him to the Senior National Intelligence Service in 2009.

He subsequently served in a Defense Intelligence Senior Level assignment with the U.S. Army before joining the Defense Security Service in 2015.

He serves the Director, DSS, as the lead for Industrial Policy and Programs.

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

I was an average kid from New York City who was given extraordinary opportunities to serve the public in the U.S. Department of Defense and national security arena. I graduated from the University of Maryland, was commissioned a second lieutenant in the U.S. Air Force and served for 26 years.

I transitioned to civilian service and will celebrate my tenth anniversary this year. I'm indebted to so many great leaders who invested in me over the years.

Highlights of my service include commanding an Air Force Wing, helping create the Office of the Director of National Intelligence, multiple assignments with the U.S. Marine Corps and Army, and now helping DSS evolve to fill a critical risk management role for the Department of Defense and National Industrial Security Program (NISP).

What led me to this position? It was the DSS senior leadership who sold me on the opportunity to serve the nation by creating a risk management framework for the NISP. Their leadership was bold and spirited. I wanted to be part of the team and I feel blessed to be here.

## You bring extensive DoD experience to this position but not industrial security experience. Do you think that's a benefit or has it made your job harder?

More industrial security experience is always a plus in our agency. But a number of other factors allowed me to contribute a range of national security experiences from the day I arrived. The first is the extraordinary professionalism and kindness of the DSS workforce. Leaders at every level — newcomers and seasoned veterans alike — were willing to teach. And I was eager to learn.

The dialogue continues to be rich and exciting. The late evening discussions with talented analysts in Policy and Programs allowed us to arrive at an important idea within the first 60 days of my arrival: we needed to transform the way Policy and Programs supported the DoD industrial security enterprise.

To develop the idea, and mature the enterprise framework, we needed tremendous support from across the agency. The DSS Deputy Director and Director, and our colleagues across the agency, helped shape what has become a new way of doing business in Policy and Programs and with the rest of our agency.

## IP is a disparate group (i.e. policy, FOCI, international). What are the challenges associated with managing such a diverse group?

I feel really fortunate to have landed in IP. We describe the DSS mission space as complex and hybrid. And we need a diverse team of generalists and specialists to

understand the mission space and contribute to the partnership of the U.S. government with private industry.

While our professional resumes may be among the most diverse in DSS, we're connected by a shared sense of what we're here to do: to ensure that U.S. and allied forces are equipped with the very best — uncompromised!

This strengthens the connective tissue and helps us ensure that we bring the whole of IP — and the whole of DSS — to meet the industrial security demands of DoD and the National Industrial Security Program.

## What do you see as IP's role in supporting the agency's industrial security mission?

DSS serves in partnership with private industry to protect classified information and technology. We are evolving into the premier risk management agency for DoD and NISP. In this context, the IP role is two-fold. First, to address the impact variable in the risk formula (risk is a function of the following variable: threat, vulnerability, and impact.).

The impact variable focuses on that intersection of government and private industry partnership, and addresses the factors of time, cost, and potential for loss of life. We work with Counterintelligence, Field Operations, and the Center for Development of Security Excellence, the executive interagency and industry to synthesize the three variables and provide a risk assessment.

In turn, the risk assessment drives decision-making in execution of the NISPOM, and offers recommendations to DoD and the executive interagency on matters related to the Committee on Foreign Investment in the U.S. and National Interest Determinations.

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

Risk management — the heart of the DSS mission — is inherently a networked, enterprise undertaking. DSS mission success relies on dynamic collaboration among headquarters, mission directorates, and field operations.

The purpose of my visits was to listen and learn. Policy and Programs had created a concept of operations for how we would support the enterprise. During the visits, I shared our ideas, invited critique, and sharpened our concept of operations.

I'm indebted to the regional directors and field office chiefs who made the experiences so valuable. We discussed risk management in theory and then applied it to a specific case — a really tough one — being handled by the regions.

Each visit was fantastic! But the most valuable take-away was that DSS has an incredibly talented workforce in the field. Taken as a whole, the DSS team is formidable and up to the challenges we face in the complexity of the 21st century business environment.

“
The most valuable take-away was that **DSS has an incredibly talented workforce in the field**. Taken as a whole, the DSS team is formidable and up to the challenges we face in the complexity of the 21st century business environment.
”

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

The greatest strength? That's easy! Policy and Programs comprises an extremely diverse and talented workforce. We've been given the opportunity to be part of something much larger than ourselves, and we're embracing it.

Concerns? That's a bit tougher. In a fiscally austere environment, we'll need to work hard to ensure we've got the tools necessary to support an aggressive risk management program aimed at delivering rigorous security for classified information and technology in private industry.


**FOR REFERENCE:** The DoD Special Access Program Security Manual, composed of four volumes, is now available at www.dss.mil/isp/specialprograms.html for use by government organizations and cleared industry.

# DoD Special Access Program Security Manual arrives

**by Scott Harkema**
*Industrial Policy & Programs*

The DoD Manual 5205.07, "DoD Special Access Program (SAP) Security Manual" is now available on the DoD Issuances website. The manual is composed of four volumes, each focusing on a different aspect of SAP security.

The purpose of the manual, in accordance with the authority in DoD Directive (DoDD) 5143.01, is to implement policy established in DoDD 5205.07, assign responsibilities, and provide security procedures for DoD SAP information.

- **Volume 1, "General Procedures"** assigns responsibilities, implements policy and describes the general procedures for the administration of DoD SAP security. It also incorporates and cancels Revision 1 Department of Defense Overprint to the National Industrial Security Program Operating Manual Supplement.
- **Volume 2, "Personnel Security"** assigns responsibilities and provides procedures for personnel security for DoD SAPs. It incorporates and cancels Under Secretary of Defense for Intelligence Memorandum, "Special Access Program Nomination Process," from 2013.
- **Volume 3, "Physical Security"** implements policy and assigns responsibilities and provides procedures for physical security for DoD SAPs.
- **Volume 4, "Marking"** provides guidance and procedures for the application of control markings on DoD SAP information. It also cancels Directive Type Memorandum 07-021, "Declassification Marking Guidance for DoD Special Access Program (SAP) Classified Material," from 2007.

Processing procedures, documents, forms, and templates associated with these volumes are on the DSS website, Special Programs page (www.dss.mil/isp/specialprograms.html) for use by government organizations and cleared industry.

Questions about policies and procedures for the implementation of the new DoD SAP Security Manual volumes should be directed to the appropriate servicing Special Access Program Central Office.

TABLET TEST PROGRAM

# Expanding technology for the mobile DSS workforce

**by Ryan Deloney**
*Industrial Security Field Operations*

DSS performs an industrial security oversight mission through the efforts of hundreds of personnel overseeing thousands of cleared industry locations spread across all 50 states. This leads to substantial time on the road for DSS personnel as they visit industry sites to accredit information systems, approve safeguarding, conduct security vulnerability assessments, and provide critical advice and assistance.

These visits can require personnel to bring large amounts of reference material, electronic equipment, and folders of facility specific information to perform their duties. Recognizing the need for automation, data, and collaboration tools at their fingertips, DSS is undertaking efforts to provide modern technology solutions to fulfill mission requirements.

One solution is providing DSS field personnel with custom tablet devices that are full-desktop replacements in a portable form and provide all the capabilities they need on the go. With hardware custom configured and accredited for use in secure environments, these devices are a single tool that can be used across office, field, and industry locations.

## BENEFITS INCLUDE:

- Easy access to policy documents, such as the National Industrial Security Program Operating Manual, industrial security letters, and other reference materials and information, such as industry site specific data.
- Integrated smart card readers for authentication, data encryption, and log-on security.
- Improved connectivity with a mobile hotspot allowing connection to the DSS network.
- Remote access to key systems of record, such as Industrial Security Facilities Database, ODAA Business Management System, and Joint Personnel Adjudication System.

**SUCH SUCCESS:** Personnel in the pilot program were so impressed that many did not want to return their tablets.

- Increased processing power and memory improve system functionality and multitasking.
- Stylus and virtual keyboards allow for on-site digital capture of information, eliminating manual notes

In early 2016, DSS began a pilot program allowing field office and headquarters personnel to test the devices and provide critical feedback on functionality. Feedback from headquarters personnel was overwhelmingly positive, and users were so impressed many stated that they did not want to return their devices.

This pilot will support a larger technology modernization strategy, driving wide deployment of modern mobile capabilities for the workforce. Over the next year DSS will embark on the first stage of this strategy, deploying new tablets and laptops across the agency. Future stages will include activities such as developing mobile applications and optimized websites, as well as integrating cloud technology into daily operations.

There are many exciting enhancements on the way to improve automation and efficiencies within the DSS workforce so that it can continue to serve as a risk-focused security partner with industry and government stakeholders!

# Online collaboration facilitates insight, increases

**by Wayne Lund**
*Center for Development of Security Excellence*

As you read this article, over 100 security professionals across the federal government are engaging in online discussions regarding important issues related to Department of Defense security programs.

These discussions range from evolving cybersecurity challenges to in-depth studies of the Constitutional and legal bases for security requirements and are led by subject matter experts (SMEs) working under contract as instructors for the Center for Development of Security Excellence (CDSE).

This online collaboration occurs among students as they complete the graduate courses offered by CDSE. Each semester, students study topics for insight into their security responsibilities and to prepare them for challenges they will encounter throughout their careers.

These graduate courses require students to consider the topic, post 200 to 500 word answers to related questions, and respond to posts made by their classmates, evolving the study into meaningful and thought-provoking discussions.

Examples of these discussion topics from CDSE instructors include:

- What legal challenges might emerge in the future as technology advances?
- Discuss specific U.S. security concerns involved with foreign attempts at acquiring U.S. missile technology.
- Provide a recent specific example of the threat posed by a "friendly" intelligence agency.
- Are legal requirements in human resource management consistent with and complementary to personnel security requirements?

The weekly student responses are based on the lesson reading assignments, course material and their own personal and professional experience and opinions. In some discussion forums, students are required to cite authoritative documentation to prove their points, while other discussions are less formal.

Once a student responds to the topic, their classmates critique the initial response and often ask follow-up questions or add comments based on their own experiences. Since students have diverse work histories and experiences, they often address the same question from very different perspectives, adding to the richness of the online discussion.

As the nature of threats to the nation's resources changes, security professionals are required to make sound, data-driven risk management decisions, often requiring them to identify issues from a security perspective different from their own.

The perspective of a counterintelligence professional, for instance, often diverges from a professional who has spent years doing classification management and derivative classification duties in a research facility.

This diversity adds value to the online discussions and encourages collaboration in developing strategies in a rapidly evolving security landscape.

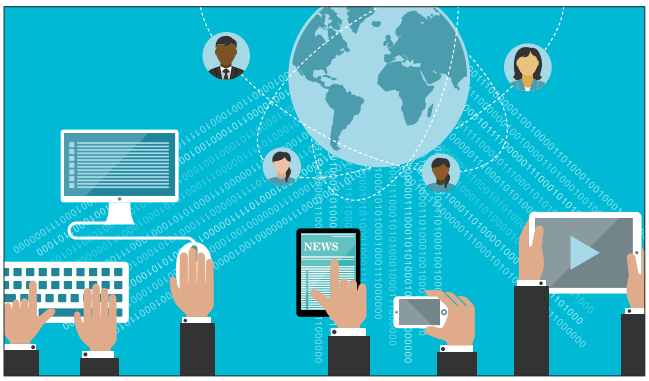
Active duty military service members comprise approximately 15 percent of the student population. The majority are non-commissioned officers of rank from E-6 to E-8 or officers at the rank of O-1 to O-3; however, at some point, nearly every rank and grade has been part of the student population.

Some have security duties as their main area of responsibility, others may be responsible for operations dependent on sound security programs, and still other service members are taking classes to help them prepare for transition into a civilian career as a security professional.

DSS employees from across the agency and all security disciplines comprise approximately 12 percent of the student population. The specific industrial security experience DSS employees bring to the discussions is of great value to their classmates.

This is particularly true when they participate in courses such as "Security in the DoD Acquisition Process" (ED 513), which is closely related to the National Industrial Security Program.

# understanding of graduate course material




Students develop professional relationships with their classmates by participating in the online discussions. Students typically interact one to three times per week over the course of a 16-week semester.

In some cases, students have the opportunity to meet in person after being in class together. Several have commented that the camaraderie developed in online courses is similar to that developed among classmates in a traditional classroom setting.

CDSE offers 17 graduate courses, presented online using a collaborative learning environment. This format allows the instructor to present material and lead students in discussions based on lesson content and reading assignments.

Each course is presented during a 16- or 17-week semester and is equivalent to a three-credit graduate course that may be offered by a university. A student may also choose to earn a certificate by completing four courses (12 graduate credits) in an area of concentration. These certificates include:

- Certificate in Risk Management
- Certificate in Security Leadership
- Certificate in Security Management
- Certificate in Security (Generalist)
- Certificate for Systems and Operations

For course descriptions and enrollment information, please visit www.cdse.edu/education.

"

I'm taking away more from the class than I thought I would. Specifically, I was able to learn from the instructor and the students because **some of the students were subject matter experts** on a course topic that was introduced during the given week.

**I really enjoyed ... the deep discussions that were posted in the forum** by the students and the instructor.

— **GEROLD GOUDY,** *Information Protection Specialist, U.S. Air Force*

Overall, **these forums do facilitate bringing the class together** over the 16 weeks of the course.

I've seen many examples where, by the middle of the class, **students are using their classmates to help solve work-related problems**, like inquiring about how other agencies are approaching a particular policy issue or asking for another student's opinion regarding how they would solve a particular security problem.

— **DUSTIN FRAZIER,**
*Security Specialist, U.S. Army*

"


**SLAMMIN':** DSS senior leadership discuss aspects of the risk-based approach to the DSS mission during the three-day annual meeting a

# Senior Leader Annual Meeting

In what has become an early spring tradition, the DSS senior leadership attended an annual meeting in early March at the Bolger Center in Potomac, Md.

The three-day agenda focused on transition — to a more risk-based approach to doing business, as well as leadership transitions — and was particularly relevant as incoming director, Dan Payne, attended the event in advance of his official arrival at DSS.

Day One of the meeting focused on "Thriving through Transition — It Starts with Us." The opening session focused on organizational culture, and included discussions on the behaviors that contribute to culture, how the agency's internal culture affects its relationship with industry and how the agency wants to be perceived by its stakeholders.

The discussion ended with the leadership team gaining a better awareness of how their individual actions contributed to the agency's culture.

Payne then provided introductory remarks to the group. He said he was privileged to have been selected as the director and looked forward to getting into the 'nitty gritty' of the agency and its mission. Payne also stated that he viewed the current counterintelligence threat as "... more significant than I've ever seen, due partly to increases in technology."

Payne added that security is the front line of every counterintelligence program, whether personnel or physical security. He closed the first day by stating his intention to listen and learn.

Day Two of the meeting focused on "The Future is Now." The leaders listened to several updates from subject matter experts from across DSS who provided the latest initiatives in analyzing data from companies under Foreign Ownership Control or Influence, the annual trends analysis, and cloud and mobility strategy.

In each case, the briefers presented detailed analytic products that were used to frame discussions in their office as well as in the field and in their engagements with industry.

at the Bolger Center in Potomac, Md. The Regional Directors discussed how a risk-based model helps them prioritize their workloads.

# brings together new director, new focus

The afternoon session looked over the horizon at emerging missions that were still being defined and discussed within DoD, but that are expected to include DSS, such as unauthorized disclosure and continuous evaluation.

The day ended with a discussion on initiatives underway in the Department to look at budget, manpower and organization structures and how they affect the agency.

Day Three of the meeting focused on "Work Left Undone." A major topic of discussion was the agency's movement from a compliance-based review of industry under the National Industrial Security Program to a risk-based analytic approach.

The regional directors in particular discussed how a risk-based model helps them prioritize their workloads and know where to dedicated limited resources. The Western Region also reported on their success in developing risk criteria on which to schedule and frame their assessments.

A critical component of the risk approach includes an automation tool such as a content management system that would provide a dynamic digital environment in which to operate. Such a system would also provide the Center for Development of Security Excellence with a collaborative and adaptive learning environment.

Jim Kren, Deputy Director, presented a list of priorities for the agency for 2016, such as continued leadership development, support to and integration with the defense security enterprise, and enhanced information technology and cyber security systems.

Before wrapping up the final day of the offsite, Clarence Johnson (Director, DoD Office of Diversity Management and Equal Opportunity) spoke about the importance of diversity and inclusion in effective organizations. The leaders then discussed how to further enhance diversity and inclusion in DSS.

In his closing remarks, Payne said as director, he would be looking for collaboration, cooperation and innovation. He urged the leadership to be open to trying new things. "That's what makes a good organization," he said.

# Growing cyber security experts through collaboration

**by Selena Hutchinson**
*Industrial Security Field Operations*

Recently, the DSS Human Capital Management Office recruitment team participated in the CyberCorps® Scholarship for Service Job Fair. They were accompanied by subject matter experts from the Office of the Designated Approving Authority, who helped identify and evaluate candidates suitable for information systems security professionals developmental positions in the Capital Region.

Karl Hellmann, ODAA, noted that "CyberCorps® is an excellent program and the perfect recruitment venue for identifying developmental or entry level cyber personnel." Hellmann learned of the scholarship program while serving as the Regional Director of the Western Region.

"People would look at the newspaper in the old days," he added. "That's not how it's done today if you're looking for highly technical skilled personnel."

To gain an edge in hiring, many federal agencies use CyberCorps® to attract qualified technical candidates. After the initial recruitment phase, ODAA will work with HCMO by handling the full range of hiring duties including initial outreach, scheduling interviews, reference checks, and preparation for new employee orientation.

Attending the event from the HCMO recruitment team were Laura Szadvari, Recruitment Manager, and Shon Todd and Israel Seda-Sanchez, Human Resource Specialists (Recruitment).

The CyberCorps® Scholarship for Service is a nationwide scholarship program designed to increase and strengthen the number of federal cybersecurity professionals who protect the government's critical information infrastructure. The scholarships are funded through grants awarded by the National Science Foundation and are coordinated by the Office of Personnel Management.

The scholarships require a mandatory paid internship during the course of the scholarship and a commitment to work for the federal government in a position related to cybersecurity for a period equal to the length of the scholarship.

Although DSS does not currently have any CyberCorps® interns, previous participants of the program included Jenna Kingsbury, Center for Development of Security Excellence; Nathan O'Neill, San Antonio Field Office; and Marcellus Williams, Virginia Beach Field Office.

**RECOGNITION**

# Complex trusted

**by Nicoletta Giordani**
*Industrial Policy & Programs*

[**Editor's Note:** The below article is a personal account of the efforts taken by the Foreign Ownership, Control or Influence Operations Division, Industrial Policy and Programs, in developing FOCI mitigation for a complex trusted foundry acquisition.]

The Department of Defense's ability to provide superior capabilities to the warfighter is dependent, in part, on its ability to incorporate rapidly evolving, leading-edge microelectronic devices into its defense systems, while balancing national security concerns.

However, DoD's access to trusted leading-edge microelectronics faces challenges stemming from manufacturing costs, supply chain globalization, and market trends.

To address the risk related to foreign sources, DoD initiated the Trusted Foundry Program in 2004 with only one company providing government-wide access to leading-edge microelectronics in a trusted environment. Later DoD expanded, through an accreditation process, the number of trusted suppliers.

However, only the original company offered leading-edge technologies that met the needs of DoD and, for over a decade, DoD relied on that sole source for trusted leading-edge microelectronics.

In October 2014, DSS received a draft FOCI mitigation plan from a foreign-owned business entity, in connection with its proposed acquisition of the sole source for trusted leading-edge microelectronics. However, the mitigation proposal did not mitigate FOCI, and I was asked to lead the negotiation of FOCI mitigation of this complex case.

# foundry acquisition requires unique mitigation

The target of the foreign acquisition was the sole source supplier to the U.S. government of microelectronic products that supported 33 percent of DoD's acquisition programs, and no alternative options were available.

In order for the company to achieve profitability it needs to operate as a globally integrated business. This presented several challenges from a FOCI perspective, especially in relation to governance of the entity under FOCI and shared services.

Based on my understanding of the core business considerations, knowledge of sovereign funds' structures and FOCI policy, DSS was able to develop a unique mitigation plan that met the requirements of the company while also addressing the concerns of the U.S. government.

Instead of addressing the FOCI related issues through a traditional analysis of FOCI factors, DSS used a risk-based approach that took into account the threat, the vulnerabilities, and the impact variables to identify an innovative solution that would mitigate ownership, control, and influence.

The mitigation plan allows the company to continue to work as a globally integrated business while providing the U.S. government with the appropriate level of oversight.

Furthermore, the mitigation plan broke new ground in the history of DSS and will be used for similar cases going forward.

In recognition of the efforts taken to mitigate FOCI, the team — Allyson Renzella, FOCI Operations branch chief, Sara Coonin, FOCI Operations action officer, and me — received an Award for Excellence presented by the Under Secretary of Defense (Acquisition, Technology and Logistics) Frank Kendall.

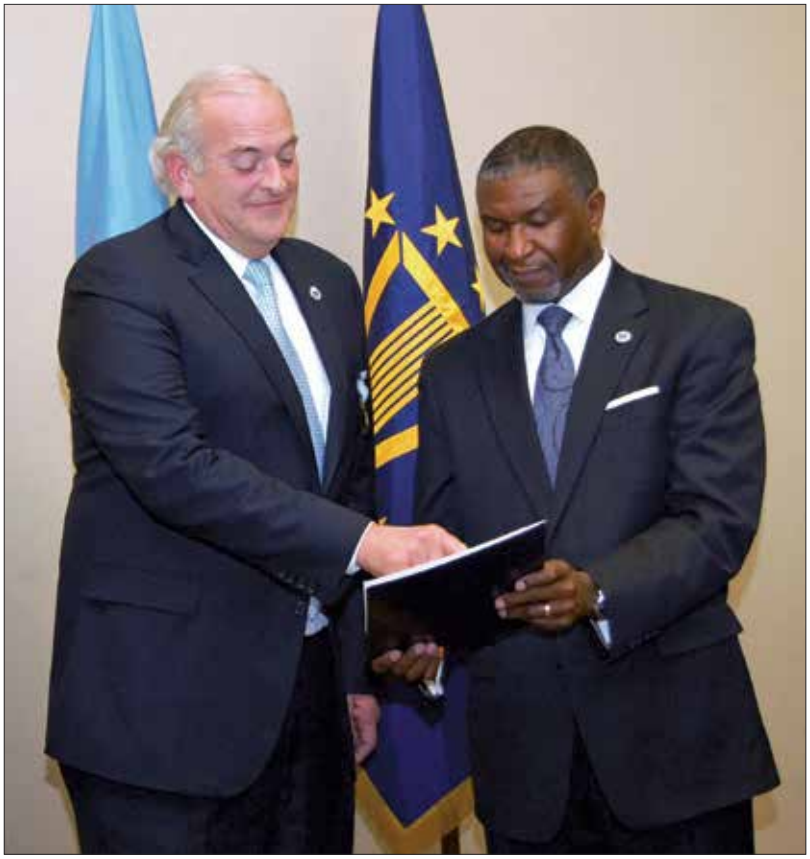
---


**CREDIT DUE:** Purdue University received the 2015 Defense Security Service Award for Excellence in Counterintelligence in recognition of their accomplishments in helping thwart foreign-directed theft of U.S. defense technology.

At the award presentation, from left, are Purdue President Mitch Daniels; Mary Millsaps, Purdue research information assurance officer; Suresh Garimella, Purdue executive vice president for research and partnerships; and Daniel E. Payne, director of the Defense Security Service.

*(Purdue University photo/ Vince Walter)*

# Chief Financial Officer retires



**FAREWELL:** Barry Sterling (left), former DSS chief financial officer, and former DSS Director Stan Sims read the Secretary of Defense's letter.

Barry Sterling, Chief Financial Officer and Director of Business Enterprise, retired in late January, having spent the previous 10 years with DSS.

Sterling, a retired Air Force officer, was dispatched to DSS by the director of Counterintelligence and Security, Under Secretary of Defense for Intelligence, in November 2006 to assist in determining the financial status of the agency.

He arrived, in an acting capacity, not long after the agency discontinued processing Personnel Security Investigations for Industry (PSI-Is) due to systemic budget shortfalls.

Upon arriving, Sterling found a financial management office in disarray with few established processes and a demoralized staff with vacancies in key financial and budget positions. He also found he was the ninth comptroller in just four years at the agency.

In spite of these challenges, Sterling accepted a permanent position at the agency in September 2007 and was instrumental in putting DSS on firm financial footing.

Under Sterling's stewardship, DSS executed four major initiatives. The DSS Transformation Plan and Future Options Study identified the baseline funding for DSS to execute its mission and brought additional personnel and financial resources to the agency.

Funding for the PSI-I mission was stabilized and rigorous oversight was implemented to monitor expenditures under the program. And DSS relocated from Alexandria, Va., to Marine Corps Base Quantico as part of the 2005 Base Realignment and Closure Act.

Sterling established the Business Enterprise Directorate to consolidate like functions and get the largest agency support elements moving in the same direction — at the same time.

This initiative provided significant dividends to Industrial Security Field Operations as Logistics Management, the Office of Chief Information Officer and Acquisition were all on board with field office closures, relocations, and delivering SIPR capability.

Stan Sims, previous DSS Director, spoke at the ceremony and noted Sterling's strong military background and sense of duty. He also said of Sterling, "Few will ever know what you did at DSS, but we know. We know what you contributed."

Sterling cited the contributions of agency personnel in turning DSS into an efficient, model agency. "It wasn't me," he said. "It was all of you. The mission of DSS is phenomenal and the people are phenomenal."

In closing he said, "I'm not worried about DSS, I think the credibility of the agency is now well-established, and it's clear the value the agency provides to national security. I think DSS can serve as a model of financial rigor and efficiency, but the challenge will continue to be demonstrating the return on investment DSS provides," he said. "I encourage everyone at DSS to remember your past, define your present and continue to move the agency forward."

**NEVER FORGOTTEN:** Attendees of the 21st Anniversary Remembrance Ceremony of the Oklahoma City Bombing walk around the Field of Chairs.

# Ceremony marks 21st anniversary of bombing

A cold, damp morning forced hundreds of family members, survivors and community members inside First Church for the annual ceremony marking the bombing of the Alfred P. Murrah Federal Building in Oklahoma City. First Church, located across the street from the memorial site, was damaged in the bombing and has long served to support the local community.

Oklahoma City Mayor Mick Cornett noted the day's resemblance to the weather in 1995 in his remarks. He also shared the mission statement of the National Memorial Foundation, "We come here to remember those who were killed, those who survived and those changed forever. May all who leave here know the impact of violence. May this memorial offer comfort, strength, peace, hope and serenity." He added that Oklahoma response to the attack, "dared the world to pull us apart."

Oklahoma Governor Mary Fallin told the audience, "Today we're back and we haven't forgotten, 21 years later, that there were people who suffered tremendous loss ... and there were certainly so many men and women who faced evil with courage." She also acknowledged and thanked first responders, "We pay tribute to those who displayed acts of heroism. We have not forgotten."

Michael Turpen, Chairman of the Oklahoma City National Memorial Foundation, read a statement from President Barack Obama, which stated in part, "We will never forget the innocent souls taken from us that day, nor will we forget the resilience the survivors demonstrated in the wake of this unspeakable tragedy. Refusing to succumb to fear, people went back to work within days of the bombing, and in the years that would follow, a community of friends and neighbors came together to lift each other up.

"The bombing of the Alfred P. Murrah Federal Building reminds us that in times of need, Americans of all backgrounds can join in common purpose to shape a safer and more peaceful tomorrow.

The ceremony concluded, as it does each year, with family members and survivors reading the names of the 168 individuals killed that day.

**From the Defense Investigative Service:**

Harley Richard Cottingham
Peter L. DeMaster
Norma "Jean" Johnson
Larry L. Turner
Robert G. Westberry

Defense Security Service