

DSS ACCESS

Official Magazine of the Defense Security Service | Volume 7, Issue 4

THIS ISSUE

NISP Enterprise
Wide Area Network
Authorization minimizes
operational burdens,
leverages efficiencies



DSS ACCESS

Published by the
Defense Security Service
Public Affairs Office

27130 Telegraph Rd.
Quantico, VA 22134

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

DSS LEADERSHIP

Director | Dan Payne

Executive Director | Troy Littles

Chief, Public Affairs |
Cindy McGovern

Editor | Elizabeth Alber

Layout and Graphics |
Marc Pulliam

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

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

All pictures are DoD photos, unless otherwise identified.



COVER STORY: NISP ENTERPRISE WIDE AREA NETWORK AUTHORIZATION MINIMIZES OPERATIONAL BURDENS, LEVERAGES EFFICIENCIES

NISP Authorization Office launches Enterprise WAN initiative **4**

INSIDE

Initial deployment of NISS brings new FCL system of record **6**

DSS CI special agent receives DoD award **7**

DSS LDP Capstone Projects address agency issues, challenges **8**

DSS employee selected for White House Leadership Program **12**

"Innovation: Advancing the Security Paradigm" is focus of 2018 DoD Security Conference **14**

2018 'Insight for Industry' is DSS' first Small Business event **16**

Paid Student Internship Program
'Shaping a new generation of Federal leaders' **18**

From the Director

By the time you read this issue of ACCESS, we will be in the midst of the holiday season and starting to put 2018 behind us as we look toward 2019. As the year comes to a close, I want to mention a couple of major DSS initiatives highlighted in this issue.

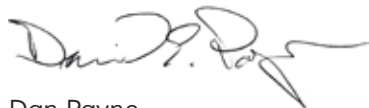
Our cover story features an initiative called the NISP Enterprise Wide Area Network (eWAN) Authorization. The NISP eWAN allows cleared contractors operating information systems distributed at multiple sites to work within a centrally managed system under a single authorization to operate. This is in contrast to the old way, where each individual site had to be authorized separately. This helps streamline the process and minimize operational burdens on both industry and the government. The feedback we've received from industry so far has been very positive: the eWAN process offers contractors a competitive, cost-effective approach that mirrors the best practices of the Risk Management Framework.

Also on the technology front, DSS deployed the National Industrial Security System (NISS) in early October. NISS replaces two legacy systems — the Industrial Security Facilities Database (ISFD) and the Electronic Facility Clearance System (e-FCL) — both of which were manually driven, cumbersome, and ineffective for a 21st-century environment. NISS is the result of a lot of hard work and long hours by a dedicated team of professionals who were, and remain, committed to providing a system that uses automation to streamline the facility clearance process and enable faster, easier communication between DSS and our industry and government partners. Stay tuned for additional improvements and features as NISS develops.

As of this writing, we are still awaiting guidance from the White House on the transfer of the background investigation mission from the National Background Investigations Bureau (NBIB) to DSS. In the meantime, we are continuing to work hand in hand with NBIB leadership on the nuts and bolts of the transition.

In late October, NBIB Director Charlie Phalen and I visited the DSS field office in Irving, Texas, and stopped by a cleared facility in the area where NBIB employees work on site. Mr. Phalen and I also visited NBIB's National Training Center in Slippery Rock, Pennsylvania, as well as the NBIB offices in Boyers, Pennsylvania. Each of these engagements was overwhelmingly positive, and many DSS and NBIB employees are excited to begin the transition process. The number one concern we heard from employees is job security, which is an understandable concern in any reorganization. Of course, it would be naïve to think that nothing will change as a result of the transfer, but we are committed to doing everything possible to minimize disruption to the workforce and to our missions. Toward that end, we're looking at a number of different organizational structures and will continue to adjust as we prepare for the transition. Within the next couple of years, DSS and NBIB as we know them today will be significantly different as we merge two organizations into one. This is a very complex undertaking that will not happen overnight, but much of the new organization will come into focus as we enter the new year. We will share our progress with you in future issues of ACCESS.

Thank you for reading and thank you for all you do.



Dan Payne
Director



AROUND THE REGIONS

QAISC holds annual kick-off meeting **20**

Making a Difference: How to stay motivated in a process that is never completed **21**

DSS pays tribute to former employee **23**

ASK THE LEADERSHIP

A Q&A with Richard T. Naylor, Deputy Director, Counter-intelligence (Cyber) **10**

NISP Authorization Office launches Enterprise WAN initiative

by Selena Hutchinson, GSLC

Industrial Security Field Operations

The Defense Security Service and cleared industry have successfully transitioned the National Industrial Security Program (NISP) to the Risk Management Framework (RMF). The transition challenges were time consuming and tedious as RMF requires more rigor and security acumen than the previous certification and accreditation methodology. In an effort to minimize operational burdens and leverage efficiencies, Karl Hellmann, the NISP Authorization Official (NAO), created a new initiative called the NISP Enterprise Wide Area Network (eWAN) Authorization.

The NISP eWAN concept

A NISP eWAN is a corporate network that connects geographically dispersed user areas that could be anywhere in the United States. As is the case with



Four DSS information systems security professionals conducted the first eWAN assessment in industry - (from left) Jonathan Cofer, DSS Headquarters; Keith Wagner, Capital Region; and Mike Ott and Rob Riggle, Western Region.

most WANs, an enterprise WAN links LANs (local area networks) or an individual system in multiple locations. The enterprise -- cleared contractor facilities in this case -- owns and manages the networking equipment within the LANs; however, the LANs are generally connected by a service provider. The NISP eWANs are unique in that the architecture design and data exchange must meet security control requirements in addition to interconnection and data exchange requirements. The authorization would allow NISP organizations operating distributed systems at dispersed sites into a large, centrally managed system under a single Authorization to Operate (ATO).

Pilot partnership

The eWAN initiative, which is voluntary, began with industry partners who already operated a single system at multiple locations or multiple systems and locations as the core criteria for participating in the pilot. This would be key in moving the idea from conception to reality. These mission partners would benefit from a single ATO for an enterprise system construction. Each eWAN will be unique to the NISP participant and the organizational business requirements for their specific operations. The pilot targeted three large contractors who met the core criteria for the NISP eWAN authorization initiative implementation. On the DSS portion of the pilot, the NAO team conducted an extensive technical analysis to ensure that the current authorization processes and applicable procedures were adequate or modified to meet the eWAN complexity and risk management requirements. On the cleared industry side, their team focused on design, selecting the security controls and risk implementation strategy. The collaborative partnership produced the pilot objectives:

- Standardized system and security management by leveraging centralized resources
- Shift to cloud computing
- Impact of increased amounts of real time traffic
- Support the rigorous RMF processes without an increase in industry or government workforce size or person-hours required

- Refinement of eWAN assessment and authorization processes

Additionally, to meet these strategic objectives the participating companies and supporting facilities will be required to have Enterprise Mission Assurance Support Service (eMASS) accounts. The eMASS application will enable industry partners to develop the artifacts required for the authorization package, track the documentation, and monitor the package through each step of the process. After an authorization decision all continuous monitoring and corrective actions for the several dozen plans of action and milestones can be tracked in the system. Currently, eWAN participation is voluntary. Industry participants were challenged to compose a team with the right combination of technical and security skills to design and develop a security compliant eWAN during the pilot.

The Initial Assessment

The assessment process was preceded by a series of collaborative technical reviews conducted over several months between the NAO Headquarters and the industry technical and security teams. These meetings allowed the teams to iron out system details and thoroughly evaluate the security controls and the voluminous documentation submitted to support the assessment. Any new assessment procedures or considerations were captured and documented to ensure the unity of design and security control management. The eWAN authorizations will be approved by NAO Headquarters as the majority of the eWANs will span more than one region.

During the first week of October, the eWAN Program Manager Jon Cofer assembled a multi-regional team of four information systems security professionals (ISSPs) to conduct the first eWAN assessment and document the assessment analysis. The team was composed of:

- Jonathan Cofer, senior ISSP, NAO Headquarters
- Keith Wagner, ISSP, Capital Region
- Mike Ott, ISSP, Western Region
- Rob Riggle, ISSP, Western Region

During the week-long assessment, the team conducted an in-depth validation of the nationwide classified network of the Raytheon Corporation, the first company to complete the pilot. Their eWAN will consolidate over 200 separate or disparate systems and supporting ATOs into one centrally managed

authorized classified information system. This system is both the first of its kind in the NISP, and the largest single system ever authorized by DSS in both size and complexity.

Also attending the Raytheon eWAN assessment kick-off and out-brief sessions was Hellmann, who stated, "(The) Enterprise WANs will be the way forward for the largest cleared contractors to consolidate risk and operations under the Risk Management Framework; allowing them to centralize security operations and subject matter expertise while providing real-time vulnerability response and mitigation as well as near instant response to insider threat actors."

Enterprise WAN benefits

The NISP eWAN authorization has the potential to provide the following benefits:

- Support the company WAN dependencies
- Allow DSS and the facility to manage one authorization
- Reduce long-term workloads for industry and DSS
- Provide opportunity to optimize scarce resources
- Enable centralized authorization decision management
- Centralize incident response or disaster recovery
- Standardize continuous monitoring and insider threat monitoring
- Define and identify system and network boundaries

Conclusion

The eWAN authorization initiative requires security professionals to use critical thinking skills to integrate RMF into company business operations in response to evolving threats and new security requirements. The eWAN is not a fad and will not disappear as they have become a staple in cleared industry. Industry has concluded that the eWAN provides them with a competitive, cost-effective approach to security that mirrors the best practices of RMF.

Industry security professionals who put in the rigor to meet the complex requirements of the eWAN are likely to see considerably more risk management in their security posture for years to come. The path to an ATO may be long and difficult in the early stages, but for those companies that can harness their technical resources and security professionals on mission needs, the eWAN is paying dividends.

Initial deployment of NISS brings new FCL system of record

by **Lauren Firich**

Industrial Security Field Operations

After a lot of hard work from DSS, industry, and government partners, the National Industrial Security System (NISS) deployed Oct. 1, 2018, as the system of record for facility clearance (FCL) information. NISS is the new DSS information system architecture that replaced and expands upon Industrial Security Facilities Database (ISFD) and Electronic Facility Clearance System (e-FCL) capabilities to provide an on-demand, data-driven environment with automated workflows accessible to industry and government partners.

The initial deployment of NISS provides key capabilities to industry and government partners, to include:

- Submit and view progress on facility clearance sponsorship requests
- Submit facility clearance verification requests in a streamlined fashion
- Automatically receive notifications for key events such as updates to facility clearance status or a change in the DSS industrial security representative (ISR)
- Access to a knowledge base with system-related content, such as system training video shorts, and links to relevant external information
- View "for official use only" notices, such as cyber threat bulletins
- View new and archived DSS information, such as the Voice of Industry newsletter
- Overall improved timelines for DSS processing through automated workflows
- Single sign-on, role-based access through the NISP Central Access Information Security System (NCAISS)

Industry partners will have additional benefits, to include:

- Submit and view progress on facility clearance documentation packages

- Submit and view progress on reportable facility change conditions
- Submit annual self-inspection certifications
- Message your ISR (to include sending security violations, suspicious contact reports, and other content)
- View facility information (DSS facility data such as classified holdings, programs, key management personnel, foreign ownership, control, or influence information, etc.)
- Complete surveys such as the Personnel Security Investigations for Industry (PSI) Projection Survey

To register for a NISS account, users must establish an NCAISS account. Once the user logs into NCAISS, the user can request a NISS account using the "Create/Modify Requests" button. Industry account requests are routed to the assigned ISR for review and approval. Government account requests are routed to the DSS Knowledge Center for review and approval. Detailed instructions on how to register for a NISS account are on the NISS webpage under the "Registration" section.

Training for NISS is available through the Security Training, Education, and Professionalization Portal (STEPP): "National Industrial Security System (NISS) External User Training Course IS127.16." Additionally, system training video shorts are available on the user's dashboard upon logging in to NISS. Finally, webinars and conferences on NISS functionality are provided throughout the year. The NISS team is visiting national and local industry security professional groups to provide NISS demonstrations and answer questions.

Automation enhancements won't stop with the deployment of NISS, as additional enhancements will provide smart-forms, information availability, and mobile capabilities.

DSS CI special agent receives Secretary of Defense award

Counterintelligence Special Agent (CISA) Rob Dela Rosa, San Francisco Field Office, received the 2018 Secretary of Defense Award for the Outstanding Department of Defense Civilian Employees and Service Members with Disabilities during a ceremony in October at the Pentagon.

Dela Rosa is a 15-year Marine Corps veteran who began his civil service career at DSS soon after successfully completing an internship through the Operation Warfighter Program.

A CISA since 2015, Dela Rosa provides CI support and liaison to cleared industry, the Intelligence Community, and law enforcement agencies, to include the FBI, CIA, Department of Homeland Security, and others. As a part of his duties, he presented unclassified and classified threat briefings to more than 400 cleared facilities, resulting in over 1,800 suspicious contacts from which nearly 500 intelligence reports were generated. Additionally, he provided classified briefings to Congressional delegations on illicit technology transfer to foreign nations.

"I believe it's simply a willingness to continue serving and being a good steward of what I'm responsible for, which includes providing meaningful service and support to our industry and government partners, strengthening those relationships and partnerships, and trying to forge new ones as best I can," said Dela Rosa of his job responsibilities.

Active in his community, Dela Rosa serves as an outreach coordinator for a local church, which involves organizing holiday dinners for the homeless, leading initiatives to support families in need, facilitating faith-based financial and marital guidance, assisting in leading young adult ministries, and facilitating a holiday initiative to provide meaningful gifts to those who are incarcerated.

"I'm involved in faith-based outreach efforts, and recently as part of this involvement, the team I'm working with discussed ways to contribute more to



the local community," he said. "We're looking at ways to strengthen and expand our efforts."

Dela Rosa has twice received the DSS Western Region CI Special Agent of the Quarter Award, and has been nominated for various other national- and DoD-level awards. When asked why he believes he received the award, Dela Rosa noted it should have been won by all involved in carrying out the DSS mission.

"I'd like to relate this to all DSS employees and the efforts everyone is contributing," he said. "I think there are other employees more deserving who should receive a DoD award like this. Within the last several months and as we speak, the talent within each DSS element and from every discipline contributes to forging a new way for DSS to do business as the organization grows in numbers and responsibility.

"I am grateful I get to continue serving beside very talented folks and leaders, especially in the Western Region – folks who recognize the skills and talents of each other, and believe in the importance of the mission and impact of our teams," Dela Rosa said. "Most importantly to me, I'm grateful that I have a patriotic wife and children who know the importance of this work which makes it easy for me to continue serving."

DSS LDP Capstone Projects address agency issues, challenges

by Dr. Fred Bolton

Human Capital Management Office

One of the hallmarks of the year-long DSS Leadership Development Program is the Capstone Project.

These projects represent a significant investment by program participants to address an issue or challenge of significance to the agency. These projects spanned issues across DSS and were the focus of attention for senior DSS leaders.

During the first face-to-face LDP session, participants were placed in cross-functional teams of five to eight participants to examine complex issues and leadership concepts using an experiential action-learning approach. LDP teams met face-to-face or virtually on a recurring basis throughout the 12-month program as participants learned to both lead a team and lead as part of a team. Team activities stressed the importance of interpersonal skills, critical thinking, and problem solving, while a cadre from the Center for Creative Leadership supported the teams with periodic engagement activities throughout the year.

Project topics were submitted by various directorates, linked to the DSS Strategic Plan and DSS in Transition, and were broadly divided into technical and organization culture issues. These included:

Technical issues:

- Security violation process
- Review DSS in Transition (DiT) and the National Industrial Security Program (NISP)
- DiT communications
- Training and education strategy -- performance management and metrics
- Strategic Plan ownership and relevance

Organization culture issues:

- DSS retention "Stay Interview" initiative
- Employee turnover and work-life and incentive benchmarking project
- Federal Employee Viewpoint Survey (FEVS) results *

- Defense Equal Opportunity Management Institute Survey results *
- DiT culture analysis
- MD-715, "EEO Requirements for Federal Agencies," Barrier Analysis *

Capstone project presentations were a key focus of the Leadership Development conference conducted at the end of the first LDP iteration. At the beginning of the conference, skills related to team presentations were provided by members of the local Toastmasters club. Each team rehearsed and refined their presentation before making a 30-minute presentation to DSS senior leaders. Through this process, LDP participants successfully demonstrated their ability to research, analyze, interpret, and provide recommendations on important agency issues.

The Capstone presentations were well received, and resulted in an engaged and lively discussion with DSS senior leaders. As a result, the projects transitioned into the DSS governance process for review and action. During August and September, members of the Capstone teams presented the project results to the Executive Steering Committee and Deputies Council. Through this process the project recommendations were accepted and assigned to an office of primary responsibility for action.

The Capstone project concept has been widely hailed as a success. Comments from DSS senior leaders demonstrated the value of the projects with a high level of praise for the professionalism and quality of the research and results. In addition, the Capstone projects were identified as an essential element of the DSS LDP by participants. By focusing on critical aspects of teamwork, DSS employees were able to enhance their skills as leaders through the development of the Capstone projects.

(End Notes: The FEVS, conducted by the Office of Personnel Management, serves as a tool for employees to share their perceptions in many critical areas including their work experiences, their agency, and leadership. The results give

agency leaders insight into areas where improvements have been made, as well as areas where improvements are needed.)

The DEOMI Organizational Climate Survey is a commander's management tool that proactively assesses critical organizational climate dimensions that can impact the organization's mission. This voluntary survey focuses on three primary areas: Organizational Effectiveness, Equal Opportunity/Equal Employment Opportunity/Fair Treatment, and Sexual

Assault Prevention and Response.

MD-715, "EEO Requirements for Federal Agencies," is the policy guidance which the Equal Employment Opportunity Commission provides to federal agencies for their use in establishing and maintaining effective programs of equal employment opportunity; and provides a roadmap for creating effective equal employment opportunity programs for all federal employees as required by Title VII and the Rehabilitation Act.)



TOP LEFT: Mery Neal, San Antonio Field Office, presents a portion of her group's Capstone project. **TOP RIGHT:** Patricia Stokes, director of the Defense Vetting Directorate, asks a question during the Capstone briefings. **BOTTOM LEFT:** Sal Urbano, St. Louis Field Office, briefs on the security violation process. **BOTTOM RIGHT:** Dawn McCalvin (left), Program Integration Office, briefs on the DSS in Transition culture analysis, while Mike Sheehan, Boston Field Office, provides slide presentation support. (Photos by Marc Pulliam, CDSE)

A Q&A with **Richard T. Naylor**, Deputy Director, Counterintelligence (Cyber)

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



Richard T. Naylor, a Defense Intelligence Senior Level Executive, is the Deputy Director, Counterintelligence (Cyber) in DSS. In this capacity, he oversees the execution of DSS' efforts to derive intelligence from

the behaviors in the cyber domain. He joined DSS in September 2011.

Prior to joining DSS, he was as the Deputy Director, Communications, Computers, Architectures and Chief Information Officer, U.S. Cyber Command.

A retired Air Force colonel, Naylor had a distinguished military career and served in a variety of organizations, to include: U.S. Space Command, Air Force Office of Special Investigations and U.S. Special Operations Command, before retiring in 2011. Naylor was twice selected to command and served as the 2nd Air Force vice commander. He is the recipient of numerous military decorations, including the Defense Superior Service Medal and the Legion of Merit.

Naylor received a bachelor's degree from the University of Tennessee in Computer Science, a master's degree from Troy State University in Human Resources Management, and a master's degree from the University of Colorado in Computer Science.

Q: How does DSS CI Cyber support the overall mission of DSS?

Is it possible to "protect classified information and to preserve our Nation's economic and technological interest" without considering the risk of the cyber

domain? Clearly our adversaries have asymmetrically leveraged the cyber domain to their advantage. The almost daily reports of nefarious activity in the cyber domain demonstrates not only that our constituents are at risk, but our adversaries are using the cyber domain as part of an all-source approach. DSS CI Cyber endeavors to derive intelligence from behaviors occurring in the cyber domain to, in turn, thwart them.

Q: Where do you see DSS CI Cyber evolving as we bring on additional missions and restructure the agency?

DSS CI Cyber will become an even more essential component. Not only is the cyber domain, especially in the Controlled Unclassified Information (CUI) arena, arguably the most troublesome spot with the greatest surface vulnerability, it also holds promise to be leveraged to our advantage. It is, perhaps, the only domain in which we can rapidly scale up to meet the new coverage areas.

Q: What increased capability does CI/Cyber bring to the Intelligence Community (IC) table? What does it bring to DSS in Transition and the National Industrial Security Program?

As DSS embraces CUI, vetting, and Comprehensive Security Reviews, leveraging the cyber domain will be the quickest, most efficient way to scale up to cover the user base and spot suspicious activity. Given the recent press coverage of our adversaries' successes, especially in the unclassified cyber domain, as the DSS mission expands, Cyber is positioned to lead that charge.

Q: What is CI/Cyber doing to adapt to IC missions and processes?

I suggest the question is not "doing to adapt to"



but should be “doing to mature the integration of intelligence derived from the cyber domain.” In this era of unprecedented cooperation, we are working closely with the Analysis Division to greatly inform their efforts as they bring true rigor to the intelligence products to meet the IC standards. Related to the discussion above, Cyber is the one area where DSS can rapidly scale to meet the coming growth.

Q: What is the difference between Joint Cyber Intelligence Tool Suite (JCITS) and DC3's framework agreement?

Other than involving activity occurring in the cyber domain, they have little similarity. The Framework Agreement is a voluntary group who share information to make each other more secure. JCITS is a process which informs all-source analysis by, in a machine learning environment, deriving intelligence

from cyber-based threats. In its current state, it casts a “net” over 1,000 companies and looks for adversarial activities both aimed at a company and after an adversary has been successful. A side benefit is JCITS also illuminates network vulnerabilities. JCITS can rapidly scale up to cover all the CUI companies.

Q: What is on the horizon for the division and cyber in general?

Big times! As the Defense Science Board states, “Defense only is a failed strategy.” Pursuing a cybersecurity focused strategy is a recipe for losses. We are, more and more, proactively putting the tools and processes in place to engage the adversary in an all-source way. The goal should be to eventually mitigate the need to worry about post-loss damage assessment.

DSS employee selected for White House leadership program

by **Beth Alber**

Office of Public and Legislative Affairs

Nicoletta Giordani, Industrial Security Integration and Application (ISIA), was selected for the next iteration of the White House Leadership Development (WHLD) Program, which began in October 2018.

The WHLD, which is sponsored by the Executive Office of the President (EOP), provides a unique opportunity for participants, who will work on the President's Management Agenda highest priority and highest impact challenges that require the coordination of multiple Federal agencies to succeed (<https://www.performance.gov/>).

"The White House program develops senior leaders who manage at an interagency level," said Giordani. "This program challenges you to reach beyond your area of expertise and the organizational boundaries of your division or agency to build coalitions, re-think and modernize how we achieve the overall mission, and drive change on some of our nation's most systemic challenges."

"Many issues facing the federal government have become government-wide problems," she said. "This program helps develop the enterprise mindset leaders need to work those issues."

Giordani served as the assistant director of the Business Analysis and Mitigation Strategy division within ISIA before starting a detail with the Office of Management and Budget (OMB) in May 2018. During the detail, Giordani is overseeing a number of different accounts in the OMB National Security Division, to include Army Operation & Maintenance, Army Readiness, the Committee on Foreign Investment in the United States (CFIUS), and personnel security clearance and background investigation issues from a budget aspect. She is also monitoring the transition of the background investigation mission from the National Background Investigations Bureau to the Defense Security Service, and associated policy reforms.

After being accepted as a WHLD Program Fellow, the program senior leaders coordinated with OMB to keep Giordani in the National Security Division during the fellowship, where she will continue to work on the issues mentioned above.

The idea for applying to the WHLD began a couple of years ago, when Giordani identified it as an objective on her Individual Development Plan.

"Identifying long-term career objectives is something I tried to foster within my entire team," she said. "Once we identify the objective, then we try to translate it into specific training opportunities. The application



Nicoletta Giordani, Industrial Security Integration and Application, speaks at the 2018 Foreign Ownership, Control or Influence conference. (Photograph by Hollie N. Rawl)



for the fellowship was in my IDP about two years ago."

When the announcement for the WHLDP came out, the application process began. According to Giordani, the first step was for her package to undergo an agency review, which involved a screening where applicants explain why they would be good candidates for the program and how it benefits DSS. Supervisors also have to explain why the individual would be a good candidate for the program. Candidate applications are then reviewed by a board of DSS senior leaders, and a nominee is forwarded to the Office of the Under Secretary of Defense for Intelligence (OUSD(I)). After OUSD(I) makes its selection, nominees are forwarded to the Office of the Deputy Secretary of Defense, who has the final review for the Department. For all of DoD, a maximum of four nominees are forwarded to compete for the WHLD Program.

Once the nominee packages are at the White House, the candidates undergo a phone interview.

"It's only a 30-minute phone conversation, but it is very fast paced," Giordani said. "Questions focused on leadership and the characters of a good leader."

If a person makes it past the first screening, then they are called in for an in-person interview – but with an assignment.

"You are given a topic, with a few days to develop a presentation on a government-wide related issue,"

Giordani said. "When you arrive for the interview appointment, you have to brief WHLDP officials on your assigned topic, and be prepared to respond to questions."

Selections are made based on the outcome of the second appointment.

When Giordani transitions to the WHLDP, she has numerous objectives she hopes to achieve.

"I hope to learn to be a more effective leader in the 21st century," she said. "I'm hoping to develop the mindset to handle interagency issues, and be exposed to situations where I'll be challenged and learn to deal with them effectively."

After finishing her fellowship, Giordani is looking forward to bringing her experience back to DSS.

"As the first DSS employee to participate in this program, I'm going to share my knowledge," she said. "I'm hoping to help others who are looking to improve themselves as leaders and expand their opportunities. I will focus on building a culture of continual change and improvement, and prepare my team to meet the challenges of interagency collaboration and to tackle government-wide initiative.

"I want to instill excitement about this opportunity, and for those people with a desire to grow, get them to realize this is one way to improve themselves as leaders," she concluded.

"Innovation: Advancing the Security Paradigm" is focus of 2018 DoD Security Conference

by **Paige M. Blache**

Industrial Security Integration and Application

In July, DSS hosted its first DoD Security Conference in three years, welcoming personnel from Defense agencies around the country. More than 300 security professionals, speakers, and staff gathered in Phoenix, Ariz., for information sharing and networking, training, and critical community exchange on current and emerging industrial security trends and solutions.

The conference's theme, "Innovation: Advancing the Security Paradigm," supports DSS's expanding role as the only DoD agency with the mission of providing security education, training, and certification to the Department and cleared industry, in addition to strengthening the Department's capabilities to protect information and technology vital to national interests.

The Center for Development of Security Excellence (CDSE) provided overall management and planning of the conference, led by Adriene Brown. As program manager, Brown led an interagency steering committee comprised of 15 mid- to senior-level security professionals from across the Department who developed the conference theme and topics. Additional DSS staff provided acquisitions, security, and administrative support leading up to the event.

"The planning and execution of the DoD Security Conference is a major effort, but worthwhile," Brown said. "The steering committee was instrumental in developing content for the event. As representatives of the community, they have a pulse on what our constituents need to know. I enjoy the planning process, and seeing the result is exhilarating."

The conference occurred at a very opportune time for DSS as the agency takes on a mission that will exponentially expand its workforce and increase its visibility across the defense community. DSS Director Dan Payne welcomed the group, informing everyone about the new Defense Vetting Directorate (DVD), its composition, and how continuous evaluation will change the way all cleared personnel are investigated.

Later Patricia Stokes was introduced as director of the new DVD. This gave her a unique opportunity



TOP: Welcoming DoD security professionals from around the globe, DSS Director Daniel Payne kicks off the 2018 DoD Security Conference. **BOTTOM:** Jason Taylor, Master of Ceremonies for the 2018 DoD Security Conference. (Photographs by Hollie N. Rawl, CDSE)

to discuss the personnel investigation mission with a large cross section of the defense workforce. After the background investigation is transferred to DSS, DVD will be responsible for personnel

security investigations for the entire defense portfolio. Breakout sessions on personnel security and continuous evaluation were standing room only, demonstrating the interest in the topic.

This year's conference had something for everyone. There were abundant policy updates, and most significantly, insider threat took center stage.

Paul Iacobucci, Air Force Office of Security, Special Program Oversight and Information Protection, said, "I found the policy updates to be most useful and walked away with a better understanding of changes coming down the road, especially the changes coming to the insider threat mission."

Emerging topics such as supply chain risk management and the ever-evolving cyber security risk were also highlights. Allyson Renzella, Industrial Security Integration and Application, said she "liked the overview on supply chain and critical program information risk mitigation sessions because of their relevance to DSS in Transition."

Representatives from Office of the Under Secretary of Defense for Intelligence and the Information Security Oversight Office explained the process for a new policy or regulation to become final. The long process involves several opportunities for the public to comment, including industry partners. Overall, participants learned that the process truly ensures public input and impact. Discussion on physical security policy became quite animated with a vigorous discussion about who should carry weapons at installations and at what clearance levels.

So how does a small agency like DSS end up hosting a conference for the expansive Department of Defense? As functional manager of Security Education, Training and Certification for DoD and industry, DSS has responsibility for leading this conference each year, whether held virtually, in person, or through both mechanisms, and he is supported by the DoD Security Training Council (DSTC). The DSTC is composed of DoD entities and provides a forum to discuss and coordinate security education and training issues and policies, recommend education and training standards, identify emerging training and needs, and promote professional development for the security workforce.

Feedback on the conference and its content was favorable, as participants enjoyed hearing about the



Delice Bernhard, Deputy Director DITMAC, speaks on "Insider Threat Reporting and Insider Threat Indicators: What the Security Specialist Needs to Know" during the DoD Security Conference. (Photograph by Hollie N. Rawl, CDSE)

latest developments in the various security disciplines.

First-time attendee Jerry Yost, security manager at Naval Air Station Jacksonville, Fla., said, "I thought the topics provided an overview of where the security industry is heading for the future.

"I believe the people and assets in the DoD are evolving and it's refreshing to know that the DoD is being proactive in evolving with the ever-changing security world," he continued. "I noticed several versions of insider threat briefings by different organizations, so it's important for security managers across DoD to utilize the resources to educate all members of the serious threats that our adversaries pose to the United States."

Andrianna Backhus, Industrial Security Field Operations, enjoyed the opportunity to attend the event alongside others in DoD. "I was reminded that there are other stakeholders dealing with the same situations, and hearing their questions helped me to understand what was important to them," she said. "I hope they had similar experiences of being aware that there are other people with relatable experiences so that we can work towards the same goal."

DSS plans to host a virtual conference in 2019, and the next in-person event in 2020.

2018 'Insight for Industry' is DSS' first Small Business event

by **Elizabeth Mudd**

Office of Small Business Programs

The DSS Small Business Office held its first small business event, “Insight for Industry,” in July at the National Museum of the Marine Corps, Quantico, Va. The various sessions of the event provided diverse perspectives to give small businesses a greater understanding of the agency and how companies can best align themselves to do business with DSS.

The audience of 80 industry participants, representing over 65 small businesses, ranged from companies that are doing business with DSS today to those eager to build relationships with DSS for the future. A few of the current small businesses in attendance were Metis Solutions, which provides administrative and analytical support services, Rockwood, which provides consulting services, and G Cubed, which provides counterintelligence subject matter expertise.

DSS Deputy Director James Kren kicked off the event by enlightening the audience on the transition of “DSS of Today” into the “DSS of Tomorrow,” noting how

small businesses are intertwined at all levels of the DSS mission. The small business community listened intently as he described the current threat landscape and how DSS is transitioning from a compliance-focused approach to an intelligence-led, threat-driven and asset-focused methodology which contributes to the protection of critical technology. Kren linked the mission to small businesses, noting that the first phase of the new DSS in Transition methodology has demonstrated that small businesses are contributing innovation to critical technologies.

“It is clear, small business is working on some of the technologies we see as the most important to protect under this new methodology,” Kren said. He added that DSS engages with small business from a contracting perspective as DSS has successfully contracted \$32 million directly with small businesses accounting for 72 percent of DSS dollars executed in Fiscal Year 2018.

Michael Halter, Industrial Security Field Operations (ISFO) deputy director, and Dr. David P. Grogan, Industrial Security Integration and Application (ISIA)



More than 80 industry participants, representing over 65 small businesses, attended the event at the Marine Corps Museum.



James Kren, DSS Deputy Director, provides a DSS update to the event attendees. (Photos by Beth Alber, OPLA)

deputy director, impressed the audience during the DSS Directorate Panel. Elaborating on Kren's opening remarks, the panel provided powerful insight into the directorates, painting a picture of how directorates integrate to accomplish the mission and then opening the floor to questions. The small business community jumped at the opportunity, and asked questions ranging from supply chain risk management to the Small Business Association's newly available All Small Mentor-Protégé Program, where joint ventures formed under this authority run into a hurdle with facility clearances. Later feedback on the event indicated this was a popular session, as participants noted, "I liked the opening discussion about DSS, ISIA and ISFO priorities and the dialog with these leaders." For many small businesses, this was a unique opportunity to learn how they can provide solutions to enhance the success of the DSS mission, but first they need to understand the priorities and mission of the directorates.

Following the Directorate Panel, details were provided about the small business program, and the new communication offerings available, such as one-on-one meetings and how DSS strives to keep every small business in the know by sharing new opportunities via email. A discussion of the Fiscal Year 2018 Forecast highlighted the small

business opportunities available for the remainder of the year and elaborated on how companies can best align themselves to do business with DSS. Educating small businesses on requirements for the end of the year allows DSS to receive high caliber contractors prepared to respond to DSS needs. Finally, statistics were offered on year-to-date small business achievements in the following categories: Women-Owned, Service-Disabled Veteran-Owned, Small Disadvantaged Business, and HubZone, noting how DSS exceeded the contracting goal in each category and highlighting how significantly small businesses contribute to the success of the DSS mission. The small business community shared how DSS invigorates them to engage in requests for information and solicitations.

The event concluded with a Contracting Officer Roundtable comprised of members of the Office of Acquisitions, including Tara Petersen, chief of Acquisitions, Ashley Maddox, Operations Branch chief, and Shenita Sylvain, Specialized Branch chief (acting). This provided an exclusive opportunity for industry to ask contracting questions directly to the DSS contracting team and likewise, for the contracting officers to ask questions of industry. In return, industry provided insight on their year-end process, stating they have to pick and choose which efforts to bid on that require past performance questionnaires due to the work involved for the contracting officer representatives. The open and collaborative dialog provided understanding for both sides as well as key take-aways that the Acquisitions Office is already considering for implementation in the future. This panel was a small business favorite as industry noted, "The contracting panel was great, as it was nice to hear directly from folks that release solicitations and make awards."

Each speaker and all who helped support the event exemplified the DSS motto of "Partnering with Industry to Protect National Security" with their openness, accessibility and transparency to educate the small business community in a collaborative manner that companies commented is not often seen in the government landscape. Small businesses often have to choose which events will provide them the most benefit for their time and money. DSS, by providing a free forum to speak directly with leadership, hit the mark on all accounts with this event.

Paid Student Internship Program

Shaping a new generation of Federal leaders

Editor's note: The following is a first-hand account of a DSS intern, and the article reflects her thoughts and opinions.

by Nicole Decker

Intern, Alexandria Field Office

"You are in control of your own career," said DSS Deputy Director James Kren during a roundtable discussion with a table of seasoned DSS interns. Varying in scholarship, age, and experience, all of the interns sat up straighter as they listened intently to Kren recount his experience in the federal government. He described periods of difficulty, uncertainty, and tragedy as well as great accomplishments. Like many of us in the room, he even admitted that he too was an intern, unsure of what he wanted to do.

The roundtable was held as part of the Paid Student Internship Program (PSIP), which was coordinated by Leila De'Vore of the DSS Human Capital Management Office (HCMO). The program is a summer-long, full-time, temporary employment experience designed to attract high caliber college and graduate level students with an interest in federal government careers. The program provides real-life, relevant work experience, and the opportunity to network with professionals in a variety of fields.

The PSIP students are sourced throughout the fall recruitment season and asked to submit applications on USAJobs.gov during the open acceptance period in late October. The qualifications for the PSIP include being a United States citizen, enrollment in an accredited college or university pursuing a bachelor's or master's degree, minimum grade point average of 3.0, completion of at least 24 credit hours, and the ability to obtain and maintain a Secret clearance.

The program also encourages recent graduates to participate, whether they are heading to graduate school, or simply looking for necessary work experience. These students work in various field offices and directorates, all with different reasons for choosing the federal government as summer employment.



DSS Paid Student Internship Program participants listen to DSS Deputy Director James Kren provide career development advice and guidance during a roundtable discussion. (Photo by Beth Alber, OPLA)

I am a student at George Mason University, in Arlington, Va., pursuing my master's degree in Public Administration, with a build-your-own concentration in Science, Technology, and Security. My experience is primarily in law and investigations, including a small stint in the District of Columbia's Superior Court. I came to DSS with the hopes of confirming my interest in federal service. Although the jury is still out on my decision, I can happily say that my experience was versatile and stimulating.

During my time at the Alexandria Field Office, I had the opportunity to shadow several Industrial Security Field Operations (IO) employees. I participated in security vulnerability assessments with industrial security representatives, sat in on a counterintelligence brief to industry, and attended a Risk Management Framework meeting with information systems security professionals. My favorite experience was participating in an annual foreign ownership, control or influence (FOCI) board meeting. I was given the opportunity to explain the process of continuous monitoring to the company's executive staff and outside directors, one of whom

was the former director of the National Security Agency and the Defense Intelligence Agency.

However, my experience is only a piece of the larger puzzle that is interning. Justin Walsh, director of the Capital Region, reiterated this point.

"Interning is not just a great experience for the individual developmentally, but it also greatly benefits the agency by alleviating workloads, meeting directorate goals, and bringing a fresh perspective," he said.

Other regions also benefited from the support of the interns. "The Western Region summer interns, Clint Gertsch and Richard Hana supporting counterintelligence, and Sydney Reck supporting IO, provided direct analytical support, which enhanced and comprehensive security vulnerability assessments in the Western Region," said Dave Bauer, director of the Western Region. "Improving on a process developed under previous interns, the interns supported field operations through open source analysis and threat products for sensitive technologies."

For interns like Amanda Clary, a senior at American University, the federal government provides experience that can't be found elsewhere. "In my field of interest (intelligence), you cannot receive the same type of quality training anywhere else," she said. "DSS provided a great foundation for beginning a career in intelligence, and taught me tactics used by our adversaries."

"Interning at DSS for the Office of Acquisitions has helped me grow so much, both personally and professionally. Observing leadership, sitting in on meetings, and participating in roundtable discussions inspired me to learn more about strategy and maintaining perspective when making important decisions," said Victoria Sanker, a graduate student at Pace University.

"The DSS Paid Student Internship Program has been invaluable in my professional and personal development. I developed my soft skills, got exposure to a number of different federal agencies in the DoD and Intelligence Community, and made lasting connections with some amazing individuals that helped guide and teach me," said Brittani Blanchard, a recent graduate of George Washington University who worked in the Diversity and Equal Opportunity Office.



Clint Gertsch (right), intern in the Western Region Office, receives a certificate of accomplishment during the DSS Intern Recognition Ceremony. (Courtesy photo)

Not only does the PSIP positively impact the individual interns, it can be extremely helpful to supervisors as well. When prompted, both Walsh and Dave Scott, Capital Region Authorizing Official, agreed that interns provide a fresh perspective on everyday challenges at DSS.

Scott further illustrated this point by recounting a personal experience. There was a moment when intern Matthew Pagano, a senior at Bridgewater College, came out of a meeting feeling a bit overwhelmed by the acronym soup. "At that time, I realized I needed to slow down and pause," Scott said. "Sponsoring an intern can humble you, but also assist in mastering your own work."

As for me, I felt humbled as well. It is important to learn about the peaks and valleys of government service, but it is a completely different experience to witness it firsthand. Not only was my work at DSS meaningful, and relatable to my studies, it was also eye-opening. Every day I learned something new, whether it be the countermeasures used to protect yourself from adversaries abroad, or simply eating lunch with two retired generals, swapping stories of travel or soliciting life advice.

QAISC holds annual kick-off meeting

by Randall Stacey

Industrial Security Field Operations

For the 11th annual Quantico Area Industrial Security Council (QAISC) kick-off meeting, held in August, at the Stevenson Ridge Event Center, Spotsylvania, Va., facility security officers (FSOs) were strongly encouraged to bring their management and program managers to the event. As a result, there were over 240 facility personnel in attendance.

The QAISC, founded in August 2007, is managed by a board of seven FSOs and meets monthly. The QAISC has grown from 50 members to over 550 security professionals representing various defense contractors in the Quantico and northern Virginia regions.

The annual kick-off event was hosted by the Spotsylvania County Economic Development Council Authority and the event showcases the “hard work and trying environment” the FSO must work in today. The Council has hosted this event for several years. Tim McLaughlin, Spotsylvania County Supervisor provided opening remarks and welcomed the honored guest, Mark Cole, Virginia House of Delegates, 88th District.

DSS Deputy Director James Kren discussed the importance of securing critical technologies with a trusted workforce, and how DSS is taking an intelligence-led, asset-focused, threat driven approach with industry and the government stakeholders. Unique to this year’s presentation, DSS used a team approach to field questions from the audience. John Massey, Industrial Security Field Operations assistant deputy director, and Justin Walsh, Capital Region director answered questions ranging from field operations across the country to those specific to the Capital Region.

Mark Riddle, a senior program analyst for the Information Security Oversight Office (ISOO) at the National Archives and Records Administration, was the guest speaker. He serves as lead for implementation and oversight activities for the Controlled Unclassified Information (CUI) Program. Riddle has developed a protocol for assessing existing executive branch agency programs that prescribe

protections for sensitive information. He establishes inspection criteria for evaluating implementation and ongoing operational efforts related to the CUI program. He also co-authored the National Institute for Standards and Technology Special Publication 800-171, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,” (June 2015). This publication recommends standards for protecting CUI in nonfederal electronic environments that may be prescribed in agreements between federal and nonfederal partners.

Feedback on the kick-off cited the interactive and dynamic nature of the meeting. Several company key management personnel commented on the information being invaluable to planning for the future of their facilities.

“This meeting is always the highlight of our year, and this year’s speakers definitely delivered. The collaborative presentations given by DSS’ James Kren, Justin Walsh, and John Massey provided an informative perspective on the direction the security industry is headed in partnership with DSS,” said Diane Moulton, QAISC chairperson working for Polaris Alpha Advanced Systems, Inc.

Several members of the AECOM Executive Management team attended the annual QAISC and lauded the opportunity to interface with DSS senior leadership and other government speakers.

“In particular, we were very interested and impressed with Mark Riddle’s presentation on CUI. AECOM strives to continuously comply with 32 CFR 2002, ‘General Guidelines for Systematic Declassification Review of Foreign Government Information,’ and this brief was extremely valuable,” noted Randon H. Ullrich, AECOM.

The QAISC will continue to meet monthly to provide security education to the contractors along with their monthly ‘Lunch and Learn’ conference calls that serve as a question-and-answer session on the changes occurring in industry.

MAKING A DIFFERENCE:

How to stay motivated in a process that is never completed

Editor's Note: The following reflects the thoughts and opinions of the author on his personal experiences at DSS and the evolution of the DSS mission.

by Kevin Flowers
San Francisco Field Office

Shortly after graduating from college, I was hired by then Defense Investigative Service (DIS) as an industrial security representative (ISR) in the National Capital Region. I worked as an ISR in various locations until 1999. From 1999 to 2016, I served as a counterintelligence special agent (CISA). Currently I am serving as the field office chief in San Francisco Field Office.

THE PAST: (1989-1999)

The past consisted of carbon paper (it did exist, seriously, it did); floppy disks (8 and 3.5"); typewriters; Commodore 64s; computer systems running 3.1 with a 30 megabyte hard drive and 8 megabyte of RAM. During this time DIS had one computer specialist for the entire region. The Cold War ended but there were defined enemies. We were learning about the events of the "Decade of the Spy." Military equipment was specialized technology. Classified information was mainly paper. Foreign ownership, control or influence (FOCI) was mainly foreign acquisitions. DIS was conducting compliance-based security inspections. Threat information wasn't readily available. DIS had the personnel security investigation mission which was organized as a separate mission set. Multinational partnership on commercial and military products started to form.

I remember how busy I was, and how we were on the cutting edge of technology...remember the carbon paper? How could things change or get any more complicated? I did many inspections and cited many deficiencies. I was making a difference. I conducted security inspections finding numerous example of deficiencies, such as improper markings, destruction



certificates not completed, closed area DSS Form 147's not filled out correctly, SF 312's not being done, or classified documents improperly stored. Case in point: I found hundreds of classified documents partially burned in a trash can at one cleared facility. The customer and I spent months tracking down the origin of these documents, trying to assess the damage to national security. Eventually one of key management personnel had his personal security clearance and facility clearance revoked. VICTORY!!! Wow, what a difference I was making. As you will see, I was lost in the moment and not forward-leaning. I was concerned about paper, briefings, storage, markings, etc. I was so busy in the now, that I was oblivious to the future, which is where our enemies were operating. Several hundred documents – half burned, seriously? It is only funny and obvious looking back but, I assure you, I believed I was in the thick of the battle.

THE PRESENT: (1999-2016)

In the present, we see Google just coming on the scene, CDs; web services; smart phones; electronics vs paper concerns; megabytes vs terabytes. Standard RAM is now at 6 GB. DSS is now looking at export controlled and International Traffic in Arms Regulations information; and FOCI associations and

investments with many countries. During this time DSS has approximately three information system security professionals (ISSPs) per DSS office. CISAs are new positions and gradually multiplying their presence to two per office. Known state actors are blurred and now include any 13-year-old with a computer and access to the internet. DoD is relying heavily on commercial off-the-shelf products. Threat information is now being disseminated to industry.

I remember how busy I was, and how we were on the cutting edge of technology...remember thumb drives? Now I am a CISA, ferreting out export-controlled information, involved in cases of U.S. and non-U.S. citizens convicted of stealing our technology, leading to arrest and seizures of millions of dollars. Insider threat issues are on the scene. I am connecting the dots with my fellow counterintelligence and law enforcement partners. One of the cases I worked led to the discovery of over 500 U.S.-based front companies operating illegally in the United States. Another case led to the arrest of a U.S. permanent resident caught red-handed with export-controlled, radiation hardened integrated circuits he planned to give to an East Asia Pacific country's ship captain at the port of Long Beach! Wow, what a difference I am making. I am super slammed and so busy, I can't get all the work done. I am working at an up-tempo pace that is tiring but exhilarating. How can things get any worse or more complicated? Again, I am caught up in the now and not realizing that we are winning a battle but losing the war. Despite all of my efforts, our adversaries are making leaps and bounds toward technology superiority. What happened?

THE FUTURE (2016-??)

Neuromorphic and quantum computing; "The Humanized Internet;" 2020 global electrification; big data; end of fossil fuels; renewables powering mobile networks; internet of everywhere; and technology eliminates third world designation. DSS takes on a new approach. We realize, possibly for the first time, that excellence, operating in the current state is failure. DSS starts DSS in Transition (DiT) where we are intelligence-led, asset-focused, and threat-driven. For the very first time, DSS looks to make industry a co-equal partner. Protection of critical technologies and Controlled Unclassified Information is the new battlefield. Continuous vetting, in regards to personnel security clearances, is the only way to free up resources to help conduct quality background investigations. Delivering a product to the military uncompromised not only can be done but needs to be

done. There is a fourth leg to the acquisition process, and it is security!

Now I am a field office chief where both nationally and locally, industrial security and counterintelligence are blending and becoming one versus two different disciplines. People, information, equipment, facilities, activities, operations, and supplies are assets we all need to be concerned about. These assets are surrounded by exponential opportunities for compromise that we have to constantly look to see if vulnerabilities exist. If DSS or industry finds these, we share with each other and put a security countermeasure against it. This is not a one and done process; it is continual! Our battle space has grown from a little sandbox to the Sahara! How can things get any worse or more complicated? We know they will, are we agile enough to pivot and change? I still have many years of work left but, to answer that question, I will have to come out of retirement to write a follow-up article.

SUMMARY

Change is never comfortable at first but, looking back, can you imagine life without change? It was easy when industrial security and counterintelligence did their own thing. Security Vulnerability Assessments were defined, standardized, and easy. Compliance solely to the National Industrial Security Program Operating Manual was understood and welcomed. Only classified information/systems were a concern, and intellectual property was outside the scope. We lived in a "bubble" all the while believing we were making a difference when in reality we were barely keeping up.

Sometimes we need to remember where we came from to appreciate where we are, and to know where we need to be. Feel free to quote me on that, it does sound pretty good right? We tend to wait for change to end before we embrace and move out. We fall into the trap that once this change is over, we will have time to move out and make a difference. We are not looking forward in our drive to make a difference we are looking at our rear view mirror.

Now is the time! Become agile, forward-thinking security and counterintelligence professionals. DSS, you have a partner (industry) with a whole lot of talent and abilities. Industry, you have a partner (DSS), with a whole lot of talent and abilities. Let's join forces to identify and prevent the loss of critical information and technologies. Let's make a difference!!

Paying tribute to a colleague who valued partnership

Editor's Note: The following reflects the thoughts and opinions of the author on the contributions of Senior Industrial Security Representative James C. McCulloch, who recently passed away.

by Ann Marie Smith
Tacoma Resident Office

In the mid-1990's, during the National Industrial Security Program's (NISP) infancy, I met Industrial Security Representative (ISR) Jim McCulloch of the Capital Region Crystal City Field Office, who embraced the new era of industrial security. Previously under the DoD Industrial Security Program (DISP), DSS (then the Defense Investigative Service) was relegated to fulfilling

a strict compliance role for national security concerns entrusted to industry.

Jim quietly influenced many security professionals; he was, unofficially, an astute mentor-protégé matchmaker and a local NISP community manager. He persuaded multiple area FSOs to volunteer countless hours fueling the effective government-industry, Crystal City Industrial Security Awareness Council (ISAC). Also spurred by Jim's vision of partnering, an annual, larger-area "Joint ISAC" event gained momentum which continues today to aid government-industry communication and to re-inspire attendees as partners in our important NISP mission.

His pride as a civil servant played no small part in my decision to pursue a career as an industrial security representative, and Jim became my formally-assigned mentor. Now, I attempt my own personification of the NISP partnership, when I enter a cleared contractor facility or answer their phone call, while Jim's spirit resounds in my heart and sets my tone for the interaction.



DSS supports local fire department

Recently, employees from the Western Region and San Diego Field Office toured Fire Station 33, San Diego County, in Rancho Bernardo. Afterwards, DSS personnel provided dinner for the firefighters and paramedics assigned to the station. California has been ravaged by wild fires and these firefighters are called into service routinely to fight fires in other parts of the state and their communities, in addition to responding to myriad emergencies. Fitting the occasion, the event abruptly ended when the firefighters had to respond to an event.

