# DCSA ACCESS

Official Magazine of the Defense Counterintelligence and Security Agency | Volume 8, Issue 3

VOL 8 | ISSUE 3

## DCSA LEADERSHIP



Published by the
Defense Counterintelligence
and Security Agency
Public Affairs Office

27130 Telegraph Rd.
Quantico, VA 22134

DCSA.pa@mail.mil
571-305-6562

*DCSA 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 DCSA.*

*All pictures are DoD photos, unless otherwise identified.*

COVER STORY 06

# CONTENTS




## COVER STORY



## INSIDE



## ASK THE LEADERSHIP



## AROUND THE REGIONS

# FAREWELL INTERVIEW WITH DIRECTOR PAYNE

*Editor's Note: Since its inception, the DCSA ACCESS has included a column or message from the Director. This issue marks the final one for Dan Payne. Rather than pen a farewell, Mr. Payne sat down for an interview to share his thoughts on his tenure.*

**Q What was your biggest surprise when you came to the Defense Security Service (now the Defense Counterintelligence and Security Agency (DCSA)) over three years ago?**

**A** Unquestionably, it was the high quality of the workforce. I'm not sure what I was expecting, but what I saw immediately was that DCSA had a very skilled workforce that was dedicated to the mission, creative and hard-working. The longer I worked at DCSA, the more impressed I became and the workforce continued to exceed my expectations by a long shot. No matter what challenges were thrown at the DSS workforce, they always rose to the challenge. Creative, well thought out solutions to problems came from every corner of DCSA. I am very proud of the DCSA workforce and very proud of their accomplishments..

**Q During your time at DCSA, what did you see as your biggest challenge?**

**A** The DoD bureaucracy! I come from an Agency that is small in comparison to DoD. As a result, they are very nimble, and bureaucracy is held to an absolute minimum. If there are policies that get in the way of completing the mission, the workforce, the middle managers and senior managers will rebel. They simply won't do it. So there is immediate feedback that a bad policy has been put in place and very quickly it is abolished or amended. The culture in DoD is a bit different. As I see it, it is a culture that follows orders and is loath to break chain of command. As a result policymakers don't always get the immediate feedback that there

is a policy in place that hinders completing the mission. Plus, once a policy has been established, the cumbersome policy process almost ensures that it will never be retracted without a significant amount of pain.

**Q What do you see as your most significant accomplishment?**

**A** Definitely the change to a risk-based methodology for reviewing the security of facilities under our cognizance. Our old methodology was simple and comfortable for everyone. It was also highly administrative in nature. The methods our adversaries were using to steal our information and technology changed over time. Our methods of protecting it did not. As a result, we were losing huge amounts of critical technology and information. That is not to say that those security measures outlined in the NISPOM [National Industrial Security Program Operating Manual] are ineffective, rather, the entire fabric of what needs to be protected and how we need to protect it has expanded well beyond the NISPOM.

Our adversaries do not differentiate between classified and unclassified information. We do. As a result, they take advantage of the gaps. Our adversaries don't distinguish between classified and unclassified information technology systems. We do. As a result they greatly exploit largely unprotected unclassified systems. We are at a point where we must look at the threat to industry and academia holistically, and we did not do that in the past. We have to keep a warfighting mindset. Our adversaries are trying to steal our technology so that they can kill our people in battle. We must fight their efforts on every front to save the lives of those we send into battle. To do that, we must look at this challenge holistically.

I think DCSA personnel have shifted to that mindset. I believe industry largely has also. But we have to be vigilant to ensure that complacency doesn't set in, both within DCSA and industry and academia.

**Q What did you not accomplish that you wanted to?**

**A** I don't look at it as things I didn't get to accomplish, I look at many things as evolutionary. We have a number of initiatives in play right now that I think are headed down the right track. And we wouldn't be in a position to make those changes without the accomplishments we have already made.

> **Three years from today, what we are doing now will seem so elementary. This is truly an exciting time to be in DCSA.**

For one, I think there needs to be a complete rewrite of the NISPOM. It must fundamentally change. What is policy in the NISPOM should be very high level goals. How you achieve those goals should be outlined in documentation that is less than policy and falls under the authority of the Director of DCSA with a governance structure that involves industry and academia. That would give us the flexibility to change our defenses as our adversaries change.

I think security has to be embodied in the entire lifecycle of an acquisition. We have a number of initiatives moving forward in this regard.

I think further refinement of Risk-based Industrial Security Oversight (RISO), the Security Rating Score, the development of the National Access Elsewhere Security Operations Center (NAESOC), refinement of the facility clearance process, development of supply chain risk mitigation methodologies, controlled unclassified information (CUI), all will have a significant impact on our ability to protect our critical technologies from our adversaries.

Three years from today, what we are doing now will seem so elementary. This is truly an exciting time to be in DCSA.

.

**Q How do you think adding the vetting mission will impact DCSA?**

**A** I think it will have an overall positive impact on both workforces as well as on our mission sets as a whole. First, I think this merger presents a lot of opportunity for our employees to move up, to take leadership roles, and learn new skill sets. Secondly, I see these two mission sets as having a lot of synergies across the board. There are a lot of similarities in the vetting processes utilized for individuals and companies. We can use developments in one to enhance how we complete the other. Additionally, our knowledge of what is taking place in the cleared facilities can lead to enhanced understanding of important issues related to the individual vetting process. I am very excited about DCSA and the impacts it will have.

I also believe that once DCSA can demonstrate that it can handle these new missions, I think others are likely to follow providing even more opportunities for the workforce.

**Q Any final thoughts?**

**A** As many of you know, I have had a pretty colorful career, but being Director of the Defense Security Service, and the first Director of the Defense Counterintelligence and Security Agency, will stand out as the highlight. I have thoroughly enjoyed working with all of you on a mission of incredible importance. I am so proud of this workforce and of having led this organization. This organization has an incredibly bright future. Individually, I ask that you never forget the big picture and always keep focused on why we do this mission…to protect our country. There are few things more important

## DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY BIDS

# FAREWELL TO FIRST DIRECTOR

The Defense Counterintelligence and Security Agency (DCSA) bid farewell to Director Dan Payne in a ceremony held on July 19, 2019, at the National Museum of the Marine Corps. The event reflected on Payne's tenure at DCSA and the role of the agency in protecting national security. The audience included senior DoD and government officials, industry partners, family, friends and the DCSA workforce, many of whom watched remotely.

Officiating was Under Secretary of Defense for Intelligence, Joseph Kernan. In his opening remarks Kernan said, "We celebrate today an organization that for 47 years has quietly been the foundation of the Department of Defense's personnel and industrial security enterprise. As of June 20, 2019, the Defense Security Service was officially renamed to the Defense Counterintelligence and Security Agency (DCSA), making Dan the last DSS Director and DCSA's first. And he is quick to tell you, he is the first."

Kernan noted that Payne's first federal job was as a GS-5 investigator making $12,000 a year at the Defense Investigative Service. "As I stand here today, I can think of no more appropriate position for Dan to end his federal career than as the director of the organization he began his federal career with," Kernan said.

Kernan briefly described the history of the organization and noted that the investigation mission was moved to the Office of Personnel Management in 2005, leaving two core missions: Industrial Security and Education and Training. Since 2005, DSS grew to just under a thousand personnel at 42 locations overseeing the protection of U.S. and foreign classified information and technologies at almost 13,000 cleared contractor facilities. Effective Oct. 1, 2019, DCSA will again have the personnel security mission and will grow to a government workforce of about 5,000 employees at 160 locations. It will also include the DoD Consolidated Adjudications Facility which will make it the largest personnel vetting organization in the federal government.

"That's a snapshot of DCSA and the agency Dan is leaving. But I want to highlight Dan's stewardship of DSS and DCSA, because without it, the agency would not be poised to assume the investigation mission," Kernan said.

The Honorable Joseph Kernan (center), Under Secretary of Defense for Intelligence, prepares to award Dan Payne (right), former DCSA director, the Department of Defense Medal for Distinguished Civilian Service, with Anita Galle, DCSA Executive Secretary, acting as proffer.
(Photos by Nina Orlando, CDSE)

Kernan noted that when he took the position as DSS Director, Payne made his first priority the integration of counterintelligence and security at DSS. "He believed the two missions are sides to the same coin and must work in unison," said Kernan. The result of Payne's vision is a risk-based methodology for reviewing the security of facilities under the agency's cognizance.

Payne's second priority was better integration and collaboration at the Federal level to include the larger Intelligence Community and federal departments. Kernan said Payne once again worked to break down these stovepipes and under his leadership, DSS forged new relationships and leveraged existing ones.

Kernan also addressed the pending transfer of the National Background Investigations Bureau (NBIB) to DCSA. "Moving any organization is hard, but one as large and complicated as the National Background Investigations Bureau, is unbelievably difficult," Kernan said. "Dan understood the synergies with the mission sets and viewed this as yet another way to eliminate stovepipes and develop a truly integrated, end-to-end personnel and facility vetting system."

After thanking the DCSA workforce for their support to Payne, Kernan addressed the industry and government partners in the audience. "I think this is direct evidence of Dan's outreach, but also a shared recognition that success in protecting our great nation lies in cooperation and partnership. Please know that this new DCSA, with a larger mission, will remain a valuable asset for your organizations and I ask you to continue to partner with them."

"And a final word to the team that now holds the DCSA leadership reins," said Kernan. "Charlie [Charlie Phalen, Acting DCSA Director], thank you for taking on these additional responsibilities. Even though you weren't the first DCSA director, it now falls on you to shepherd the agency through the complex transfer challenges ahead."

Kernan concluded by saying, "Dan, you leave quite a legacy. Please accept my sincere appreciation for the outstanding job you have done at DCSA. You have led the agency during a time of transition and positioned it well for the future. I wish you and your family all the best in the future."

Following his remarks, Kernan presented Payne with the Department of Defense Medal for Distinguished Civilian Service. The award cited Payne's extraordinary leadership and strategic vision which enabled the agency to deliver exceptional support to 26 Department components and 33 federal agencies as part of its mission to administer the National Industrial Security Program on behalf of the Secretary of Defense.

It also noted his strategic and operational guidance, coupled with his sustained engagement with senior stakeholders across the federal government, which positioned the Department to transform the personnel vetting mission and positively impact the nation's security posture. And finally, the citation said Payne had championed ground-breaking initiatives to enable risk-based, intelligence-led industrial security oversight processes that achieve departmental objectives to protect the nation's most critical technologies and information.

In his remarks, Payne described walking in to direct an agency that had an incredible workforce. "I had an extraordinarily talented workforce that was about as dedicated and hard working as I had ever seen. Their sense of mission and willingness to do whatever it took to complete the mission was unparalleled," Payne said. "I couldn't have walked into a better organization."

Payne noted that DSS and now DCSA had been lucky to have the right leaders at the right time. "When Kathy Watson took over as Director, DSS was on the verge of extinction. Kathy Watson put DSS on solid footing, was able to secure the budget, demonstrate the importance of DSS, and begin growing it. She was the right leader at the right time.

"When Stan Sims arrived, Stan added some structure to DSS, truly professionalized the organization and began to grow a partnership with industry. Again, the right leader at the right time," Payne continued.

"As I look at my three years here, my contribution was to change the direction of the ship, get DSS looking at the protection of critical technology in a different light, implement new methods of doing business, and most importantly ensure that the workforce and industry clearly understood the importance of our mission and the necessity of being successful. I hope that I have accomplished that," he said.

Payne then looked to the future of DCSA and predicts an organization that will be unrecognizable three years from today. "I look at all of the new programs and ideas that are being designed now and the things that are on track for implementation. Those programs that are being developed right now will change the way we protect critical technology profoundly and will put us in a far better place to protect our weapons systems from our adversaries," he said.

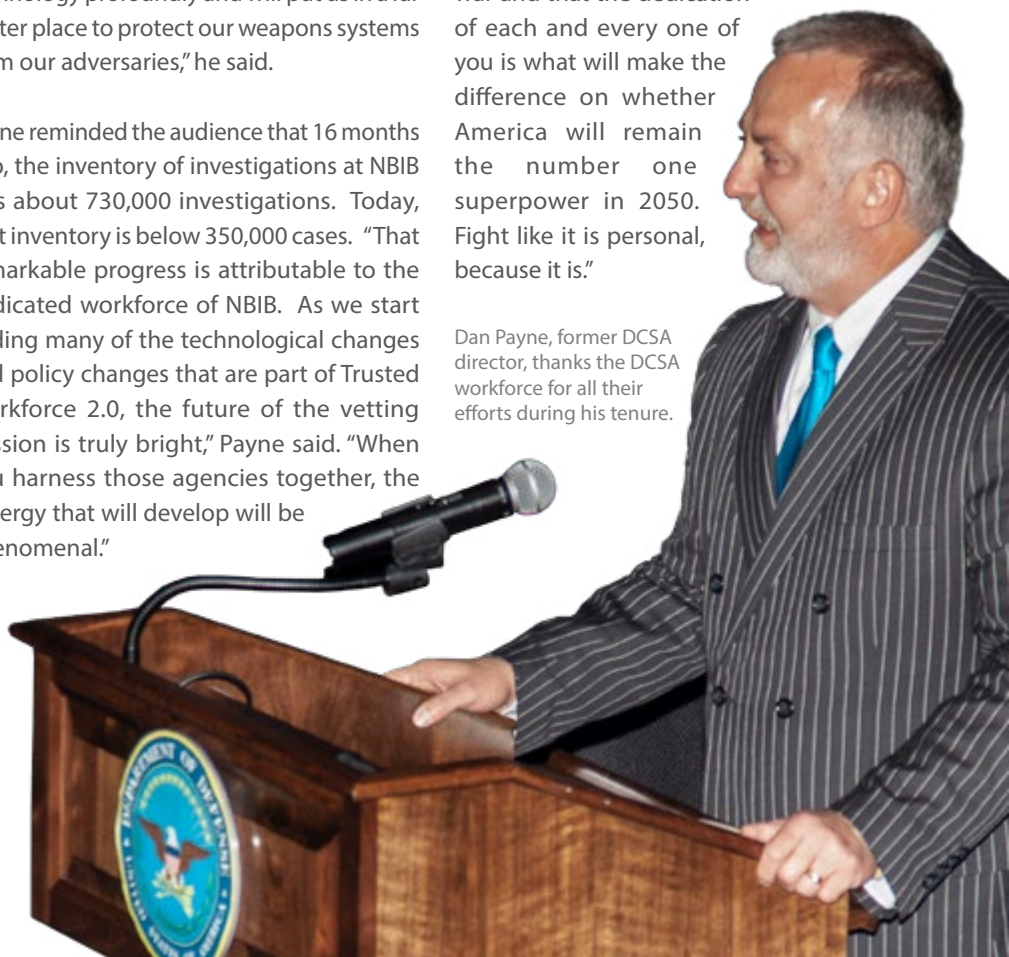
> **"Never forget that we are in the war before the war and that the dedication of each and every one of you is what will make the difference on whether America will remain the number one superpower in 2050."**

Payne reminded the audience that 16 months ago, the inventory of investigations at NBIB was about 730,000 investigations. Today, that inventory is below 350,000 cases. "That remarkable progress is attributable to the dedicated workforce of NBIB. As we start adding many of the technological changes and policy changes that are part of Trusted Workforce 2.0, the future of the vetting mission is truly bright," Payne said. "When you harness those agencies together, the synergy that will develop will be phenomenal."

"From a leadership standpoint, we couldn't ask for a better leader to get this new Agency rolling than Charlie Phalen," said Payne. "Over the years, Charlie has demonstrated time and time again to be the calming voice in the crowd, the rational decision maker, and the person you can depend on to speak the truth. DCSA is lucky to have Charlie as its SECOND Director!"

Payne closed by addressing the DCSA workforce. "Never forget the importance of our mission and the importance of your role in protecting this country. Never forget that China has vowed to overtake the United States militarily and economically by 2050. Never forget that the keys to modernizing China's military lies with the secrets and critical technology developed by and housed in industry and academia. Never forget that as a result, securing cleared industry and academia IS the tip of the spear. Never forget that our adversaries will continue to try to steal our secrets through people and that ensuring that our workforce can be trusted is of vital importance to the protection of our nation.

"Never forget that we are in the war before the war and that the dedication of each and every one of you is what will make the difference on whether America will remain the number one superpower in 2050. Fight like it is personal, because it is."



Dan Payne, former DCSA director, thanks the DCSA workforce for all their efforts during his tenure.

# DCSA HONORS THE BEST IN INDUSTRIAL SECURITY; 51 FACILITIES RECEIVE COGSWELL AWARDS

**by Beth Alber**
*Office of Public and Legislative Affairs*

On June 12, 2019, the Defense Counterintelligence and Security Agency presented the annual James S. Cogswell Outstanding Industrial Security Achievement Award to 51 cleared contractor facilities during the 55th annual NCMS training seminar in St. Louis, Mo. The Cogswell awards represent the "best of the best," and the winning facilities' security programs stand as models for others to emulate. These 51 facilities represent less than one-tenth of one percent of the approximately 12,500 cleared facilities in the National Industrial Security Program (NISP).

Each year, DCSA partners with NCMS to host the Cogswell Award presentations during its annual training seminar. DCSA Director Dan Payne noted, that for 55 years, NCMS has been delivering security education and providing training forums that align with DCSA; has been bringing security professionals together to learn from each other; and has been building bridges between government and industry security professionals. "NCMS and DCSA have had a long-standing relationship since NCMS' establishment," Payne said, "and we want to continue to maintain this relationship with the hope of impacting our nation in a greater way."

The Cogswell Award was established in 1966 in honor of the late Air Force Col. James S. Cogswell, who articulated the underlying principle of the Industrial Security Program -- the need for a true partnership between industry and government to ensure the protection of classified information, materials, and programs.

During his remarks, Payne described the Cogswell selection process as rigorous. The process begins with a DCSA Industrial Security Representative who nominates a facility. That facility must have achieved two consecutive superior ratings just to be considered for the award. "This just gets you in the door, but demonstrates a consistent, committed program over time," Payne said.

Once nominated, the facility enters an eight-month DCSA internal review process that includes a National Review Team of DCSA Regional Directors and representatives from across DCSA who consider each nomination. The National Review Team vets all nominations with 57 external agencies and makes recommendations to DCSA senior leadership for a final decision based upon the following criteria:

- ☆ Overall security program
- ☆ Security education and awareness
- ☆ Senior management support
- ☆ Facility Security Officer (FSO) and security staff level of experience
- ☆ Security vulnerability assessments
- ☆ Classified material controls

In closing, Payne said, "The rigorous selection process shows you just how hard it is to achieve this honor and the significance of the achievement. It demonstrates the commitment of the awardees in maintaining the highest standard in securing our nation's assets."

Congratulations to the 2019 Cogswell Award Winners!

**AM General, LLC**
South Bend, Ind.

**Applied Research Laboratories, The University of Texas at Austin**
Austin, Texas

**ARC Technologies LLC, a Hexcel Company**
Amesbury, Mass.

**Auburn University**
Auburn, Ala.

**BAE Systems, Inc.**
Arlington, Va.

**BAE Systems Land & Armaments LP**
Minneapolis, Minn.

**BAE Systems Land & Armaments LP**
Sterling Heights, Mich.

**BAE Systems Land & Armaments LP**
York, Penn.

**BAE Systems Technology Solutions & Services, Inc.**
Fort Walton Beach, Fla.

**BioFire Defense, LLC**
Salt Lake City, Utah

**CAE USA, Inc.**
Tampa, Fla.

**DCS Corporation**
Lexington Park, Md.

**Dynetics, Inc.**
Huntsville, Ala.

**EDO Western, Harris Corporation**
Salt Lake City, Utah

**Engility, a wholly owned subsidiary of SAIC Company**
San Bernardino, Calif.

**Esri**
Vienna, Va.

**Hydroid, Inc.**
Pocasset, Mass.

**L3 ForceX**
Nashville, Tenn.

**L3 Technologies, Broadband Communications Sector, Communication Systems-West**
Salt Lake City, Utah

**L3 Technologies, Sonoma EO**
Santa Rosa, Calif.

**Leonardo DRS – Advanced Acoustic Concepts, LLC**
Hauppauge, N.Y.

**Leonardo DRS, Inc.**
Arlington, Va.

**Leonardo DRS – Naval Power Systems, Inc.**
Danbury, Conn.

**Leonardo DRS – Network & Imaging Systems, LLC**
Melbourne, Fla.

**Lockheed Martin Corporation, Enterprise Business Services**
Denver, Colo.

**Lockheed Martin Missiles and Fire Control Autonomous Systems**
Littleton, Colo.

**Lockheed Martin Rotary and Mission Systems**
Burlington, Mass.

**Lockheed Martin Rotary and Mission Systems**
Littleton, Colo.

**Lockheed Martin Rotary and Mission Systems, Clearwater, Fla., Operations**
Oldsmar, Fla.

**MZA Associates Corporation**
Albuquerque, N.M.

**nou Systems, Inc.**
Huntsville, Ala.

**Oceaneering International, Inc.**
Hanover, Md.

**Peraton, Inc.**
Greenbelt, Md.

**Pinnacle Solutions, Inc.**
Huntsville, Ala.

**Raytheon Company**
Richardson, Texas

**Raytheon Missile Systems**
Tucson, Ariz.

**Retlif Inc. dba Retlif Testing Laboratories**
Ronkonkoma, N.Y.

**SAIC**
Arlington, Va.

**SAP National Security Services, Inc.**
Newtown Square, Penn.

**Sauer Compressors USA**
Stevensville, Md.

**SciTec, Inc.**
Princeton, N.J.

**SI2 Technologies, Inc.**
Billerica, Mass.

**Signature Research, Inc.**
Navarre, Fla.

**Smiths Interconnect, Inc.**
Tampa, Fla.

**SubCom, LLC**
Eatontown, N.J.

**TenCate Advanced Armor USA, Inc.**
Goleta, Calif.

**The Aerospace Corporation**
Arlington, Va.

**The MITRE Corporation**
Lexington Park, Md.

**Transoceanic Cable Ship Company, LLC**
Baltimore, Md.

**Ultra Electronics – USSI**
Columbia City, Ind.

**Vertex Aerospace LLC**
Madison, Miss.

## IN THEIR OWN WORDS

A representative sampling of the 2019 Cogswell winners were invited to share their formula for success with ACCESS readers. The following are tips and lessons learned from facilities with proven track records on how to establish and maintain a high quality security posture.

**by Zach Kierstead**, *Security and Compliance Coordinator*
**Ian Moss**, *Vice President, Compliance and Legal*
*Hydroid, Inc.*
*Pocasset, Mass*

## I AM REMUS

Hydroid, Inc. is located on Cape Cod in Pocasset, Massachusetts. The Hydroid team provides Autonomous Underwater Vehicles (AUVs) to foreign and domestic militaries, expeditionary companies, and universities around the world. Our REMUS technology supports marine research, search and salvage missions, field mapping, and mine countermeasure operations. We are proud that our technology plays a key role in protecting the lives of our nation's warfighters.

We are humbled to be chosen as recipients of the Cogswell Award from the Defense Counterintelligence and Security Agency. The recognition is testament to the hard work and dedication of not only the Compliance and Security Department, but to Hydroid as a whole.

## CREATING A SECURITY COMMUNITY

Hydroid works consistently with nearby contractors in the industry to establish a full view of current security threats. We have established a cyber working group, organized by the Department of Homeland Security (DHS), with other security personnel in the region to share firsthand threats and potential vulnerabilities.

Persistent threats are likely targeting an entire industry rather than a specific company, so coming together and sharing our experiences helps us to patch everchanging holes and to protect our intellectual property. Working directly with DHS allows us an inside look at current threat scopes that they consider realistic and particularly serious. The participants use the information to patch vulnerabilities and enhance their security programs.

**Persistent threats are likely targeting an entire industry rather than a specific company, so coming together and sharing our experiences helps us to patch everchanging holes and to protect our intellectual property.**

## MULTI-AGENCY COLLABORATION

Building relationships with government agencies, such as the Navy Criminal Investigative Service, the FBI, the DHS, and DCSA, allows us a direct line in any potential or actual emergency. These branches provide support and insight that help us overcome unfamiliar obstacles.

## AUDITS; THREATENING, BUT HELPFUL

Audits are widely known to increase stress levels within a business. From the time one is scheduled, employees rush to organize, strategize, and survive their audit. At Hydroid, we see audits as potential for program enhancements. Whether we are being evaluated by DCSA or by one of our customers, audits are seen in a positive light.

When a company provides honest information during an evaluation, they receive a high return on investment. Although threatening at times, the recommendations following an audit are always helpful. The feedback we receive is taken seriously and implemented in a timely manner. The longer the findings sit stagnant, the greater the chance that the recommendations will never be implemented. We always appreciate any opportunity we get to show our company's reliability and willingness to evolve.

## REALISTIC TIMELINES

For situations in which government or customer requirements change, Hydroid management has discussed setting realistic deadlines for project completion. Accounting for potential delays during the project planning stage avoids the need for dramatic restructuring during the implementation phase. This also relieves stress from employees that can be working with multiple deadlines at one time and allows time for preparation that is required when workflows are inevitably broken.

## IN CLOSING

We are honored to be accepting our first Cogswell award on behalf of all Hydroid employees. With a Security and Compliance Department of three, we would not be here if not for employee dedication to security excellence. We thank every member of Hydroid for creating a product that investigates, maps, and protects in support of our nation's warfighters and that functions for those organizations who continue to rely on REMUS technology around the world.

LEONARDO DRS

# 'CULTURE OF COMPLIANCE' KEY TO LEONARDO DRS SUCCESS

As the recipient of three Excellence in Counterintelligence awards and 11 James S. Cogswell awards for Outstanding Industrial Security Achievement over the past seven years, Leonardo DRS has clearly demonstrated its commitment to protecting national security and supporting the mission of the Defense Counterintelligence and Security Agency (DCSA).

Leonardo DRS understands that effective security requires a true partnership with DCSA and a comprehensive security program with a full organizational commitment that encompasses each of its key elements: industrial security, information security (cyber), physical security, insider threat and counterintelligence.

"We appreciate that our partners at the DCSA have a big job to do and that companies with strong compliance programs lighten the government's load," said John Hanfere, facility security officer of the corporate headquarters of Leonardo DRS. "Our security program is built on a foundation of strong cooperation with the DCSA with open lines of communication in furtherance of our common goals."

Leonardo DRS has instituted a 365-day readiness approach which it measures through continuous monitoring and established monthly milestones. The company develops and employs interactive security tools to foster information exchange and collaboration among security professionals and key stakeholders. DRS also looks outside the company and actively seeks external information, training tools and other resources from leading industry organizations like NCMS, the Center for Development of Security Excellence and the local industrial security awareness council. The overarching goal at Leonardo DRS is to far exceed baseline security requirements. "Our compliance program is championed by leadership, supported by education and training, and reviewed by peers," Hanfere said.

"At Leonardo DRS, our commitment to supporting our men and women in uniform extends beyond developing and producing advanced technology and cutting-edge products and systems. We bring a similar determination to protecting classified and other sensitive information, which if compromised, could potentially put the safety and security of our warfighters at risk and undermine our national security" said the company's Insider Threat Program Senior Official (ITPSO) and Executive Vice President and General Counsel Mark A. Dorfman.

> "Our security program is built on a foundation of strong cooperation with the DCSA with open lines of communication in furtherance of our common goals."
>
> John Hanfere
> *Facility Security Officer*

Hanfere states that the Leonardo DRS Security Program builds on the company's "culture of compliance" and commitment to security. He explains that it has flourished through its collaborative and passionate security professionals and other dedicated stakeholders. At the direction of senior leadership and under the oversight of the DRS Board of Directors and its Government Security Committee, the security leadership team builds a strategic plan to address the evolving security threat-scape. The senior team then sets and communicates clear metrics to ensure that the plan is appropriately implemented. The company's local security professionals are given training, tools and other support to help ensure that these objectives are met. Peer reviews are regularly conducted to identify gaps and propose solutions. And as a matter of routine, Leonardo DRS regularly reaches out to the DCSA for guidance and countermeasures when dealing with potential risks.

The company's security program promotes the sharing of best practices, counterintelligence threat information, and guidance covering Foreign Ownership, Control or Influence (FOCI) mitigation and facility clearance processes. As a result, Leonardo DRS has become recognized as an industry champion when it comes to information sharing among cleared defense contractors, and in particular, other foreign-owned defense companies that operate under FOCI mitigation agreements.

**by Cherea Adams,** *Facility Security Officer*
**Kathy Chamlee,** *Technical Writer/Editor*
*The MITRE Corporation*
*Lexington Park, Md.*

The MITRE Corporation is a not-for-profit organization that works in the public interest across federal, state and local governments, as well as industry and academia. We operate federally funded research and development centers that assist the U.S. government with scientific research and analysis, development and acquisition, and systems engineering and integrations. MITRE's mission-driven team is dedicated to solving problems for a safer world.

Receiving the Cogswell award underscores our commitment to this mission. Placing security as a top priority is critical to our nation's safety. The success of our security program can be attributed to several factors, including strong relationships with DCSA; management support; employee participation/buy-in; and intentional security education, training and awareness.

## PARTNERSHIP WITH DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

Regular communication with our DCSA representative, Nick Reynolds, has contributed greatly to the success of our program. We always feel respected and valued by Mr. Reynolds, and we appreciate his guidance and advice.

## MANAGEMENT SUPPORT

Management support is critical to a strong security program. Without management buy-in, many security efforts will be in vain. I am proud to say that our management places security high on the totem pole. They help influence and shape the security culture within our company. Their regular All-Hands meetings emphasize security and incorporate security education for our staff.

"The important work we perform across the National Security Sector demands attention to every detail at all times in order to protect our nation's critical information," said Tom Wright, manager of our Naval Aviation portfolio. "Our sponsors embrace us as their special trusted partners and have come to expect that our facilities, our staff, and our procedures meet or exceed security standards."

> **"The work that goes into each annual inspection is intense and requires extreme dedication to excellence, as well as patience."**
>
> Todd Maddox
> *Center for Programs and Technology's Naval Aviation Systems department*

"The work that goes into each annual inspection is intense and requires extreme dedication to excellence, as well as patience," said Todd Maddox, head of the Center for Programs and Technology's Naval Aviation Systems department.

Director of Global Security Services John Wojcik added that the award is "the highest recognition of our efforts to emphasize the importance of security in all aspects of our mission."

## EMPLOYEE PARTICIPATION

If our employees did not actively engage in our security program, it would not be effective. To obtain Superior ratings, our employees must be engaged and compliant with policies, procedures and reporting obligations, such as adverse information and/or insider threat concerns. They willingly participate in staff interviews during our quarterly self-inspections to help us ensure our education efforts are effective. They stay vigilant and are willing to report any counterintelligence concerns they may encounter.

## INTENTIONALITY

Overall, achieving Superior ratings requires being intentional about security. We plan our security calendar for each year, including quarterly self-inspections, where we review all aspects of the security program, such as personnel security records, physical security requirements, classified holdings, and information security systems.

We invite speakers from various agencies to discuss topics of importance during periodic security seminars, and we provide tip sheets to staff to help with classified meetings, marking classified material, Controlled Unclassified Information handling, etc.

Our annual planning also includes enhancements, such as maintaining 100 percent classified holdings accountability, unannounced security inspections, mentoring programs, etc., all of which go above what the National Industrial Security Program Operating Manual requires. Without the team effort, Superior ratings would not be possible. It is such an honor to accept the Cogswell award on behalf of The MITRE Corporation – Lexington Park, Md.

**by Hazel Martinez**
*Director of Security*
*MZA Associates Corporation*
*Albuquerque, N.M*

MZA Associates Corporation was founded in 1991 and has become a world leader in the modeling, analysis, design, development, integration, and testing of High Energy Laser (HEL) and advanced optical systems. Headquartered in Albuquerque, New Mexico, with an office in Dayton, Ohio, MZA provides research and development services to defense and aerospace customers in support of advanced beam control systems, atmospheric characterization, and optical systems engineering. MZA provides unique expertise in the areas of wave-optics modeling, adaptive optics systems, and scientific data acquisition, analysis, and management.

My career with MZA began in May 2011. Already a seasoned security professional with 27 years of experience and one Cogswell under my belt from a previous employer, I immediately set a goal for MZA to receive the coveted James S. Cogswell Award. I knew very well I would need to maintain the strong partnership I had established with the Defense Counterintelligence and Security Agency over the years, ensure I was always informed and knowledgeable of the latest security processes and procedural changes, establish a strong security team, and cultivate a robust relationship with MZA senior management, consisting of communication and commitment.

## PARTNERSHIP WITH DCSA

Many years ago, while working as an administrative coordinator for a small defense contractor, I was approached by the technical director of that company to be their facility security officer (FSO). I did not have a clue what that meant, nor did I appreciate what I was getting myself into. I was provided with a security manual and directed by management to read it and make certain I followed the processes outlined. Shortly after, I made my first contact with DCSA. Initially, I was intimidated by their presence. This was due, in part, to the fact that I did not understand the information I was reading and did not know what to ask for in the way of support. It wasn't long before I realized that DCSA was there to "advise and assist;" a relationship grew from there. DCSA had a responsibility to ensure that our facility was in compliance with the Department of Defense (DoD) guidelines and it was up to me to learn the requirements and call on them for assistance when needed. DCSA has supported me from the beginning and the relationship has flourished over the years.

## SECURITY EDUCATION AND TRAINING

DCSA recommended that I pursue a membership in NCMS, a resource for learning and networking with other security professionals. Determined to be the best I could be, I did just that. Through networking, I learned there were a variety of educational courses offered for FSOs and I took full advantage of all that applied. As a result of my association with NCMS since 1987, and with the additional training accessible through the Center for Development of Security Excellence, I have learned to be one of the best in this profession. The key is to take full advantage of the training offered. The ongoing education has enabled me to keep up with the many changes that have taken place over the years.

## A STRONG SECURITY TEAM

While I have always had overall responsibility for the security programs wherever I was employed, I learned that it takes a team to build and maintain a winning program. Security has evolved over the years with many changes having occurred in every aspect of the process. Security excellence can only be achieved by selecting individuals who share in the importance of the mission and who have similar goals to be the best at developing a top security program. We have that and more at MZA.

## MZA SENIOR MANAGEMENT COMMITMENT TO SECURITY

Senior management's commitment to security excellence is absolutely essential for the success of a security program. Their involvement is critical to the mission. It is essential that management understands the threat and are willing to apply risk-management values that will aid in protecting our assets and the government's assets. As the security manager overseeing a program and a team, it simply would not be possible to operate without continued communication and commitment from MZA's senior management. This starts at the top with the President and continues on down with every manager in the organization.

## CONCLUSION

Partnering with DCSA, continued security education and training, maintaining a strong security team, and cultivating a robust relationship with senior management are the ingredients necessary to build and maintain a strong security program and, ultimately, to become the recipients of the James S. Cogswell Industrial Security Award. The mission is on-going and our work will never be complete as long as there is a single asset to protect.

RETLIF TESTING LABORATORIES

**by William K. Hayes,** *Executive Vice President/Facility Security Officer*
*Retlif Testing Laboratories, Inc.*
*Ronkonkoma, N.Y.*

Retlif has successfully held a facility security clearance for more than 30 years, and I have been its FSO the entire time. We have formulated a solid security program by building on smaller successes and by incrementally integrating the advances made at each step along the way.

We continually strive to apply what we have learned and to utilize the multiple self-inspections conducted between DCSA assessments to continue to ingrain and refresh them. This is an important part of Retlif's policies and procedures protocols.

An effective security education program is a direct result of our efforts to impress upon all Retlif employees that security is an integral part of everyone's job, and not something that only senior management and the facility security officer do.

Executive management support is essential. We consistently use guest speakers such as the FBI, Naval Criminal Investigative Service and DCSA Counterintelligence staff to present material on key topics applicable to our staff. These briefings are tailored to ensure that the message is clear and understood. After meetings, we encourage feedback from our staff regarding the impact and invite suggestions for further improvement. Most recently we have developed a testing regime to ensure that we are achieving success in this area.

We regularly apply DCSA training and resources to solve problems at our facility in an efficient manner. For example, we constructed special closed areas and secured the needed DCSA approval. These closed areas are used as radio frequency shielded enclosures employed by Retlif for its military-standard, electromagnetic interference/electromagnetic compatibility testing business. We used Retlif's in-house engineering and security resources to develop special locking mechanisms that comply with DCSA access requirements which did not conflict with the shielding effectiveness of the closed areas. During the process, we consulted with our local DCSA representatives to ensure that the access requirements were being met and we remained on track to obtain the needed approvals for these closed areas.

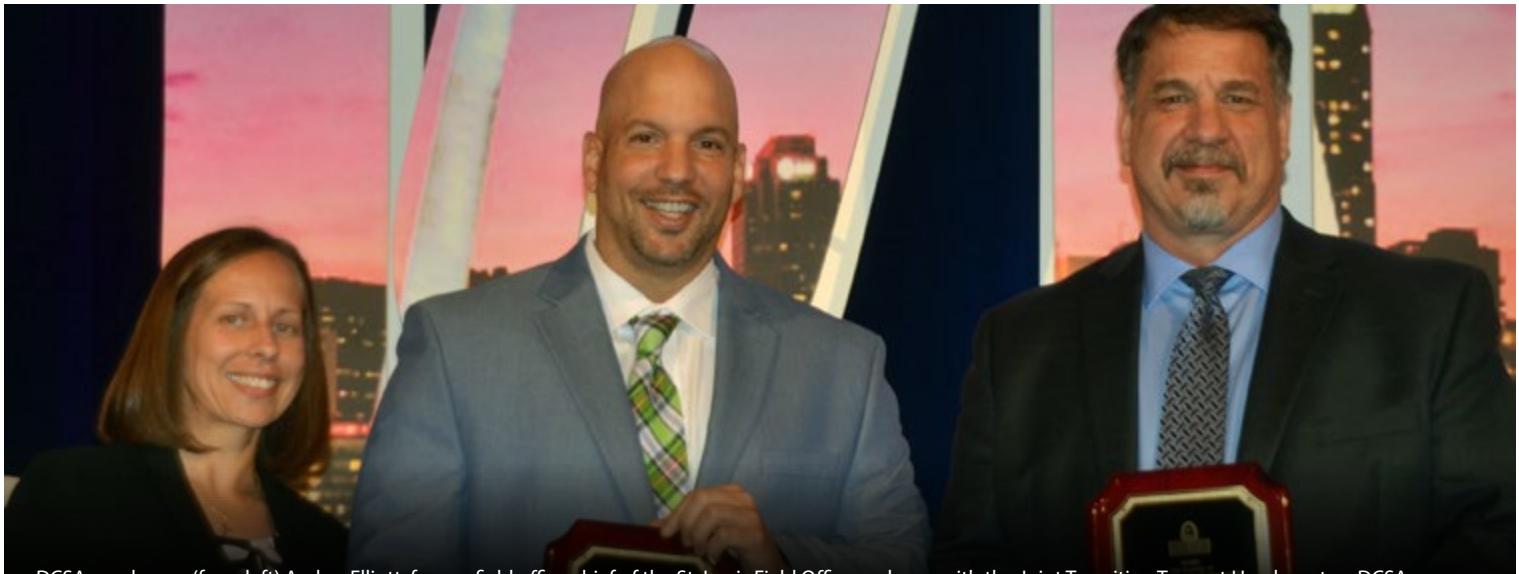
**Over the years, the collaboration with our assigned DCSA representatives have been the ingredient that pulls all the pieces together, resulting in our program success.**

Over the years, as Retlif progressed from Satisfactory ratings, through Commendable ratings, and then ultimately to Superior ratings, we have always stayed focused on implementing the standards of the Cogswell award. Retlif has maintained a process improvement philosophy in our approach to our security system. We also observe how others approach security issues, especially while visiting prime contractors and during government activities. By adapting what we learn to our needs, our ratings have climbed consistently.

Retlif prepares for DCSA assessments by maintaining an active readiness posture. We have had unannounced DCSA assessments, so essentially, we begin preparations for a subsequent visit once one has concluded. We have executed all the Center for Development of Security Excellence training available on the topic, we consult with industry peers, and we use the DCSA handbook to the maximum extent. Retlif management evaluates the effectiveness and scope of the effort.

Over the years, the collaboration with our assigned DCSA representatives have been the ingredient that pulls all the pieces together, resulting in our program success. Their frank commentary, insightful interviews of our staff and out-briefs of management make it all work. Their input is invaluable and compels us go the extra distance.

We have learned time and time again that comprehensive self-inspections are the primary tools to reveal emerging issues that need to be dealt with before becoming serious issues impacting safeguarding classified material.



DCSA employees (from left) Amber Elliott, former field office chief of the St. Louis Field Office and now with the Joint Transition Team at Headquarters DCSA; Salvatore Urbano, senior industrial security representative in the St. Louis Field Office; and Raymond DuVall, counterintelligence special agent in the Tacoma Field Office; hold their industrial security awards at NCMS. (Photo by Chris Gillis, NBIB)

# DCSA EMPLOYEES RECEIVE AWARDS AT NCMS TRAINING SEMINAR

During this year's annual NCMS training seminar, three DCSA employees received Industrial Security Awards:

**Raymond DuVall**, counterintelligence special agent in the Tacoma Field Office, received the award for his support to the Pacific Northwest.

**Amber Elliott**, former field office chief of the St. Louis Field Office and now with the Joint Transition Team at Headquarters DCSA, received the award for her efforts in the greater St. Louis area.

**Salvatore Urbano**, senior industrial security representative in the St. Louis Field Office, received the award for his support of NCMS.

The Industrial Security Award is presented to an individual or organization that has significantly contributed to industrial security and meets a minimum of two of the following criteria:

- Individual or organization that has materially and beneficially affected the security community (e.g., functional areas include education, training, operations or like activities which improves or enhances individual, organizational or corporate performance);
- Individual or organizational contribution which improves security procedures, practices or policies of national interest (e.g., develop partnerships between industry and government, involvement in ISACs, industry teams, etc.);
- Individual or organization continuing contributions to the Society by enhancing the mission, vision, and goals of the Society;
- A member or associate member in good standing.

**Raymond DuVall**

DuVall acted as mentor, collaborator, and advocate for the Pacific Northwest industrial security community. His tireless efforts ensured the industrial security community received a variety of support, to include providing training on any subject (with and without notice), sharing his expertise and encouragement, especially if it involves being our advocate within our companies, and facilitating communication between industry and government.

**Amber Elliott**

Elliott is a former facility security officer and a founding member of Chapter 50, The Greater Saint Louis NCMS Chapter. Under her leadership since joining DCSA, there has been a DCSA presence at every NCMS chapter meeting. Elliott was instrumental in building a collaborative relationship between NCMS and DCSA, which has led to a true "open door" policy that includes hosting meetings at the DCSA office to address specific topics of concern. Due to her efforts, the local security community is prepared to face the many changes taking place within the National Industrial Security Program at this time.

**Salvatore Urbano**

Urbano provided unparalleled service to countless cleared defense contractors, and is typically the first to provide updates on changing policy at chapter meetings or at one-on-one meetings with facility security officers. His goal is to ensure that the partnership between industry and DCSA remains strong. Urbano worked diligently to repair the local relationship between government security managers and industrial security officers, and his effort resulted in regular attendance at joint meetings as well as improved security programs for on-base contractors. His willingness to support all facility security officers, whether assigned to him or not, has resulted in improved security ratings and a prolific exchange of best practices. He provided constant support and guidance, which was invaluable to the industrial security community.

# DCSA EMPLOYEES SUPPORT ANNUAL NCMS SEMINAR

**by Christopher P. Gillis**
*National Background Investigations Bureau*

(From left) Ryan Deloney, Larissa Caton, and Lauren Firich, all from Industrial Security Field Operations, manage the National industrial Security System (NISS) help desk area.

On an annual basis, NCMS holds a seminar attended by hundreds of security professionals, which features a variety of guest speakers, workshops and training sessions. Each year, the Defense Counterintelligence and Security Agency (DCSA) recognizes the James S. Cogswell Outstanding Industrial Security Achievement Award winners during the seminar. This year, as in years past, DCSA employees provided a variety of support at the 55th Annual NCMS Training Seminar held in June in St. Louis, Mo.

Retired U.S. Air Force Capt. Scott F. O'Grady kicked off the training seminar as the first keynote speaker and told the story of his real-life experience of how he survived in hostile territory for six days before being rescued by U.S. military personnel. O'Grady ended his presentation by providing his views on the importance of the work that industrial security personnel perform every day.

"I'm thinking about this, looking at you, going—this is a group of security professionals that has a professional duty to protect," O'Grady said, noting the cross section of industrial security professionals in attendance at the seminar's general session.

"You protect lives, fortunes and the pursuit of happiness as Americans and Americans' way of life," he said. "So that all Americans can live prosperously and at peace, and free--and that, to me, makes you all heroes in your profession."

DCSA Director Dan Payne opened the seminar's second day as the keynote speaker, where he unveiled the seal of the DCSA, which will be comprised of various entities to include the personnel of the National Background Investigations Bureau.

Payne encouraged the industrial security community to continue the hard work and persistence of its day-to-day operations, as DCSA works to continue to change the paradigm on acquisitions to better support the mission.

"Security is no longer something that cost the company. Security is something that can make that company money," Payne said. "Security can potentially win you contracts."

Payne highlighted the fact that the battlefield today is very different from past challenges, especially in the area of critical technology protection. Industrial security professionals are on the front lines of the battlefield and must stay vigilant.

"That's where all of you come in; all of you play a significant role in protecting our national security and protecting the economic well-being of your company," Payne said, about the current U.S. national security challenges, defense and its global economic standing.

"We're in a battle; one that most in the United States don't know is happening, don't recognize it's going on, but it is a battle we can't lose," he concluded.

DCSA representatives spoke at several seminar workshop sessions on the following topics:

- The DoD Consolidated Adjudication Facility/Vetting Risk Operations Center
- Evaluating Insider Threat Programs
- Defense Security Service-in-Transition (DiT) 2.0
- Transition Transformation
- Best Practices in Asset Identification
- Industry and DCSA Collaboration: Working With Your DCSA Representative
- Navigating the Risk Management Framework (RMF) Process and the NISP eMASS
- NISP Authorization Office Update and RMF Tips
- NISP Contract Classification System (NCCS) Update

DCSA also provided four help desk stations for NCMS attendees during the seminar to assist them with any challenges they might be experiencing in relation to personnel security clearances, the RMF, or the National Industrial Security System and the NCCS.

# A Q&A WITH EDWARD (NED) FISH & MARIANNA MARTINEAU

Editor's Note: In this issue, we focus on the move of the DoD Consolidated Adjudication Facility (CAF) to the Defense Counterintelligence and Security Agency. Edward (Ned) Fish, is the former director of the CAF and now the deputy director of the Defense Vetting Directorate. Marianna Martineau is the acting director of the CAF. We invited both to tell us about their respective roles as well as introduce the CAF to the DCSA workforce.

**Edward (Ned) Fish** was appointed to the Senior Executive Service in 2013 to serve as the first director of the DoD CAF. On May 13, 2019, he assumed the duties of the deputy director of the Defense Vetting Directorate (DVD) under which the CAF falls. Fish retired from the U.S Army as a Colonel in January 2013 after nearly 28 years of service. He graduated from The Citadel and served in Armor units as platoon leader, executive officer, and Battalion intelligence officer. He served in increasingly responsible command and staff Military Intelligence positions culminating as the commander, U.S. Army Central Clearance Facility, Fort Meade, Md. His other Military Intelligence assignments included: 66th Military Intelligence Brigade; Defense Intelligence Agency; chief, Intelligence Planner and chief, Intelligence Operations Center, Intelligence Directorate, European Command; deputy Corps Intelligence and chief, Corps Intelligence All-Source Center, NATO Rapid Deployment Corps – Spain; and deputy chief of staff for Intelligence, Force Strategic Engagements Cell, Multi-National Forces – Iraq.

**Marianna Martineau** is the acting director of the CAF. She previously held the positions of CAF deputy director and Operations Division chief. Prior to joining the CAF in 2015, she served as the deputy chief of staff and Resource Management Division director at U.S. Marine Corps Forces Cyberspace Command, and the director of Business Operations and Management Division at the Defense Manpower Data Center. Prior to returning to federal service in 2010, Martineau worked in cleared industry for nearly eight years in roles of increasing size, complexity and responsibility. She also served as an Air Force Contracting Officer. Martineau earned a Bachelor of Science degree in Management and Computer Information Systems from Park University and a Master of Business Administration and Technology Management degree from University of Phoenix. She is a Syracuse University National Security Fellow and maintains numerous professional certifications including the Defense Acquisition Workforce Improvement Act Certifications in Program Management, Contracting and Procurement; OPM LEAD Executive Program Certification, and the Project Management Institute's Project Management Professional Certification.

**Q Tell us about your background and what led you to this position?**

**A Fish**: I spent almost 28 years in the Army, first in the Armor Corps and then Military Intelligence. My last assignment on active duty was as commander of the Army Central Clearance Facility (CCF). During my tenure as an Army officer, I had the honor of serving our great nation while stationed at multiple locations across the United States and around the world. In 2012, as I contemplated transitioning out of the Army, the Deputy Secretary of Defense directed the consolidation of seven of the 10 Department of Defense Adjudication Facilities into the DoD CAF (Army, Navy, Air Force, Joint Staff, Washington Headquarters Services, Defense Security Service, and the Defense Office of Hearings and Appeals.) I applied for the job, was selected, retired from the Army, and was installed as the first director on Feb. 4, 2013. It was my privilege to serve as the director of the DoD CAF for over six years. As the employees well understand, our enterprise is experiencing a period of great growth, mission expansion, change, and opportunity as we establish the newly designated Defense Counterintelligence and Security Agency (DCSA). Given those changes, on May 13, 2019, I shifted by my duties from CAF director to serve as the deputy director, Defense Vetting Directorate (DVD). Simultaneously, Marianna Martineau transferred from being the deputy director, DoD CAF, to serve as its acting director.

**Q Can you describe your new role at DVD as the deputy director?**

**A Fish**: As the deputy director, DVD, my primary task is to assist the director, Patricia Stokes, in doing whatever it takes to establish the preeminent vetting organization in the world. Once the current DVD is fully established, through both the hiring of personnel and the transfer/realignment of personnel from various organizations to include the DoD CAF and elements of the National Background Investigations Bureau (NBIB), it will consist of just under 1,500 civilians, nine military, and a significant number of contractor personnel. The DVD is a large, dynamic, and multi-faceted organization and we are fortunate to have so many fantastic personnel vetting professionals within its ranks today, and ready to join tomorrow. In addition to the normal duties expected of a deputy, I am also responsible for overseeing key operational elements within the DVD. These include the Vetting Risk Operations Center (VROC), the current NBIB Quality Oversight Division, the Federal Investigative Records Enterprise (FIRE) and the CAF. In addition, NBIB's Integrated Counterintelligence and Support Activity and the recently established Expedited Screening Center further reinforce the array of capabilities within DVD.

**Q Tell us about your background and what led you to this position?**

**A Martineau**: I have served in a variety of different position including uniformed military service, private industry, and federal civilian service. I held positions of increasing scope and responsibility across contracts, business, resource and project management disciplines. Since returning to federal service in 2010, I worked at the Defense Manpower Data Center, U.S. Marine Corps Forces Cyberspace Command, and the DoD CAF. At the CAF, I served first as the Operations Division chief focused on supporting adjudications; then as the deputy director and now as acting director.

**Q Can you describe your new role as the acting director, DoD CAF?**

**A Martineau**: As the acting director, I prepare the CAF for current and future changes in the personnel vetting enterprise while working toward achieving a steady state for the adjudicative inventory. To do this, my leadership team and I work together setting strategic goals and objectives, leading change initiatives including reorganization planning, communicating to and with our customers, and improving the quality and efficiency of adjudicative operations.

**Q Many people in DCSA don't know much about the CAF. Can you tell us a little about the CAF and the people who work there?**

**A Martineau**: The CAF is the federal government's largest clearance adjudication organization processing over 1 million personnel security actions annually. We render adjudicative determinations for the DoD (non-IC components), Judiciary, Congressional staff members, and contractor personnel under the National Industrial Security Program (NISP), which covers about 85 percent of all cleared government and industry personnel. To execute this mission, the CAF is staffed with approximately 650 government civilian employees and nine uniformed Air Force personnel. Our adjudicative staff obtain and maintain the Adjudicator Professional Certification under the Security Professional Education Development program, and many also maintain the Due Process Credential.

**Q Many people understand the investigative process; we all have to fill out an SF-86. But most of the adjudication is done behind the scenes. What does an adjudication involve?**

**A Martineau**: An adjudication is a determination, rendered by a certified adjudicator, using the 13 Federal Adjudicative Guidelines, to determine whether an individual is reliable, trustworthy and loyal for eligibility to access our national security information, systems, facilities, or other resources. Adjudicators use the "whole person" concept meaning we review disqualifying conditions and steps an individual may have taken to mitigate those concerns. An adjudicator is not a judge and normal criminal standards of "beyond a reasonable doubt" or civil standards of "preponderance of evidence" do not apply. All adjudicative determinations are made in the best interests of national security.

If the adjudicator can make a favorable decision at the initial review, he/she does so. Otherwise, adjudicators may request additional reviews or seek subject matter expert support for added information. If a favorable decision remains unachievable, the adjudicator initiates due process (denies or revokes the security clearance). Adjudication is a team sport and we leverage our complete team (CAF, VROC, NBIB, DITMAC and others across the DoD and beyond) in making complex decisions; we want the right decision based on all available information and expertise.

**Q Not only is the CAF set to move to DCSA, but many of the existing procedures and processes are changing as well. Can you describe some of the changes under way at the CAF?**

**A Martineau**: As previously mentioned, we are involved in a three-stage process at DCSA. The first is transfer and that includes all assets and resources of the CAF to DCSA, which will be completed on Oct. 1, 2019. In conjunction with this move, we are also reorganizing the CAF for efficiency and task alignment while running multiple Lean Six Sigma projects to streamline our adjudicative business operations. We are transitioning the end-to-end personnel vetting process to the Trusted Workforce 2.0 model. We are integrating new tools, updating processes and procedures, extending our team to encompass all of the new DCSA, and ensuring we are executing best of breed security practices. Overall, it is an exciting time at the CAF and our workforce is engaged and very responsive.

**Q The CAF was established in 2012 from disparate adjudication organizations. What did you learn from that experience that applies to the current move to DSS and ultimately DCSA?**

**A Fish**: Anytime you have a consolidation or merger, it is essential that leadership take care of the people. A successful transfer means employees are paid, their benefits are in place, their information technology tools work, and they are thereby "armed and ready" to accomplish all tasks and missions set before them. I have been continually impressed by the fact that, throughout the planning and execution of the on-going transfer activities, it has been evident to me that "the people" are an enduring priority to the DCSA and NBIB leadership. Knowing that this will be a continued priority for the leaders of the newly established DCSA, I am confident that we will subsequently realize the improvements and efficiencies needed in our end-to-end processes.

**Q What is the most significant challenge you see facing DVD moving forward?**

**A Fish**: In my opinion, the most significant challenge facing the DVD is in collaborating with the Program Executive Office (PEO) for the National Background Investigations Service (NBIS), in both a timely and effective manner, as we partner to design, develop, deliver, and deploy the NBIS that is so critical to the future success of our entire enterprise. The NBIS will be a true "end-to-end" system that will enable all facets of our business and provide for submission of requirements, investigations, analysis, screening, adjudication, security management, and more. We are fortunate to have key leaders for the DVD's Enterprise Business Support Office (EBSO) and NBIS PEO, respectively. They, and their team of professionals, have already forged a strong partnership and are fully engaged in creating NBIS as our "system of dreams." That said, much work remains to be accomplished as we move forward in this process.

**Q What is the most significant challenge you see facing the DoD CAF moving forward?**

**A Martineau**: The most significant challenge facing the CAF is keeping pace with change while increasing adjudicative production to achieve a healthy or steady state inventory. We are laser focused on eliminating inefficiencies and supporting our streamlined business processes with expanded information technology capabilities. Simultaneously, we are working with our leadership to prepare for Trusted Workforce 2.0 and the population expansion in Continuous Vetting. The CAF workforce is up to the many challenges.

**Q Any final thoughts?**

**A Fish**: Communicate, communicate, communicate, and then communicate some more! Communication is never merely top-down. Effective communication is also bottom-up, horizontal, and is part of the culture of any truly adaptive organization. As a team, we are establishing the DCSA as a new, large, and dynamic organization that is essential to our nation's future security and prosperity. We are at a critical time in history when an organization with DCSA's capabilities is critical to meet our nation's "clear and present" security needs. We cannot "over" communicate as we seek to successfully transfer, transition, and transform to meet these needs.

**Q Any final thoughts?**

**A Martineau**: As we continue our integration into the DVD portfolio, I am very excited and inspired by the new possibilities for our future. As an integrated team, we are creating efficiencies that were previously limited by organizational boundaries. The DoD CAF and our DVD partner organizations are mapping our new integrated business processes, removing duplications of effort and filling gaps. The new opportunities for our workforce to cross train in other security disciplines is another big plus. I know the CAF workforce is eager to learn more.

The eighth annual Director Awards ceremony, held in April, recognized those employees who exhibit the highest standards of excellence, dedication, and accomplishment in advancing the agency's mission during the calendar year. Awards were presented for Employee of the Year; Employee of the Year Senior; Team of the Year; Excellence in Innovation of the Year; and Humanitarian of the Year.

# EMPLOYEES, TEAMS RECEIVE RECOGNITION AT

In his opening remarks, DCSA Director Dan Payne reflected on his first experience with the event. "Three years ago, I presented my first Director Awards with only two weeks in the job. I didn't know much, but I remember thinking, what a fantastic way to recognize employees. I was happy to see it then, and am pleased to see the tradition continue.

"Fast forward to today, and a lot has changed," he continued. "We are fundamentally changing the organization – what it is, what it does, its name. It is important that we recognize our personnel during this period of transition. That we recognize our employees and show them that their work is vital to the agency's overall success. And to the nation's success.

"The Director Awards Program embodies attributes that shine a light on the great work we accomplish every day; it validates the impact our products and services provide to both industry and the community; and conveys our work ethics and dedication to the mission," he said.

"Whether you were an award recipient or an award nominee, you competed among a group of highly competitive employees and teams, and this program is a win-win for us all," he continued. "As managers and leaders of DCSA, we should continue taking a vested interest in the recognition of our workforce by supporting the Director Awards Program, which inspires, motivates, and encourages the highest levels of performance excellence."

## EMPLOYEE OF THE YEAR

The Employee of the Year award is presented to the DCSA 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 2018 is Twana Harper, Office of Acquisitions.

Harper provided outstanding and skilled contracting support throughout 2018, saved DCSA over $400,000, and helped the Office of Acquisitions streamline processes, enabling early close-out of the fiscal year. While acquiring subject matter expertise to support development, operations, and maintenance for DoD Insider Threat Management and Analysis Center multi-domain database platform, Harper conducted multiple rounds of negotiations and saved the government $325,000.

Furthermore she negotiated a $100-per-hour reduction to the program manager's labor rate, saving an additional $75,000, bringing total contract savings attained for her customer, due to her shrewd bargaining skills, to more than $400,000.

## EMPLOYEE OF THE YEAR SENIOR

The Employee of the Year Senior award is presented to the DCSA employee who exhibits the highest standards of excellence, dedication, and accomplishment in support of advancing the DCSA mission. The winner of Employee of the Year for 2018 is Rebecca Morgan, Center for Development of Security Excellence.

Morgan forged strategic partnerships within the Intelligence Community, DoD and with non-title 50 agencies through extensive strategic engagement and marketing. She expanded awareness of the DCSA counterintelligence and insider threat training and awareness resources through a highly-effective marketing campaign to include social media.

She successfully led the development of over 60 counterintelligence and insider threat products accessed by more than one million users. These products included eLearning courses, micro-learn webinars, job aids, awareness posters, videos, case studies, games and the CI and insider threat vigilance video series to provide greater flexibility and train-the-trainer capability for customers. She also led the way for the development of behavioral analytics and cyber eLearning training.

Morgan collaborated with many stakeholders, both internally and externally to CDSE. Her collaboration led to the successful development of over 60 CDSE products. Her collaboration with the National Insider Threat Task Force contributed to the development of the first-ever insider threat certification examination and enabled millions of users to access relevant and high quality CI and insider threat awareness training products online. Her efforts have contributed to DCSA and CDSE receiving numerous accolades to include the Horizon and Omni training awards.

## 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 DCSA mission. The 2018 Team of the Year is Team San Diego, Industrial Security Field Operations.

The San Diego Field Office and Hawaii Resident Office truly understand and implement the intelligence-led and asset-driven risk strategy, and their performance in 2018 clearly demonstrates their tenacity and skill. The offices completed 100 percent of their priority 1 and 2 comprehensive security reviews, enhanced security vulnerability assessments (SVA), and targeted SVAs. The offices identified and corrected 210 vulnerabilities and received over 1,700 reports from industry. This reporting resulted in the identification of 13 subjects or sources, four disruptions of foreign collection activity, and 146 referrals to law enforcement or intelligence community partners.

The team represents DCSA values and has provided outstanding innovation and commitment to protecting the warfighter.

## 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 winner of the 2018 Excellence in Innovation of the Year is the Other Transaction Agreements (OTA) Process Team. The Office of Acquisitions and the Office of General Counsel collaborated to develop policy and procedures which provided a new and innovative acquisition tool, giving DCSA the ability to capture emerging and pioneering technology from the commercial marketplace.

The OTA Process Team crafted and implemented the "commercial solutions for prototyping procedures" to capitalize on special authorities granted for procurement of technological or process prototypes. The new OTA method enables DCSA to solicit solutions in response to problem statements

**2018 TEAM OF THE YEAR/TEAM SAN DIEGO:**

**Timothy Barnes**
**Shawn Case**
**David Cohen**
**Lisa Dearmin**
**Rick Disney**
**Dominic Flax**
**Thomas George**
**Michelle Montoya**
**Jared Ostertag**
**Stefan Rodrigues**
**Derek Sinclair**
**Ehren Thompson**
**Mitchell Wells**

**TOP:** Employee of the Year Twana Harper (right), Office of Acquisitions, stands with DCSA Director Dan Payne. **MIDDLE:** Employee of the Year Senior Rebecca Morgan (right), Center for Development of Security Excellence, stands with DCSA Director Dan Payne. **BOTTOM:** Members of the 2018 Team of the Year, Team San Diego, Industrial Security Field Operations, stand with DCSA Director Dan Payne. (Photos by Marc Pulliam, CDSE)

and remove lengthy federal acquisition processes to move quickly to negotiation and award of contracts that capture innovative technologies and processes to enhance operational efficiencies, address immediate program issues, and solve problems.

The OTA procedures make it possible to begin procurement before the work is defined, drawing on the unique knowledge and capabilities in the marketplace to collaborate in shaping solutions as part of the process. The highly flexible nature of the new OTA process ensures DSS has a truly 'out of the box' strategy to capture new ideas from industry, and capitalizes on flexibility and collaboration to propel those ideas to viable application.

## 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 must demonstrate significant leadership and outstanding volunteer service accomplishments and must hace 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 2018 Humanitarian of the Year award is awarded to Casey Edge, Virginia Beach Field Office, for his volunteer outreach efforts; Mark Failer, Office of the Chief Information Officer, for his support to his local community as a volunteer fire fighter and certified emergency medical technician (EMT); and Timothy Hulub, Andover Field Office, for improving the quality of life of post-9/11 wounded war veterans.

**Casey Edge**

Edge demonstrated significant and inspirational leadership and commitment to veterans across three states as a volunteer outreach coordinator for the Warriors' Keep, which is an outdoor adventure therapy for veterans. In his leadership role, he secured dozens of sponsors while volunteering over 260 hours of personal time. Edge demonstrated tremendous collaboration as a critical leader and facilitator of the 2018 National Capital Region wounded veterans run, pursuing sponsorships, committing 330 hours of voluntary service and raising over $93,000.

**Mark Failer**

Failer received the award for continually showing his commitment to his local community by volunteering as a firefighter and certified EMT for over seven years. In his various volunteer roles, he has worked a minimum of 1,040 hours per year. Failer assisted in major and fatal car accidents, medical emergencies where lives were lost, and was involved in rescuing families from burning homes. When the fire department needed leadership to support a vice president role that had become vacant, he stepped up to the challenge and volunteered to take that role as well.

## 2018 EXCELLENCE IN INNOVATION/ OTHER TRANSACTION AGREEMENTS PROCESS TEAM MEMBERS:

**Jay Fraude and SoCheung Lee,**
*Office of the General Counsel*

**Stephen Heath and David Ragland,**
*Office of Acquisitions*

**Timothy Hulub**

Hulub's efforts contributed to improving quality of life and health to post-9/11 wounded war veterans. He organized a "partnership with industry" golf tournament, which has raised large sums of money, all of which is donated to assist wounded veterans. He teamed with the Northeast chapter of the Salute Military Golf Association (SMGA), whose goal is to help our nation's veterans and their families, including wounded, injured, and those suffering illnesses.

In September 2018, more than 140 industry, government and DCSA personnel participated in the tournament that included eight disabled SMGA members. The event raised more than $18,000. These proceeds will greatly further SMGA's goal of creating a therapeutic outlet for wounded veterans undergoing prolonged medical treatment. Locally, the SMGA has served more than 125 wounded veterans, individually fitted more than 46 sets of new Taylor-made golf clubs, and helped numerous golf clinics each year of which 92 percent of the wounded veterans reported it has helped improve their physical well-being.

**TOP:** Jay Fraude (left), Office of General Counsel, and David Ragland (right), Office of Acquisitions, members of the 2018 Excellence in Innovation of the Year winners, Other Transaction Agreements (OTA) Process Team, stand with DCSA Director Dan Payne. **BOTTOM:** The 2018 Humanitarians of the Year (from left), Mark Failer, Office of the Chief Information Officer; Timothy Hulub, Andover Field Office; and Casey Edge (far right), Virginia Beach Field Office, stand with DCSA Director Dan Payne.

## NOMINATED FOR EMPLOYEE OF THE YEAR

**Matthew Kitzman,**
Industrial Security Integration and Application

**Nancy McKeown,**
Center for Development of Security Excellence

**Leslie Whitaker,**
Industrial Security Field Operations

## NOMINATED FOR EMPLOYEE OF THE YEAR SENIOR

**Joseph Cashin,**
Industrial Security Field Operations Northern Region

**Ann "Skeeter" Gallagher,**
Headquarters (Office of the Inspector General)

**Lisa Taylor,**
Defense Vetting Directorate

**Jason Theriault,**
Industrial Security Integration and Application

**Todd Tucker,**
Counterintelligence Directorate

## NOMINATED FOR TEAM OF THE YEAR

**Counterintelligence Secure VTC Initiative,**
Counterintelligence Directorate

**DoD Insider Threat Management and Analysis Center,**
Defense Vetting Directorate

**Public Key Infrastructure Team,**
Headquarters (Office of the Chief Information Officer)

**Risk Integration Officers,**
Industrial Security Integration and Application

## NOMINATED FOR EXCELLENCE IN INNOVATION

**2018 DoD Virtual Security Conference for Industry Team,**
Center for Development of Security Excellence

**Chantilly Information Systems Security Professional Team,**
Industrial Security Field Operations

**Cyber Division,**
Counterintelligence Directorate

**Transforming Workforce Vetting,**
Defense Vetting Directorate

## EMPLOYEE OF THE QUARTER

Recognized during the ceremony were the Employees of the Quarter for 2018:

**First Quarter:** **Camille Johnson,** Counterintelligence Directorate

**Second Quarter:** **Mark Hedges,** Industrial Security Field Operations

**Third Quarter:** **Jonathan Laahs,** Counterintelligence, Western Region

**Fourth Quarter:** **Anastasia Baker,** Industrial Security Field Operations

## EMPLOYEE OF THE QUARTER SENIOR

Recognized during the ceremony were the Employees of the Quarter Senior for 2018:

**First Quarter:** **Heather Mardaga,** Center for Development of Security Excellence

**Second Quarter:** **Kristy Williams,** Defense Vetting Directorate

**Third Quarter:** **Ashley Maddox,** Headquarters (Office of Acquisitions)

**Fourth Quarter:** **Ted Banks,** Industrial Security Integration and Application

# FOUR RECEIVE DCSA **COUNTERINTELLIGENCE EXCELLENCE AWARDS**

**By Dana Richard and Stephen Smith**
*Counterintelligence Directorate*

Earlier this year, DCSA Director Daniel Payne announced Auburn University, Lockheed Martin, Oshkosh Defense, and Virginia Polytechnic Institute and State University as the winners of the Fiscal Year 2018 DCSA Excellence in Counterintelligence (CI) Award. DCSA annually recognizes those cleared companies exhibiting the most impressive CI capability and cooperation with U.S. government efforts to deter, detect and disrupt the theft of sensitive or classified U.S. information and technology by foreign entities.

The Excellence in CI award is intended to recognize effective CI programs that enhance national security and promote the uncompromised delivery of sensitive and classified services and capabilities to the Department of Defense and other U.S. government agencies.

## AUBURN UNIVERSITY

Auburn University provides experimental test facilities with data analysis, supports classified contracts, and built a leading CI-focused culture to detect, deter, and expeditiously report suspicious activities to DCSA. The university established policies and procedures that heighten the security awareness of employees and ensures cooperation within the academic and government communities. Auburn University reporting in FY18 greatly increased the Intelligence Community's understanding and analysis of the foreign intelligence and economic adversary threat to academia, cleared industry, and vital classified technology.

The university leads in Insider Threat programs with innovative solutions and a dedicated liaison with government agencies. Frank Cilluffo, director of Auburn University's Charles D. McCrary Institute for Cyber and Critical Infrastructure Security, was appointed to the U.S. Cyberspace Solarium Commission and also serves on the Homeland Security Advisory Council. Auburn University's Chief Operating Officer retired Lt. Gen. Ronald Burgess serves on the Board of Directors for the Intelligence and National Security Alliance and the National Intelligence University Foundation. Members of Auburn University's Huntsville Research Center have partnered with the U.S. Army Missile and Space Intelligence Center, Missile Defense Agency, and NASA to focus on cyber challenges and threats faced at Redstone Arsenal, Huntsville, Ala. Auburn University submitted 95 suspicious contact reports (SCRs), resulting in several full field operations.

## LOCKHEED MARTIN CORPORATION

Lockheed Martin Corporation, based in Bethesda Md., is a global security and aerospace company employing approximately 100,000 people in over 500 facilities in 50 states throughout the United States and in 52 nations and territories worldwide. Lockheed Martin is principally engaged in the research, design, development, manufacture, integration and sustainment of advanced technology systems, products, and services. The Bethesda, Md., facility serves as the corporate headquarters and home office for 102 cleared divisions/subsidiaries working over 46 classified U.S. government contracts. Lockheed Martin has four major operating units: Aeronautics; Missile and Fire Control; Rotary and Mission Systems; and Space. Lockheed Martin develops and integrates products, services, and support for aerospace and defense customers, as well as civil and commercial customers around the globe, to include the F-35 Lightning II, the Littoral Combat Ship Integrated Surface Warfare System, the 30kW ALADIN/ATHENA system, and the Mars Atmosphere and Volatile Evolution (MAVEN) mission for the U.S. Army, U.S. Navy, and U.S. Air Force.

Lockheed Martin runs one of the most advanced CI and Insider Threat programs in industry using unique proprietary tool to detect anomalous activity and concerning behavior. Lockheed Martin submitted 299 SCRs to DCSA, resulting in 17 federal investigations or operations. Lockheed Martin supported federal law enforcement in cases leading to the arrest of four U.S. citizens and four foreign nationals on charges of economic espionage and export violations, and the termination of 12 employees.

## OSHKOSH DEFENSE

Oshkosh Corporation and Oshkosh Defense, LLC are collocated at the Oshkosh Company in Oshkosh, Wisconsin. Oshkosh is a leading manufacturer of specialty vehicles for defense, fire and emergency, and commercial use. Oshkosh Defense is the world's leading provider of tactical wheeled vehicles for military and security forces around the globe. These tactical vehicles directly support the warfighter with a portfolio of heavy, medium, light, armored, and unmanned ground vehicle solutions. In 2015, Oshkosh Defense won a $6.7 billion government contract to provide Joint Light Tactical Vehicles for the U.S. Army and U.S. Marines.

Candidates for the CI in Excellence award are nominated by DCSA field elements. A panel composed of senior leaders from across DCSA conducts a multistage nomination, vetting and competitive selection process to identify annual winners based on the assessment of CI/Insider Threat reports the company submitted to DCSA that specifically led to the opening of full field investigations, operations, or other activities by federal agencies. Other significant company actions that detected and countered foreign intelligence activities are also considered, including disruptions, prosecutions, convictions, debarments, and administrative actions. No more than four award winners are selected annually.

Oshkosh runs an active and mature Insider Threat program; a Supply Chain Risk Management program; an active cyber defense program; a conference, convention and tradeshow threat program; and active programs to protect critical technology and controlled unclassified information. Oshkosh submitted 62 SCRs to DCSA, resulting in three full field investigations or operations.

## VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY

Virginia Tech is a public, land-grant, research university that dates back to 1872 with its origins as a military institute. With its main campus in Blacksburg, Va., Virginia Tech is currently designated as one of six senior military colleges in the United States. It is ranked 23rd by the National Science Foundation among universities for research expenditures, which puts Virginia Tech in the top 5% of more than 900 research universities/colleges in the United States. With the classified contracts between Virginia Tech and U.S. government organizations, the university conducts some level of research, development, or education in all technologies of the Industrial Base Technology List. Virginia Tech closely participates with government agencies to identify and prevent cyber threats by foreign intelligence entities.

Virginia founded the Association of University Export Control Officers (AUECO) in 2008, with current participation from 140 universities, sponsors an annual conference of the AUECO to discuss the latest topics of concern to university peers. Virginia Tech sponsored multiple training and threat awareness briefings, including quarterly cleared contractor "brown bag" luncheons for training and security discussions. Based on the U.S. Government threat warning, Virginia Tech does not engage in any proprietary exchanges or research with Huawei, and has developed a defensive posture against threats posed by Talent Programs and Confucius Institutes. Virginia Tech submitted 81 SCRs to DCSA, resulting in several full field operations.

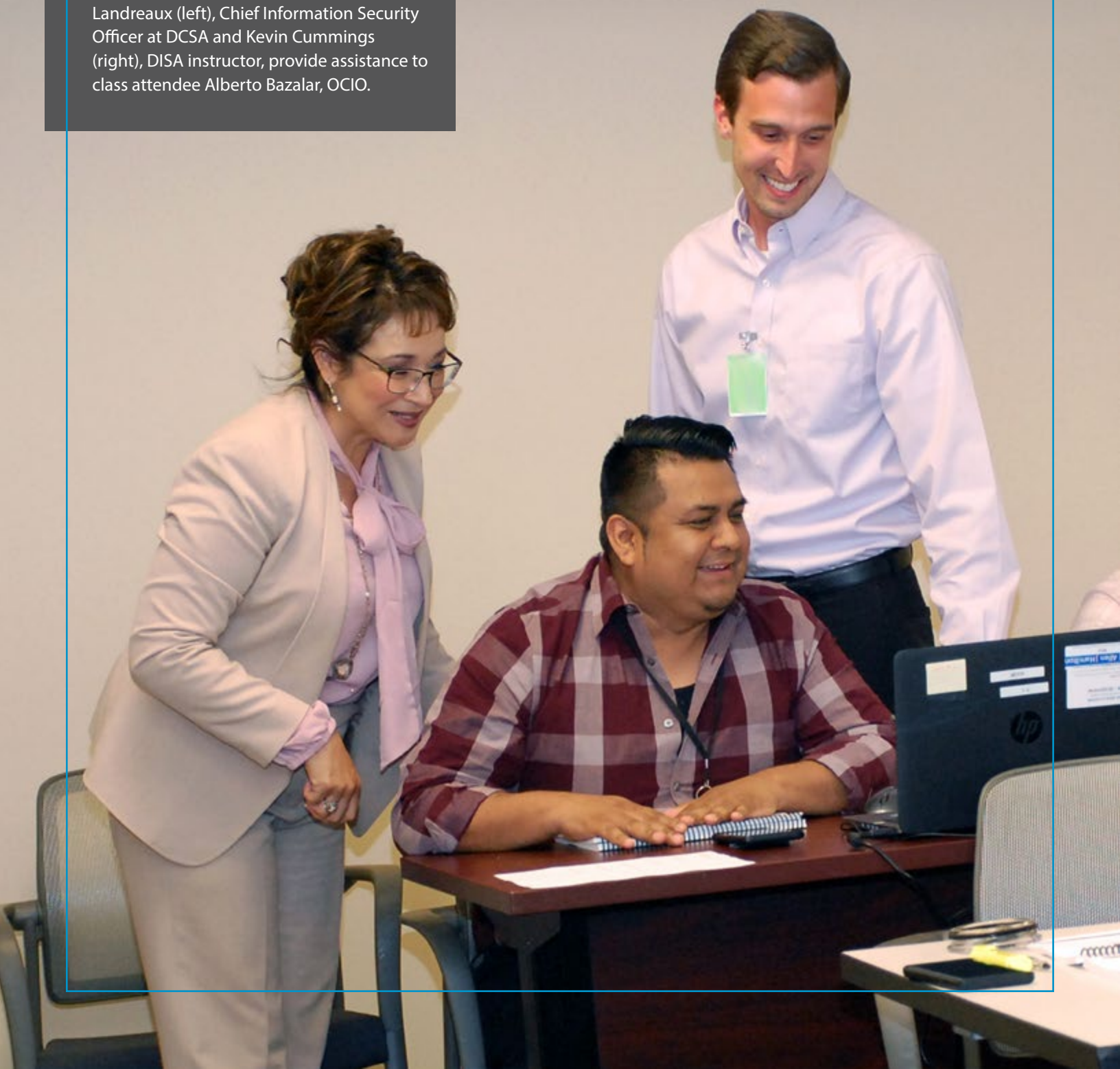

DCSA Director Dan Payne (center) presents the leadership of Oshkosh Defense with the Excellence in Counterintelligence Award at DCSA headquarters, Quantico, Va.

# SECURITY **OUTREACH**


Dan Payne (left), former director of the Defense Counterintelligence and Security Agency, and Charlie Phalen, director of the National Background Investigations Bureau (NBIB), co-presented at the DynCorp International 10th Annual Security Conference, where they discussed the merger of DCSA and NBIB, security clearances, and Trusted Workforce 2.0. (Courtesy photo)

# UNDERSTANDING eMASS

The Office of the Chief Information Officer hosted a Defense Information Systems Agency instructor-led course on the Enterprise Mission Assurance Support Service (eMASS). The eMASS is a tool that provides cybersecurity governance, risk, and compliance functions with an integrated suite of capabilities to improve cyber risk management. Approximately 20 personnel from DCSA and the National Background Investigations Bureau attended the training. In the photo at left, Roxanne Landreaux (left), Chief Information Security Officer at DCSA and Kevin Cummings (right), DISA instructor, provide assistance to class attendee Alberto Bazalar, OCIO.



# ACTIVE SHOOTER AND WORKPLACE VIOLENCE PREVENTION SUMMIT IN SAN DIEGO

*Editor's Note: The following reflects the thoughts and opinions of the author on her attendance at an active shooter/prevention of workplace violence event and practical application of the knowledge she acquired.*

**by LaHoma Kotchian**
*Regional Action Officer, Western Region*

In May 2019, I attended an Active Shooter and Workplace Violence Prevention Summit, hosted by the local San Diego chapter of Infragard. It was one of the largest events of its kind and hosted over 500 attendees at Qualcomm Incorporated in San Diego. It brought together security stakeholders from all walks of life: law enforcement, local contractor community, schools, churches, hospitals, etc. The goal was to inform, educate, and prepare the audience on critical threats facing modern society. Unfortunately, it was also a timely summit as just weeks prior, the shooting at the Chabad of Poway Synagogue made national news. This incident occurred approximately one mile from where the field/region offices are located in San Diego, Calif.

The summit kicked off with a historical perspective of the active shooter threat, highlighting current trends and active shooter characteristics. Members of the San Diego Police Department (SDPD) gave first-person perspectives about high-profile shootings in which they were involved. A now-retired SDPD officer, who was a rookie during the 1984 shooting at a McDonald's restaurant in San Ysidro, Calif., talked about his experience for the first time publicly. A SDPD SWAT officer who lived through the 2017 Route 91 Harvest Music Festival in Las Vegas spoke about his experience in escaping the gunfire and attempting to rescue many people. Both were emotional in telling their stories, but reiterated that those events forever changed their lives. They encouraged people to seek professional help if they experience a trauma of that magnitude.

The summit then delved deeper into the mind of a targeted attacker, often referred to as getting to the "left of bang," to develop greater awareness of indicators that might be evident prior to an active shooter event. Dr. Reid Meloy, a forensic psychologist from the University of California, San Diego, spoke about warning behaviors and threat assessments of the targeted attacker, specifically of pre-event indicators and the pathway to targeted or intended violence (eight patterns):

1. Pathway warning behavior (research, planning, prep or implementation of attack)
2. Fixation warning behavior (preoccupation with a person or cause, what the person is thinking about all the time, failure in work or school as a result)
3. Identification warning behavior ("pseudocommando" or "warrior mentality," big shift from what the person is thinking about to who they have become (self-identity); this is a critical time, may be signaling or mobilizing for violence)
4. Novel aggression warning behavior (tests ability to actually be violent, tests his or her mettle)
5. Energy burst warning behavior (frequent or a variety of noted activities, burst of energy prior to event)
6. Leakage warning behavior (communicates to a third party of an intent to do harm to a target through an attack, has poor operations security which leads to vulnerabilities, and presents in 60-90 percent of targeted attackers)
7. Last resort warning behavior (time/action imperative, subject feels no alternative other than violence, to him/her the consequences are justified)
8. Directly communicated threat warning behavior (tactical success, appears in less than 20 percent of cases)

Overall, in most of the situations, there are usually warning signs and we need to pay attention. Mental illness is not a predictor for this type of behavior; rather it is one ingredient among many factors – a small piece of the pie. If we can recognize the signs at the identification warning behavior stage, there is a good chance we can keep a bad situation contained and get help to those in need.

A corporate security officer and retired FBI agent spoke about workplace violence prevention, specifically threat assessment, mitigation and management. He gave specific examples of typical versus atypical behaviors to look for in the workplace, as well as reactive (driven by emotions) or predatory violence (targeted). He also spoke of the pathway to targeted or intended violence as it pertains to the workplace and methods of training, reporting, intervention and prevention. His overall takeaway was that "People don't snap, they escalate." He urged us to pay attention to behavioral indicators of co-workers on a personal level and on a professional level. At any stage of this escalation, we have opportunities to intervene in order to help our co-workers. Often, getting them on the right track or getting them help is the only intervention that is required.

Another FBI agent spoke from the angle of personal protection and challenged us to think that the "Run, Hide, Fight" mantra is good, but it should actually be: RUN, RUN, RUN, RUN, hide, fight (last resort). If you hear shots, your automatic response should be to escape and run since hitting a moving target is difficult especially as it moves farther away. Also, be aware of your surroundings and know your escape strategy in any situation. Last, if you are hiding and you are forced to fight, they demonstrated basic fighting or positioning tactics within a safe room. The first priority is to get control of the weapon and the second priority is to take the shooter down, with the emphasis on coming down hard on the shooter by everyone. At this point, use improvised weapons, fully commit to your actions, and attempt to incapacitate the shooter or worse.

In an effort to put the lessons into action, on May 30, 2019, Robert Limon, Western Region CI collection manager, Crystal Diehl, senior industrial security representative from Phoenix Field Office, and I held a training session for Western Region and San Diego Field Office personnel. I discussed highlights from the summit along with the biggest takeaways for practical use. We also discussed our current and local threats as risk factors and tried to provide some context to those takeaways. Diehl, who was recently certified as a Federal Risk Management Process professional, conducted a preliminary risk assessment of the San Diego Field Office and Western Region Office utilizing federal standards and tools. She created

> "People don't snap, they escalate."

a security baseline and a snapshot of the need to increase the overall security at our designated location and briefed the results to our personnel, Western Region leadership, and Headquarters Security for situational awareness. Limon led the discussion with personnel regarding personal safety concerns and complacency. Our goal was to open the dialogue with our colleagues and to make them aware of those warning behaviors. We wanted to encourage them to remain vigilant and avoid complacency in their everyday actions. If any of us sees something suspicious, we should not ignore it and assume someone else will deal with it.

**Every time an event happens, we always hear witnesses say that there were warning signs. Let's pay attention and begin to take a proactive approach rather than a reactive one for the safety of our fellow personnel**

Then we watched a few short videos ("Run, Hide, Fight," and "Tomorrow's News") and demonstrated basic tactics of fighting and taking down an active shooter, should the need ever arise. In the near future, we plan to do an active drill with our personnel and ensure that everyone is comfortable with an escape plan or shelter-in-place plan. Overall, discussing the potential of an active shooter situation or of workplace violence is difficult and many do not want to face it, but it cannot be ignored. Every time an event happens, we always hear witnesses say that there were warning signs. Let's pay attention and begin to take a proactive approach rather than a reactive one for the safety of our fellow personnel. According to the FBI, over 80 percent of active shooter incidents occur at the workplace. Let's be as prepared as we can be.

**OVERALL, THE KEY TAKEAWAYS OF THE SUMMIT WERE:**

- DEVELOP A PLAN/TRAIN IT/REHEARSE IT/IMPROVE IT (REHEARSING CANNOT BE OVER EMPHASIZED)
- BE SPECIFIC TO YOUR LOCATION AND STRUCTURE
- REACTIONS IMPROVE WITH MENTAL REHEARSAL
- REINFORCE YOUR ESCAPE PLAN UNTIL IT IS AUTOMATIC
- WHEN LAW ENFORCEMENT ARRIVES, THEIR FIRST PRIORITY IS TO: 1) STOP THE SHOOTING; THEN 2) STOP THE DYING
- AFTER EACH ACTIVE SHOOTER EVENT, THERE ARE LESSONS LEARNED TO HELP PREVENT FUTURE EVENTS.

Andover Field Office Chief John "Sean" Donnelly offers opening remarks at the 7th annual Partnership with Industry Day workshop, hosted by the Andover Field Office.

# OUTREACH EVENT FOCUSES ON **PROTECTION OF CRITICAL ASSETS, PARTNERSHIP**

**By Kathryn Kimball**
*Andover Field Office*

This year marked the 7th annual Partnership with Industry Day workshop hosted by the Andover Field Office. Due to its popularity, the event was split into sessions held over two days in order to accommodate the number of attendees. In attendance were approximately 165 cleared contractor personnel representing 132 facilities under the cognizance of Andover Field Office, representing the states of Maine, Massachusetts, New Hampshire and Vermont. Additionally, two representatives from the 66th Air Base Group, Industrial Security Directorate, Hanscom Air Force Base, Mass., and 16 DCSA personnel from the field office, Northern Region Office and DCSA headquarters participated.

The theme for this year's PWI workshop, "Risk-based Industrial Security Oversight' (RISO), delivered relevant and meaningful information to the attendees. Among the presentations were opening remarks and updates by Field Office Chief John Donnelly, followed by Mike Ray of the Vetting Risk Operations Center. Senior Industrial Security Representative Virginia Morrissette, Counterintelligence Special Agent Frank Bonner and Information Systems Security Professional Team Lead Hung Phan discussed Insider Threat Program updates including what an effective insider threat program entails. Patrick Fields, Facility Clearance Branch, and Dustin Dwyer, chief, Mitigation Strategy Unit, enlightened everyone on facility clearance processing and foreign ownership, control or influence overview and mitigation. The last session of the day heard

Senior Industrial Security Representatives Tim Hulub and Jim Herbert deconstruct "RISO," making it relatable to our industry partners. The day concluded with an open panel question-and-answer session, and guests completed surveys to solicit feedback on the workshop effectiveness. Overall, attendees overwhelmingly agree the outreach event was informative and well-received.

## ATTENDEE FEEDBACK

"I wanted to take a moment to reach out and thank you and your entire office for all of your collective efforts in putting on the Industry Day. I found it exceptionally informative and well put together. I will give our security team a read out of the highlights from today and prepare everyone to shift their mindset to Asset Identification.

Protection of critical information/assets is very important and the risk based approach is necessary. They made it clear and made us understand our role in this.

I feel that DiT (RISO) has created an even better partnership between DCSA and Industry. This has allowed walls to come down and provide opportunities for DCSA to understand our business."

# FIELD OFFICE CHIEF RETIRES

35 YEARS OF SERVICE

DCSA Northern Region Director Cheryl Matthew and the leadership team across the region along with Michael Halter, deputy director, Industrial Security Field Operations, celebrated the retirement of Andover Field Office Chief John "Sean" Donnelly (center) who retired from DCSA after 35 years of federal service. More than 75 people from DCSA, the National Background Investigations Bureau, and industry and government partners attended the event orchestrated by the Andover Field Office team.

# MENTORING OF NEW INDUSTRIAL SECURITY REPRESENTATIVES **ENSURES UNDERSTANDING OF AA&E OVERSIGHT ROLE**

**by Alice Kispert**
*Field Office Chief, Mt. Laurel Field Office*

Within the Defense Counterintelligence and Security Agency, there is a small cadre of trained industrial security representatives who perform Arms, Ammunition, and Explosives (AA&E) program oversight for approximately 165 contractor facilities nationwide. In support of the AA&E program, DCSA conducts pre-award surveys and assesses contractor compliance with the physical security provisions contained in contracts involving sensitive and conventional AA&E. If the contract is awarded, DCSA conducts recurring on-site physical security inspections of AA&E facilities. Industrial security representatives also provide advice and assistance to contractors regarding AA&E matters.

It is Department of Defense policy, as outlined in DoDM 5100.76, "Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives," that the security of sensitive conventional AA&E is of the highest importance to the DoD. If AA&E is compromised, sabotaged, stolen, misused, or vulnerable to malicious mischief or acts of terrorists, subversives, criminal elements, or willful interference, it has the potential to jeopardize the safety and security of personnel, activities, missions, and installations worldwide.

David Boyda, a senior industrial security representative (SISR) in the Mt. Laurel Field Office, who in addition to handling National Industrial Security Program (NISP) oversight duties, is a member of the DCSA cadre of ISRs performing duties associated with the AA&E program.

Boyda also serves as a lead advisor and mentor to new representatives as he understands the importance of educating and training newly assigned DCSA personnel. As part of the field office's continued focus on critical technology protection, Boyda took two new industrial security representatives on a Physical Security Inspection conducted at a facility involved in the AA&E Program. Terrell Adams and Allison McNish had recently completed the National Industrial Security Program Oversight Course, which provides new ISRs with the fundamental knowledge of NISP requirements, as well as DCSA internal processes and procedures. However, AA&E is specialized and therefore most of the training in this area comes from those who are already trained on performing these actions.

"This was an excellent learning opportunity as I was able to obtain knowledge of the AA&E Program focusing on categories, elements and variations of oversight from a diverse security perspective," said Adams.

"This visit enabled me to learn more about physical security issues with a focus on controlled areas and emphasis on hardening of the area where assets are stored in support of AA&E requirements," McNish said.

With the small number of personnel that have AA&E program expertise, the Mount Laurel Field Office recognizes the importance of ensuring the skills and tradecraft be passed to others in order to provide effective oversight of AA&E. Mentoring efforts such as this contribute to the success of training related to DCSA personnel assigned oversight duties and responsibilities.

# CHILDREN LEARN TO NAVIGATE THE INTERNET **WITHOUT COMPROMISING SAFETY, IDENTITY**

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

As a part of the 2019 Take Your Child To Work Day (TYCTWD) events hosted by the Defense Counterintelligence and Security Agency in April, NISP Authorization Office (NAO) volunteers presented age-appropriate lessons focused on cybersecurity.

"TYCTWD is the perfect opportunity to start cultivating future generations of cybersecurity professionals—it's never too early," said Karl Hellmann, NISP Authorizing Official.

In keeping with this year's TYCTWD theme, "Workforce Development for All," the NAO focused on delivering a program dedicated to cybersecurity educational sessions that empower young people to navigate cyberspace and the Internet. The goal was to help children of all ages to make the correct decisions regarding privacy, posting, and cyber bullying.


Selena Hutchinson, NISP Authorization Office, discusses online game safety and building a safe social media profile.

### THE LESSONS PRESENTED BY THE NAO INCLUDED:

**Lesson 1**: Safe and Secure Online focused on privacy, online game safety, stranger danger, and many other key concepts to help children begin to understand safe surfing.

**Lesson 2**: Pause Before You Post focused on social media safety, posting safe photos, building a safe profile page, and many other key concepts to help children begin to understand how privacy relates to posting practices.

**Lesson 3**: Be Kind Online addressed kind and positive behavior when interacting online, things to keep in mind when video and photo sharing, tagging, posting, and many other key concepts that help children begin to understand how their individual behavior online affects others.

DCSA distributed Garfield activity comic books, student stickers, and letters for parents, and trading cards. Older students were challenged with puzzles that contained invisible ink clues to their cybersecurity crossword puzzles.

**NAO wanted to infuse the idea that everyone, including our youth, has the right to access the Internet without fear of compromising their safety or identity.**

These lessons were aimed at making the right decision when confronted with using the Internet and social media, and overcoming some of the negative messages that students might be exposed to online. NAO wanted to infuse the idea that everyone, including our youth, has the right to access the Internet without fear of compromising their safety or identity.

The volunteers were: Robbin Branch, Shelton Mallow, Kelly Hixson, Mark Hardy, Kelly Schlienger, Jonathan Cofer, Luciana Rodriques, Tracy Brown, and India Dyson.

The NAO partnered with the Center for Cyber Safety and Education to obtain the materials. The Center for Cyber Safety and Education, formerly (ISC) Foundation, is a non-profit charitable trust committed to making the cyber world a safer place for everyone. The Center works to ensure that people across the globe have a positive and safe experience online through their educational programs, scholarships, and research.

# DCSA ACCESS

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY | WWW.DSS.MIL