DSS ACCESS

Official Magazine of the Defense Security Service | Volume 5, Issue 3

NSE • DEFENSE SUPPLY AGENCY • OFFICE OF INDUSTRIAL SECURITY

INDUSTRIAL SECURITY
LETTER

l be issued periodically to inform Industry, User Agencies and DoD Activities of developments relating reproduction of these letters in their original form for the internal use of addresses is authorized. Sug- ssion in the letter will be appreciated. Articles or ideas contributed will become the property of DSA.

29 September 1966

L AWARD" ESTABLISHED

his outstanding contributions to the Department of ecurity Program, Colonel James S. Cogswell, former ustrial Security, HQ DSA CAS, was honored by the e on 30 August 1966, by the announcement that hence- nding Industrial Security Achievement Award ISL 66L-3, 27 May 1966) would be named the "James S. nding Industrial Security Achievement." Mr. fication Management, who represented ecretary of Defense for uncheon held n.

Smyth Firm Wins
Award for Security

By IAN LEDGERWOOD
EVENING TRIBUNE Staff Writer

There is no barbed wire, no electric fence, no guards or dogs. In fact, nothing could be easier than walking through the front door of Smyth Research Associates on Kearny Mesa.

Despite this open-house atmosphere, the 12-year-old radio physics company yesterday was awarded the James S. Cogswell Award for an outstanding industrial security program.

One of four companies which received the new award in nationwide competition, the 50-man Smyth organization has only one part-time security officer, Dr. Steven Weisbrod, whose main job is director of research.

How then does Weisbrod keep the firm's secret documents secret?

"By having no grey areas where some people can be and others cannot," he said. "We keep all classified material in a safe in the center of the plant. Only three people have the combination. This way we have only one top security area to worry about.

"We can do this only because we have a small com-

DR. JOHN B. SMYTH
Avoids bureaucracy

director of the Defense Contract Administration Services Region-Los Angeles, presented the award to the company president, Dr. John B. Smyth.

Smyth formed the research associates firm in 1955 with a group of seven scientists who had worked at the Navy Electronics Laboratory.

Smyth ... small com-

without vast sums to spe like much larger corporati in the same field, researc and finds simpler and chea electronics equipment which to track satellites, at stars, and study electr and ionospheres.

One device, the only on its kind in the United St and no larger than a s suitcase, tracks satellite can pick them up when are over Guam, far belo horizon, Smyth said.

The machine's predec needed two cabinets, over 6 feet high, to cont its equipment.

Much of the materia in the manufacture firm's equipment is m the spot in machine a pentry shops where files for the library built.

"If we build it oursel don't have to wait," said. "And often w something in the You can't buy quickly."

SAN DIEGO TRIBUNE - 14 Feb 67

FIFTY YEARS of Industrial Security Excellence

DSS ACCESS

Published by the
Defense Security Service |
Public Affairs Office

27130 Telegraph Rd.
Quantico, VA 22134

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

DSS LEADERSHIP

Director | Dan Payne

Chief of Staff | Troy Littles

Chief, Public Affairs | Cindy McGovern

Editor | Elizabeth Alber

Graphics | Steph Struthers

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

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

All pictures are DoD photos, unless otherwise identified.

COVER STORY: Fifty Years of Industrial Security Excellence

INSIDE

From the Director

DSS marked a significant milestone in June with the 50th anniversary of the Cogswell Awards. The award was established in 1966 to encourage "the achievement of a superior degree of excellence in industrial security." In August 1966, the award was renamed the James S. Cogswell Award for Outstanding Industrial Security Achievement in recognition of Colonel Cogswell's outstanding contributions to the Department of Defense Industrial Security Program.

During the annual NCMS conference, we presented the 2016 Cogswell Award to 42 companies who had consistently demonstrated their level of commitment to industrial security and their leadership in the community. I was honored to be a part of the ceremony and reflect on the importance of the award. Included in the ceremony were Col. Cogswell's son Michael and granddaughter Catherine.

Michael graciously shared with us photos of his father and documents from his father's life and from the establishment of the industrial security program. He also shared his father's biography and various mementos of his father's distinguished career, which culminated as the first director of industrial security. In connecting with Michael and Catherine, we have been able to gather the history of the award, as well as the history of DSS, in those interesting and unique documents and archive them to ensure they remain part of the Cogswell and DSS tradition. We've included some of those documents in this issue.

In keeping with past practice, this issue of the ACCESS also includes input from a cross-section of the 2016 Cogswell winners. It's one thing for DSS to talk about good security programs, but quite another to hear from the winners themselves on how they achieved superior programs. In reading the personal accounts, I was struck by the level of commitment and enthusiasm each of the authors displayed for their jobs, their companies and their security programs.

Anyone who has heard me speak at NCMS or other venues knows I view today's threat environment as enduring and persistent. I believe the United States is currently facing a counterintelligence threat that is unprecedented in our history. This increased threat is a result of advances in technology (primarily cyber) and science, and the globalization of business and the American workforce. We are losing significant amounts of technology and information, most of which are unclassified. Further contributing to the challenge, the collection methods of our adversaries are constantly changing.

To meet this new threat, DSS is changing how it does business. But we cannot do this alone. Accepting this new threat environment and adapting to it will require the expertise and commitment of our industry partners; like the 2016 Cogswell award winners. The need for a strong, transparent partnership between government and industry is even more critical today than it was in 1966.

Dan Payne
Director

FIFTY YEARS of Industrial Security Excellence

A FAMILY AFFAIR: Michael Cogswell (left), son of Air Force Col. James S. Cogswell, stands with his daughter Cathy in front of the DSS display at the NCMS seminar in Nashville, Tenn.

DSS presents annual **Cogswell Awards** to 42 facilities

by Beth Alber
Office of Public and Legislative Affairs

Fifty years ago, the first James S. Cogswell Outstanding Industrial Security Achievement Awards were presented to 16 out of 15,000 cleared contractor facilities.

On June 8, 2016, the Defense Security Service presented the annual Cogswell awards to 42 cleared contractor facilities, which represent the "best of the best," and their security programs stand as models for others to emulate. These 42 facilities represent less than one-tenth of one percent of the over 13,000 cleared contractors in the National Industrial Security Program (NISP).

Each year, DSS partners with NCMS to host the Cogswell Award presentations during its annual training seminar. In presenting the awards, DSS Director Dan Payne noted the original criteria for the Cogswell included an effective security organizational structure; results of security inspections must show "an absence of serious deficiencies and prompt corrective action;" a security education program which effectively informs all employees of their particular security responsibilities; and full compliance with requirements for reporting to the appropriate government authority information required to be reported by the Industrial Security Manual. "That sounds to me like the same criteria that are used today to determine the award recipients," Payne said.

The director went on to highlight the thoughts of one of the first companies awarded the Cogswell. "In accepting one of those first awards, R.W. Lee,

president of General Precision Librascope said, 'The program is effective because management actually supports it and because our employees feel individually responsible. All of us have deep concern for our nation's safety.'

"I am guessing that the facility security officers and senior management officials who will walk across this stage would attribute their award to the same company attributes — management commitment and employees who understand how their actions contribute to a successful security program," Payne said.

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.

In recognition of the 50th anniversary, members of Colonel Cogswell's family were on hand for the ceremony. "When my daughter Cathy reached out to DSS about the 50th anniversary, we didn't know what to expect. Whether anyone would remember my Dad or how the award was regarded in industry," said Michael Cogswell, Colonel Cogswell's son. "We found a very welcoming team at DSS, who were very interested in my father and his history."

> We found **a very welcoming team at DSS**, who were very interested in my father and his history.

Michael went on to talk about his father's military career, noting that James Cogswell was a member of the greatest generation and served with distinction in World War II. He enlisted in the Connecticut National Guard in 1938, and his military career culminated in March 1965, when he was named the first chief of the Office of Industrial Security.

"Later that year, my father was diagnosed with cancer, but in spite of the diagnosis, he worked tirelessly to complete the Industrial Security Manual in 1966," Michael noted. "He retired in September 1966 having completed the goal he set for himself. Shortly before his retirement, he was honored to learn that the Outstanding Industrial

IN THANKS: DSS Director Dan Payne (right) presents Michael Cogswell with a plaque after his remarks at the Cogswell Award Ceremony.

Security Achievement Award, established earlier that year, had been renamed in his honor."

"My father believed passionately in what he was doing. He saw the need for collaboration between industry and the government. I am pleased to see that collaboration continue to this day, and I am proud and humbled to see his legacy live on in this award," he said.

During his remarks, Payne described the Cogswell selection process as rigorous. The process begins with a DSS 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 DSS internal review process that includes a national review team of DSS Regional Directors and representatives from across DSS who consider each nomination.

The national review team vets all nominations with 30 external agencies and makes recommendations to DSS senior leadership for a final decision based on the following criteria:

- Overall security program

CI Special Agent Joseph Parker, Huntsville Field Office, mans the CI booth at the annual NCMS seminar.

- Senior management support
- Security vulnerability assessments
- Security education and awareness
- Facility security officer and security staff level of experience
- Classified material controls

The 2016 award recipients include a balance of both large and small companies, and represent a myriad of technologies. "Some are research and development centers, and some are doing intelligence services. Some are steeped in hardware like electronics manufacturing and space systems, while others are involved in training and logistics support, or are major universities," Payne said. "I can say that each of these recipients shows clear management and corporate commitment for security, and the culture of security is very important and clearly present at all of these facilities.

"Companies don't make security programs, people do. The facility security officers, the security staffs, the company leadership — without your commitment and your dedication, your company would not be here today," he said. "And it's your willingness to be a partner with DSS that we honor you as well as your achievement. You are continuing a 50-year legacy of partnership and excellence."

> "Companies don't make security programs, **people do.**"

In closing, Payne said, "I want to leave you with this quote from April 1967, words even more true today than they were then. In accepting the first Cogswell award for Southern Bell, President F.M. Malone said, 'The security of information and materials relating to our nation's defense is clearly one of the most essential concerns of this business. We must take whatever measures are necessary to provide utmost security, because success in this matter is imperative and failure is unthinkable.'"

Congratulations to the **2016 Cogswell Award** Winners!

Advanced Technology International
Summerville, S.C.

Aerospace Corporation, The
Colorado Springs, Colo.

BAE Systems Technology Solutions & Services, Inc.
Mojave, Calif.

Carnegie Mellon University – Software Engineering Institute
Pittsburgh, Penn.

DRS Sustainment Systems, Inc.
St. Louis, Mo.

DRS Training & Control Systems, LLC
Stevensville, Md.

EOIR Technologies, Inc.
Fredericksburg, Va.

General Dynamics C4 Systems
Dedham, Mass.

General Dynamics Mission Systems
McLeansville, N.C.

General Dynamics Ordnance and Tactical Systems, Camden Operations
Hampton, Ark.

Harris Corporation
Rochester, N.Y.

Honeywell International Inc., Aerospace – Albuquerque
Albuquerque, N.M.

Honeywell International Inc., Aerospace – Plymouth
Plymouth, Minn.

Honeywell Technology Solutions
Lexington Park, Md.

Infinity Systems Engineering, LLC
Colorado Springs, Colo.

L-3 Coleman Aerospace
Orlando, Fla.

L-3 Communications, Electron Devices
San Carlos, Calif.

L-3 Communications Integrated Systems
Crestview, Fla.

L-3 SPD Electrical Systems
Philadelphia, Penn.

Linde LLC, Technical Center
Murray Hill, N.J.

Lockheed Martin Corporation Missiles & Fire Control
Lufkin, Texas

Lockheed Martin Corporation Missiles & Fire Control Operations Support
Chesapeake, Va.

Matthews Group, The
Purcellville, Va.

Mercury Systems, Inc.
Hudson, N.H.

MorphoTrust USA, LLC
Billerica, Mass.

NAVSYS Corporation
Colorado Springs, Colo.

Northrop Grumman, Palmdale Aircraft Integration Center of Excellence
Palmdale, Calif.

Northrop Grumman, St. Augustine Aircraft Integration Center of Excellence
St. Augustine, Fla.

Oshkosh Corporation
Oshkosh, Wis.

PAE Applied Technologies
Lexington Park, Md.

Primus Solutions LLC
Beltsville, Md.

ProLogic Inc.
Manassas, Va.

Quest Software Public
Rockville, Md.

Raytheon Company
Aurora, Colo.

Raytheon Company EWS Self Protect Systems
Goleta, Calif.

Raytheon Company Raytheon Vision Systems
Goleta, Calif.

SES Government Solutions
Reston, Va.

Ultra Electronics Advanced Tactical Systems, Inc.
Austin, Texas

Ultra Electronics Secure Intelligence Systems Inc.
Manassas, Va.

University of New Mexico
Albuquerque, N.M.

Virginia Polytechnic Institute and State University
Blacksburg, Va.

Wiley | Wilson
Lynchburg, Va.

FIFTY YEARS of Industrial Security Excellence

A brief history of the **James S. Cogswell Award**

It may be cliché, but much has changed in the security community in the last 50 years — government reorganizations, acquisitions and mergers in industry, increased globalization and foreign investment, and increasingly complex foreign threats. Most stunning, perhaps, have been the technological advancements and the notion, even in 1966, that security professionals were considering how the use of computers would present control problems.

What has remained constant, however, is that for five decades, the James S. Cogswell Outstanding Industrial Security Achievement Award has epitomized excellence in industrial security. It also serves as the foundation of the Industrial Security Program — the partnership between cleared industry and the government to ensure the protection of classified information.

The success of the program and its foundation can be traced largely to the actions of one individual: U.S. Air Force Col. James S. Cogswell. Cogswell was a native of Massachusetts. He worked at Wescott Road Motors as a salesman and service advisor and rose to become general manager in charge of the entire new and used car sales and service organization.

> “The success of the program and its foundation can be traced largely to the actions of one individual: **U.S. Air Force Col. James S. Cogswell.**”

While at Wescott, he enlisted in the Connecticut National Guard. As part of the 43rd Infantry Division, he served with distinction during the Second World War. Cogswell was wounded in action in July 1943 during fighting in the South Pacific, and he later earned the Bronze Star for service against the enemy on Luzon, Philippines.

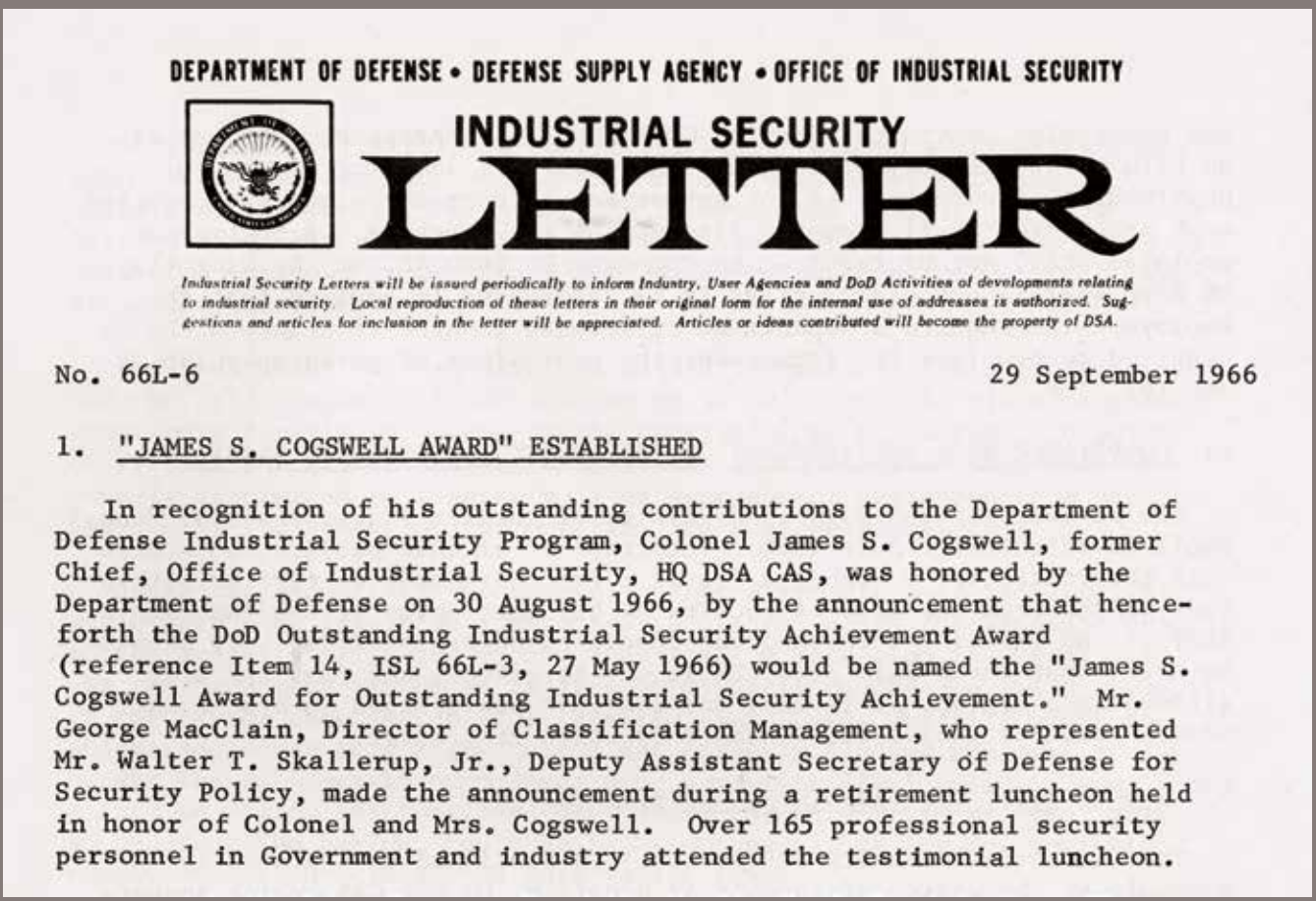
Immediately following the Japanese surrender, Cogswell served as division Provost Marshal and later as the Police and Public Safety Officer of Saitaima Prefecture. He returned to the United States in 1945 and applied for a regular army commission. He was one of 9,200 men whose names President Truman had sent to the United States Senate for confirmation. Cogswell was also one of the officers chosen from over 70,000 officers and former officers of the National Guard and Officers Reserve Corps under the Second Regular Army Integration Program. In September 1947, as an Air Corps officer, he was transferred to the newly created Department of the Air Force.

Cogswell continued to serve in the military police branch and rose steadily through the Provost Marshall career field. In 1954, he was assigned to Tinker Air Force Bae, Okla., where he attended the Army Intelligence School’s Industrial Security Course.

In 1959, Cogswell was assigned to the Security Policy Division, Directorate of Security and Law Enforcement under the Inspector General of Headquarters Air Force. In this role, he worked closely with both military and industrial stakeholders to foster a close working relationship between the Air Force and industry.

He was awarded the Legion of Merit for his efforts. Following the establishment of the Defense Supply Agency (DSA), the industrial security organizations of the various services were consolidated under the Defense Contract Administration Services Directorate of DSA. Cogswell was named the first Chief of the Office of Industrial Security on March 4, 1965.

Under his leadership, the Defense Industrial Security Clearance Office was established and 110 security offices of the military departments and 11 Defense Contract Administration Services regions were



DEPARTMENT OF DEFENSE • DEFENSE SUPPLY AGENCY • OFFICE OF INDUSTRIAL SECURITY

INDUSTRIAL SECURITY LETTER

Industrial Security Letters will be issued periodically to inform Industry, User Agencies and DoD Activities of developments relating to industrial security. Local reproduction of these letters in their original form for the internal use of addressees is authorized. Suggestions and articles for inclusion in the letter will be appreciated. Articles or ideas contributed will become the property of DSA.

No. 66L-6 29 September 1966

1. "JAMES S. COGSWELL AWARD" ESTABLISHED

In recognition of his outstanding contributions to the Department of Defense Industrial Security Program, Colonel James S. Cogswell, former Chief, Office of Industrial Security, HQ DSA CAS, was honored by the Department of Defense on 30 August 1966, by the announcement that henceforth the DoD Outstanding Industrial Security Achievement Award (reference Item 14, ISL 66L-3, 27 May 1966) would be named the "James S. Cogswell Award for Outstanding Industrial Security Achievement." Mr. George MacClain, Director of Classification Management, who represented Mr. Walter T. Skallerup, Jr., Deputy Assistant Secretary of Defense for Security Policy, made the announcement during a retirement luncheon held in honor of Colonel and Mrs. Cogswell. Over 165 professional security personnel in Government and industry attended the testimonial luncheon.

ISL NO. 66L-6, 29 SEPTEMBER 1966, DEFENSE SUPPLY AGENCY, OFFICE OF INDUSTRIAL SECURITY
JAMES S. COGSWELL AWARD ESTABLISHED

In recognition of his outstanding contributions to the Department of Defense Industrial Security Program, Colonel James S. Cogswell, former Chief, Office of Industrial Security, HQ DSA Contract Administration Services (CAS), was honored by the announcement on Aug. 30, 1966 that the DoD Outstanding Industrial Security Achievement Award (reference Item 14, ISL 66L-3, 27 May 1966) would be named the "James S. Cogswell Award for Outstanding Industrial Security Achievement.

reorganized and consolidated into a single cohesive organization with common policies and procedures.

He completed publication of the Industrial Security Manual in July 1966, and was awarded a second Legion of Merit for his efforts. Cogswell passed away on Jan. 29, 1968 and was buried in Arlington National Cemetery with full military honors.

The DoD Outstanding Industrial Security Achievement Award was established in May 1966 and renamed in Cogswell's honor in September 1966.

Upon his retirement, Cogswell was presented a certificate from the American Society of Industrial Security, which read in part:

"... Particular commendation is also deserved for his unfailing sympathy with the needs and problems of industry in these works; the sincere and cordial spirit of collaboration shown; and the inspiration these efforts have aroused throughout Government and Industry."

The Defense Security Service is proud of the accomplishments of Colonel Cogswell and honored to carry forward his vision and commitment to industrial security. DSS is also proud to honor 50 years of industrial security excellence. Congratulations to the 2016 Cogswell Award Winners!

FIFTY YEARS of Industrial Security Excellence

The following is a partial list of the first Cogswell Award recipients with related press coverage:

AC Electronics, Defense Research Laboratory – *Goleta, Calif.*

Conductron Corp – *Ann Arbor, Mich.*

Franklin Institute – *Philadelphia, Penn.*

General Precision Librascope Group – *Glendale, Calif.*
Glendale News Press, Glendale, Calif., Feb. 9, 1967, had a story on the presentation of the award: R.W. Lee, President, said "The program is effective because management actually supports it and because our employees feel individually responsible. All of us have deep concern for our nation's safety."

Grumman Aircraft Engineering Corp – *Bethpage, N.Y.*

Lockheed-Georgia – *Marietta, Ga.*
From the Lockheed Southern Star Newsletter, Feb. 16, 1967: Noted award was: "For superior performance of obligations while at work under a classified defense project contract."

Radiation Inc. – *Melbourne, Fla.*

TRW Systems Group – *Redondo Beach, Calif.*
From the Daily Breeze, Feb. 7, 1967: Dr. Ruben Mettler, President said, "It's been a point of philosophy that good security need not be in conflict with getting the job done."

In presenting the award, Brig. Gen. Arthur Exon, Director of Defense Contract Administration Services Region, Los Angeles, said TRW received the award because, "Management being security conscious and cooperative with the Department of Defense Industrial Security Program; education and training programs which made employee's aware of their security responsibilities and motivated them to perform accordingly; cooperation with the defense department's security review procedures; and a progressive program with emphasis on new security methods."

Smyth Research Associates – *San Diego, Calif.*
From a news article in the San Diego Tribune, Feb. 14, 1967: Smyth Research is described as a 12-year old radio physics company with 50 people and a part-time security officer.

Their key to success: "By having no grey areas where some people can be and others cannot," said Dr. Steven Weisbrod, director of research. "We keep all classified material in a safe in the center of the plant. Only three people have the combination. This way we have only one top security area to worry about."

Southern Bell Telephone – *Atlanta, Ga.*
From the Bel Tel News, April 1967: In accepting the award for Southern Bell, President F.M. Malone said, "The security of information and materials relating to our nation's defense is clearly one of the most essential concerns of this business. We must take whatever measures are necessary to provide utmost security, because success in this matter is imperative and failure is unthinkable. I'm sure I speak for all the people of Southern Bell when I say we will continue to meet these responsibilities in a superior manner and that you have our unfailing cooperation as we work together in this vital area."

SAN DIEGO TRIBUNE - 14 Feb 67

Smyth Firm Wins Award for Security

By IAN LEDGERWOOD
EVENING TRIBUNE Staff Writer

There is no barbed wire, no electric fence, no guards or dogs. In fact, nothing could be easier than walking through the front door of Smyth Research Associates on Kearny Mesa.

Despite this open-house atmosphere, the 12-year-old radio physics company yesterday was awarded the James S. Cogswell Award for an outstanding industrial security program.

One of four companies which received the new award in nationwide competition, the 50-man Smyth organization has only one part-time security officer, Dr. Steven Weisbrod, whose main job is director of research.

How then does Weisbrod keep the firm's secret documents secret?

"By having no grey areas where some people can be and others cannot," he said. "We keep all classified material in a safe in the center of the plant. Only three people have the combination. This way we have only one top security area to worry about.

"We can do this only because we have a small company. If you get bigger you run into all sorts of security problems which we fortunately do not have."

Brig. Gen. Arthur E. Exon, director of the Defense Contract Administration Services Region-Los Angeles, presented the award to the company president, Dr. John B. Smyth.

DR. JOHN B. SMYTH
Avoids bureaucracy

Smyth formed the research associates firm in 1955 with a group of seven scientists who had worked at the Navy Electronics Laboratory.

Smyth likes a small company.

"When you get big, you get bureaucracy," he said, "and that I want to avoid."

The Smyth organization, without vast sums to spend like much larger corporations in the same field, researches and finds simpler and cheaper electronics equipment with which to track satellites, look at stars, and study electrons and ionospheres.

One device, the only one of its kind in the United States and no larger than a small suitcase, tracks satellites. It can pick them up when they are over Guam, far below the horizon, Smyth said.

The machine's predecessor needed two cabinets, each over 6 feet high, to contain all its equipment.

Much of the material used in the manufacture of the firm's equipment is made on the spot in machine and carpentry shops where all the files for the library were built.

"If we build it ourselves, we don't have to wait," Smyth said. "And often we want something in the morning. You can't buy it that quickly."

From a news article in the San Diego Tribune, Feb. 14, 1967:

Smyth Research is described as a 12-year old radio physics company with 50 people and a part-time security officer.

Their key to success: "By having no grey areas where some people can be and others cannot," said Dr. Steven Weisbrod, director of research. "We keep all classified material in a safe in the center of the plant. Only three people have the combination. This way we have only one top security area to worry about."

Infinity Systems Engineering, LLC

by Kathy Dolan
Vice President of Industrial Security/FSO

Infinity Systems Engineering, LLC | *Colorado Springs, Colo.*

IN THEIR OWN WORDS

A representative sampling of the 2016 Cogswell winners were invited to share their formula for success with DSS 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.

Infinity Systems Engineering, LLC (Infinity) is a small business with extensive experience in space systems and associated ground systems. Founded in 1996, with corporate headquarters in Colorado Springs, Colo., Infinity provides advisory, engineering, intelligence, and information technology services for the Government sector.

We are an Inc. 5000 company (eight consecutive years) with solid growth for the past 20 years and we are honored to receive our second James S. Cogswell Award. We received the first in June 2008.

Most security professionals comprehend the criteria for their facilities to receive superior ratings, but there is so much more to consider when striving for security excellence. Thus, I will address additional aspects of the security program that may help in creating a perfect environment and the conditions necessary in fostering receiving consistent superior ratings from DSS and may ultimately result in receiving the prestigious James S. Cogswell award.

Maintaining a successful security program in the industrial security field requires implementing a multi-faceted formula. I am very fortunate to work for a company that employs a group of people who strive to be the best in everything they do and considers security a valuable asset to their success.

Management Support

For over 11 years, I have witnessed the benefits of a good management team that leads by example. Without management and employee support, there is no amount of work, no security education and awareness program, and certainly no policy or procedure that could warrant a superior rating from the Defense Security Service. To go above and beyond has to be a total team effort and takes 100 percent commitment from employees at every level.

> To go above and beyond has to be a **total team effort and takes 100 percent commitment** from employees at every level.

Security must be considered as significant as any other department in the company, and no matter the facility size, must earn and retain a seat at the corporate table. That presence is paramount to implementing a successful security program and was demonstrated by the attendance of so many executive-level personnel on stage with their FSOs, when accepting their Cogswell Awards this year.

Management support is one of the primary reasons they are up there — they all realize the significance and importance of this award, and demonstrate their understanding and support with their presence at the award ceremony.

DSS Support

Your Industrial Security Representative is a crucial measure of that formula for success as well. I have been very fortunate to partner with some of the best in the business throughout my career. They have not only provided their guidance and expertise, but they have always made me feel that they are part of my team and I theirs.

The relationship between industry and DSS must be a partnership that together considers the big picture and keeps our eyes on the ball, so to speak. In this business, we all share a common concern; the protection of our nation's assets and our warfighters. What better reason to join forces and do it right?

In addition to all of the facilities that our DSS representatives handle and oversee each day, they strive to take the time to nominate their facilities for this prestigious award. All in all, having a stand-out DSS representative is just as important as your security program.

Networking

Networking by getting involved in the security community is vital. You may not always know the answer, but there is someone among us who does. Reach out, and in turn let others reach out to you. Give when you are called upon and our security community gives back. Don't reinvent the wheel because you don't need to.

Lastly, share, share, share! For every time I have shared a written policy, a security education and awareness presentation, or my expertise to another industrial security professional, it has come back to me in a positive way tenfold.

If you have written a great policy or developed a great security education tool, share it if you can. Don't keep it close to the cuff because if it works well for you, it most likely will work well for others. United we stand, divided we fall may sound cliché, but in our world today those words ring truer than ever.

EOIR Technologies, Inc.

by Diane Moulton
Facility Security Officer

EOIR Technologies, Inc. | *Fredericksburg, Va.*

EOIR Technologies, Inc. provides advanced C4ISR solutions in support of the U.S. military and intelligence agencies. With 35 years of experience, we have earned a reputation for excellence in solving complex problems, delivering practical solutions, and driving innovation across a wide range of technologies, platforms, and devices.

We strive for excellence in all facets of our business to include our security program and it is an honor to be recognized by DSS for our diligence in this area.

When I first took on the role of Facility Security Officer (FSO) in April 2007, our security program was Satisfactory, but there was plenty of room for improvement. Our journey from Satisfactory to consistently Superior was full of challenges, and I attribute our success to three key areas: networking, an effective corporate-wide communication strategy, and the utmost level of support from our senior management team.

Networking

I recall being so anxious when I approached EOIR's first assessment that two weeks prior to the assessment, I reached out to an FSO acquaintance for advice. This first experiment with networking proved to be critical to our success and significantly enhanced our results.

With great patience and guidance from our DSS Senior Industrial Security Representative (ISR), we pulled out a solid Satisfactory that year by ensuring that we fully met all requirements of the National Industrial Security Program Operating Manual (NISPOM).

From that time forward, I incorporated this best practice into EOIR's security program on all future assessments. At the recommendation of the Senior ISR, I further expanded my network by joining a pilot program that he and a fellow FSO were forming known as the Quantico Area Industrial Security Council (QAISC). This proved to be an extremely worthwhile endeavor and provided me with a tremendous resource for peer mentorship, continuous learning opportunities and professional networking.

The payback was so great, with the support of my senior leadership, I continued to invest time in working with the Quantico area security community and DSS leadership; and in 2010, I was voted the chairman of the QAISC, a position I continue to hold.

There are more than 550 members of the QAISC today, but when I joined in 2007, the organization was comprised of only about 30 FSOs in the Quantico region. At that time I was new to the administrative responsibilities of managing a cleared facility. The monthly meetings were incredibly educational and expounded on the responsibilities of an FSO under the NISPOM.

In addition to the monthly meetings, we regularly network with our DSS counterparts, counterintelligence and FBI special agents. They provide valuable updates about what is going on within our industry and engage in question and answer sessions during regular meetings and monthly lunch-n-learn teleconferences which average 100 callers per month.

Staying true to my early success leveraging a mentor when first starting out, we initiated a formal mentorship program to provide new FSOs with an opportunity to connect with more experienced FSOs.

As a result of these interactions, I stay current on the latest security concerns and am able to use this knowledge to constantly improve EOIR's security program. I regularly use the information I gain to mentor our security staff and also to provide guidance to employees in the areas of security. If there is one piece of advice I could offer a new (or even seasoned) FSO, it is to join a local security council.

If there isn't one in your area, start one! You and your company will benefit far more than you ever could by reading the NISPOM or online security articles alone. Having a forum to network with other FSOs and to collaborate on best practices helps make all of our facilities stronger and ultimately strengthens our nation's security.

Corporate-wide Communication

Participating in a networking organization like QAISC has played a huge role in elevating our program performance to consistent Superior ratings, but it's not enough to get us the whole way there. I realized that I needed to find a way to pass on what I was learning to keep EOIR employees apprised of the latest security happenings. I also learned the value of providing reminders about security processes to keep it in the forefront of our employees' awareness as they perform their day-to-day functions.

One successful approach has been conveying the security knowledge that we gain at our monthly meetings through an internal newsletter. We had previously purchased outside stock security newsletters, but these seven-to-eight-page documents were too broad and generic to meaningfully reach our target audience. In this age of Twitter and text messages, we knew we needed to find a more succinct way to reach our employees.

> In this age of Twitter and text messages, we knew we needed to find **a more succinct way** to reach our employees.

Our solution was "The Bullet," a one-page PDF that has valuable information that is directly relevant to our company and is presented in short, quick bulleted lists that are actionable, easily digested and applied. This internal newsletter replaced long paragraphs of security policies with short points to educate our employees on hot topics such as personally identifiable information, cyber security, and suspicious contact reporting requirements.

Since we started "The Bullet," we have seen an increase in reporting to our security department, which has resulted in a better partnership between our security office and our employees.

In addition to "The Bullet," we send email updates on hot topics that may immediately affect our cleared (and uncleared) staff, such as phishing schemes and security travel alerts. With a company as geographically-dispersed as EOIR (we have employees in over 10 states and overseas), it is paramount for us to use a variety of flexible mechanisms that are easily accessible.

For more in-depth topics, we hold special in-person security sessions throughout the year with briefings given by our security staff, a member of DSS or the FBI. These methods of regular communication in a variety of formats ensure that our employees have the education they need to contribute to ensuring that our nation's secrets are safe.

Senior Management Support

Extensive networking and the opportunity to find a successful means of communicating with our staff is possible only because of the strong support we have from our Board of Directors and our CEO. Our senior management team is key to the success of our security program. They recognize that a strong security program is paramount to our defense business, and as such, they are fully supportive of our mission.

As an example, a few years ago our DSS specialist suggested that we increase our security staff to accommodate the growth of our company. Many organizations would have opted to stay as lean as possible on support staff, but our corporate management heeded the suggestion and expanded our security staff to include an export-compliance manager to aid in both security and International Traffic in Arms support.

This expansion of our security program allowed us to expand our support to our employees and focus on honing our security policies and procedures. Having a strong, committed corporate support team has made all the difference in taking our security program to new levels. Of course, none of this would have been possible without our employees and their diligence in remaining current and compliant with our policies and procedures. They are the foundation of our successful security program.

There are many factors that contribute to our success beyond what is listed, but having a strong networking group, being in constant communication with our employees, and having the unwavering support of our senior management team has been critical to our development from a company with a Satisfactory program to one that has been rated Superior for three consecutive years.

NAVSYS Corporation

by Randall G. Kurtz
Facility Security Officer/Lab Operations Manager

NAVSYS Corp. | *Colorado Springs, Colo*

NAVSYS Corporation was founded in 1986 by Dr. Alison Brown. We are a small company, dedicated to promoting the use of GPS in a wide variety of commercial and military applications. Many of the GPS innovations that are now familiar to everyone were first developed here.

Due to our innovative research and subject matter experts, we are frequently targeted by those who attempt to acquire these technologies illicitly. We have developed close working relationships with our DSS counterintelligence special agent, FBI, Department of Homeland Security, Air Force Office of Special Investigations, and others.

Being a small company also presents challenges, as those of you working for small companies know. Striking the proper balance and being able to prioritize are crucial when wearing multiple hats.

You must develop a relationship with your DSS representative; take advantage of their knowledge, perspective, and resources. Our DSS Rep has many years of experience, and she has been an invaluable source of help and inspiration.

I also owe much to our IT Manager/Information System Security Officer, and to a former NAVSYS Facility Security Officer and my mentor. I have since become a mentor myself for other facilities.

As an engineer, I have been in meetings where brilliant engineers vociferously debated some complex issue, when some wise person, often our President, would bring it back on track by saying something like, "Let's go back to Physics 101." The basics are the foundation that we build on.

For security, ultimately it is about protecting our freedoms, our way of life, and American interests and people. Many aspects of security are, frankly, painful to implement and maintain, and not cost-effective, at least on the surface. But in the larger scheme of things, it is ultimately worth it, and our job as FSOs is to communicate that, and to keep security in the forefront of everyone's mind.

Education

Continuous education — awareness and training — is the key to a successful and active security culture. I send out frequent emails and updates, and set up a procedure where employees share in the end of day check, on a rotating schedule. This gives people a sense of ownership and accountability for security that might be lacking if it was never their "official" job.

Entropy is defined as the lack of order or predictability; the gradual decline into disorder. According to Newton's Second Law of Thermodynamics, in an isolated system, entropy always increases or remains the same. This is part of our common experience; spend hours cleaning your house, your desk, your yard, and it seems to spontaneously revert back to disorder and chaos before your eyes. So the idea here is that you must continuously educate, remind, and encourage good security posture. You must develop a culture of security in your organization.

"So the idea here is that you must continuously educate, remind, and encourage good security posture. You must develop **a culture of security** in your organization."

Participation is another key. The Pikes Peak area is blessed to have a great NCMS chapter, Information Systems Security Manager Working Group, and active local government agencies. DSS attends every meeting, and we have frequent seminars, training events, and facility visits from our government partners.

Our President is the Small Business Chair of the local

National Defense Industrial Association (NDIA). NCMS brown bags and DSS online training are also great sources of information. Last year I submitted two posters that won first and third place for new design category at the NCMS Annual Training Seminar in Las Vegas. The net result of all of this is being "plugged in" to the security community.

Get out of your office and circulate among your employees. "His cardinal mistake is that he isolates himself, and allows nobody to see him; and by which he does not know what is going on in the very matter he is dealing with," said Abraham Lincoln, in relieving Gen. John C. Fremont from his command in Missouri, Sept. 9, 1861.

Leading is primarily paying attention. In this way you create a sense of commitment, collaboration, and community, and you gain access to vital information necessary to make effective decisions.

You have to care about it passionately and have a concise statement or picture of where the company and its people are heading and why they should be proud of it. That all adds up to vision. Effective visions make sense, stand the test of time and are stable yet flexible.

An effective vision empowers people and prepares for the future while also having roots in the past. Every chance you get, reaffirm, reassert, and remind everyone of the basic principles of security, and the reasons why it's important.

Finally, remain vigilant and flexible. We live in a rapidly changing security environment, and we are unprepared for the technology of the future. "No one is less ready for tomorrow than the person who holds the most rigid beliefs about what tomorrow will contain." -The Visionary's Handbook: Ten Paradoxes That Will Shape the Future of Your Business

Northrop Grumman

by Shane March
Palmdale Security Manager

Northrop Grumman, Palmdale Aircraft Integration Center of Excellence | *Palmdale, Calif.*

We are honored that DSS awarded the James S. Cogswell Outstanding Industrial Security Achievement Award to **Northrop Grumman**'s Palmdale Aircraft Integration Center of Excellence (PAICoE) in California.

Northrop Grumman's Palmdale center of excellence is a world-class facility which is home to some of the world's most technologically advanced aircraft, uniquely suited for the development, prototyping, and production and testing of aircraft systems, manned and unmanned, critical to our nation's security.

The facility is located on the Government Owned, Contractor Operated U.S. Air Force Plant 42 in Palmdale, Calif. Northrop Grumman's site has received three consecutive ratings of "Superior" in the last three years.

When I retired from the Air Force after 20 years of service, I wanted to pursue a career where supporting the warfighter was the ultimate goal. I chose to work for Northrop Grumman because the corporation recognizes that the work we do matters to our world and its future. Every day we are able to provide our customers high impact, best-value aerospace products and systems through enterprise quality, innovation and superior program performance.

The Palmdale site security team had to think outside the box to maintain a superior level of performance for our facility. As a team, we identified three areas of focus to create an extraordinary security program that represented Northrop Grumman's values of performance and excellence.

Efficiency

Our first objective looked to make our processes and procedures more efficient. We identified subject matter experts for various security assignments, assigned Integrated Process Teams to identify processes that needed to be streamlined, gathered data through customer feedback, statistics, and conducted interviews. We reviewed lessons learned regularly and partnered with our external and internal customers and peers to enhance our work instructions.

The effort put forth by the site security team allowed us to realign our organization and streamline our processes to support current and future operations during a challenging, but exciting time at Northrop Grumman's Palmdale facility.

Self Inspection

Our second objective was to upgrade our current self-inspection program to ensure we maintained a "Superior" level rating from DSS. Maintaining a diverse workforce is one of the main focusses for Northrop Grumman, and I wanted to emulate that value in our security team.

> "**Maintaining a diverse workforce** is one of the main focusses for Northrop Grumman, and I wanted to emulate that value in our security team."

We assigned senior security representatives with junior security representatives to foster a team environment and encourage different perspectives on our security processes. We also partnered with other company sites to support each other's self-inspections. Each site provided an exit report and shared best practices for others to review and implement, if needed.

We integrated DSS observations from previous assessments and National Industrial Security Program enhancements into our day-to-day operations. The integration of observations, various sites, and a diverse workforce was a key factor in ensuring that we were fostering a culture of security awareness and guaranteed continuity at the site.

Networking

The third objective was for Northrop Grumman to remain a valued and trusted partner to its customers and peers, internally and externally. We developed a close relationship with our DSS team (industrial security, counterintelligence and information assurance representatives).

We were also very engaged with our local Air Force Office of Special Investigations and FBI detachments. Furthermore, we hold two officer positions (chair and secretary) at our local chapter of NCMS. We communicate regularly with our government counterparts and industry partners to ensure we stay current with compliance requirements and current threat postures. This allows us to stay well-informed of emerging events and maintain a high security posture across our area of responsibility.

Earning the prestigious James S. Cogswell Industrial Security Achievement award for Security Excellence was a phenomenal achievement for the Palmdale team and Northrop Grumman as a whole.

My team and I could not have accomplished our three objectives successfully without the support of our site leadership team and our partnership with our industry and government counterparts. We look forward to continuing to enhance our processes and encourage innovation for our site security team in the future.

Oshkosh Corporation

by Mary L. Albrecht
Facility Security Officer

Oshkosh Corporation | *Oshkosh, Wis.*

Receiving the Cogswell Award is quite an honor. As many of you know, just to be eligible for consideration requires two consecutive superior ratings in a facility's DSS assessments. Additionally you have to be nominated by your DSS representative to receive the award.

One of the key elements to obtaining this award then, is to have a good working partnership with your DSS representative so he or she feels confident nominating you. **Oshkosh** has a customer-first philosophy, and we focus on delighting both our external and internal customers.

If I had to describe the key to attaining the Cogswell in one word, it would be, "Extra." Going above and beyond to protect classified information shows a company is committed to protecting the warfighter and national security. And without senior management support, the needed commitment won't happen.

There are many people at Oshkosh who go above and beyond — we are committed to making the best products possible, because we know our mission is to save lives. Our innovative spirit helps us to be the best we can be — and that equates to the protection of our customers.

The path to becoming a Cogswell awardee and developing a best-in-class security program requires a change in the security culture of an organization. We started traveling down the road to the necessary culture change by reviewing the DSS Security Vulnerability Assessment Enhancement Matrix.

The matrix was designed to allow organizations to improve by enhancing program content in a way that creates positive impacts on their respective security cultures. The matrix was not designed to serve as a tool to receive points and increase the audit score. You must have a change within the culture of your organization.

We chose to address accountability and control of classified information through increased auditing and recordkeeping, sharing self-inspection results and any corrective action plans with DSS, and creating a sound counterintelligence program cooperating with various intelligence agencies. A trusted partnership with DSS is essential for a successful program.

Professional Development

Proper staffing is also an essential component to developing a best-in-class security program. The professional security staff needs to be provided with professional development. The team members must have the personal drive to embrace higher levels of education and the pursuit of professional certifications such as the Industrial Security Professional, DoD SPēD certifications, or ASIS professional certifications.

With the constant changes in technology and increased use of information systems, it is essential that organizations have dedicated, qualified and certified information technology professionals as part of the security team.

A successful security program should also give back to the security community. If one reflects on the mentors in their past, you will understand the need to develop those new security programs and new security professionals. Though this is part of the DSS mission, they cannot do it alone and industry must shoulder some of that responsibility. After all, we all share the same mission of protection of classified information, the warfighter, and this nation we love.

> "After all, we all share the same mission of protection of classified information, the warfighter, and **this nation we love**."

Documentation

We developed and maintain an assessment binder. The use of the binder allows us to ensure the required documentation is up-to-date and readily available during the security

vulnerability assessment. During the assessment, the binder aids in the streamlining and efficiency of the assessment. Additionally, we use a binder to record our proposed enhancements along with supporting documentation.

While the majority of the enhancements should be noticed by the Industrial Security Representative during the assessment, the contents of the binder serve as a reminder to seek credit for those items not observed during the assessment.

Companies that go above and beyond the NISPOM requirements should receive recognition for their efforts, and we have found that such a binder serves as a reminder to help ensure recognition of all of those efforts.

Our people are dedicated to doing things the right way. Oshkosh has a culture that encourages ethics and compliance by everyone, which enhances our efforts. Advancement in technologies provides a variety of training delivery methods. These methods allow for a vast distribution of both government provided and internally produced educational products.

In summary, Oshkosh is not only dedicated to making the best life-saving products, but also to protecting the information whose release would put our customers in harm's way.

Raytheon Goleta

by Cynthia Cornelious
Facility Security Officer and Site Security Manager

Raytheon Company, Raytheon Visions Systems and Self Protect Systems | *Goleta, Calif.*

Raytheon Goleta Electronic Warfare Systems Self Protect Systems and **Raytheon Vision Systems** are privileged to have been selected to receive the James S. Cogswell Outstanding Industrial Security Achievement Award. It certainly puts all of our hard work into perspective.

With over 1,000 employees between two facilities, and approximately 70 percent of those being cleared employees supporting government classified contracts from various government agencies, our strategy had to be spot on.

I have been the Facility Security Officer for Raytheon Goleta for about three years, and I would have to say, our journey has been about getting past some missteps in order to achieve security excellence. And not just during assessment time, but all day, every day security excellence.

The success we've enjoyed at our two facilities is not complicated. It required a solid security education program, partnership with and commitment from our entire employee population, and the determination to have a security program that went above and beyond the NISPOM requirements.

> "Developing a good security program and achieving security excellence **is like building a sports team.**"

After every vulnerability assessment, we start preparing for the next one, reviewing our security program and making adjustments to our processes with a continuous improvement mindset. I guess you could say that developing a good security program and achieving security excellence is like building a sports team. Everyone has a critical position to play to make the team successful, and you are constantly making adjustments to make the team better.

And when I say everyone, I mean everyone. Whether you hold a clearance or not, you are a part of the team, so it was important to us to make sure that our cleared and uncleared employees alike have an equal understanding of just how crucial it is to have a solid and successful security program.

Our Security Awareness Training and Education program has been the cornerstone of our success. We realize that we have to stay engaged with senior management and our employees, providing security awareness and training that makes sense to everyone and translates to what they do.

Throughout the year we offer several special security briefings from our government partners, and we've tried to base the content on employee feedback. We hold annual security awareness fairs for our employees at both facilities, keeping them abreast of the latest threats, not only while at work, but threats they might encounter away from the workplace as well, to help protect their families.

Each and every employee at both facilities has become an advocate for security, and if something doesn't look right, they know that they can bring the problem to our attention with the full knowledge that we will investigate their issue fully and bring it to resolution.

Our partnerships don't stop with our employees, or senior management. We've built strong partnerships with the FBI and other local and federal law enforcement agencies, as well as our DSS counterintelligence counterparts, which have been invaluable to us.

Our partnership with DSS has afforded us the opportunity to work together with our various DSS representatives to resolve concerns before they become security issues.

So our playbook is not complicated, it really boils down to this:

Staffing – It all starts with making sure that you have the right players in every position.

Understanding – Ensuring that all the players know and understand their individual roles and that they feel secure in the knowledge that they are an important contributor to the team's success.

Commitment – Everyone needs to have the same commitment, drive, passion and desire to be a winner, all of which starts with senior management. And if they don't, every other team member is responsible for motivating them.

Consistency – Don't work your program to pass an assessment. Work your program every day to succeed at what it's designed to do, and that is to protect the classified information that has been entrusted to us. Passing assessments will be the bonus if you do this.

Education – Make sure that you are providing the most up to date security awareness training possible, utilizing all the resources that are available to you, and there are plenty. And it never hurts to seek employee feedback.

Strategy – You must have a plan of action. This speaks volumes to senior management as it makes it easier for them to envision their return on investment.

And last but not least:

Sustainability – Don't make your plan so complicated that you are reinventing the wheel every year; your plan should be easy to sustain.

All of this together spelled success for Raytheon Goleta, and as we move forward, we will continue to look at each and every day as a new opportunity to do what we do best, but do it even better to give us the advantage in our mission to protect the warfighter. Raytheon Goleta Security … We never stop pushing for Security Excellence.

Software Engineering Institute

by Kara Branby
Facility Security Officer

Software Engineering Institute, Carnegie Mellon University | *Pittsburgh, Penn.*

The **Software Engineering Institute** (SEI), a Federally Funded Research and Development Center established by the U.S. Department of Defense, was developed specifically to focus on cyber security and software. The SEI has always viewed the security of our work, as well as the safeguarding of our customer's data, as paramount to our success.

We are continuously challenged as an institute as a result of our diverse efforts and mission. On one hand, we actively support many customers and cleared efforts throughout the Department of Defense and the Intelligence Community. On the other hand, we conduct fundamental research for the good of the software engineering community, and our staff is comprised of numerous faculty members immersed within the academic community.

The 2015 DSS Targeting U.S. Technologies report identified academic solicitation as the top method of soliciting classified and unclassified but critical information from cleared contractors. As a cleared entity closely associated with Carnegie Mellon University, we are especially aware of the threat to our cleared employees and the work that they do.

Because of these challenges, the security department at the SEI has worked hard over the past few years to create a solid and comprehensive training and education program which encourages our employees to work with security by putting together transparent information about security procedures and requirements.

Education & Training

One of our biggest assets as an institute is our positive stance on training and education. The security department determined a few years back that our staff just didn't know enough about their clearances, reporting requirements, and general security policies at the SEI from emails and mailers sent to employees.

Beginning five years ago, we revamped our entire refresher training program starting with scheduling presentations that all employees had to attend in person annually. Our management got involved as well and kept track of which departments had delinquent employees to encourage 100 percent attendance at training sessions.

Our training sessions cover required topics, but we have also included many impactful topics such as a current events section using the DSS Targeting U.S. Technologies report to drive home trends we see affecting our employees, as well as a rotating section in the presentation to highlight a current area of concern. To date, this section has covered hot-button topics such as classified content in the media, insider threats, as well as the OPM data breaches.

The SEI also conducts annual training with uncleared staff, in addition to our cleared staff. Training for uncleared staff focuses on understanding the threat to our company, ways unclassified information could be targeted, and reporting requirements all staff should know and understand.

While in-person training is labor intensive to the security staff and pulls researchers off work for an hour a year, the benefits far outweigh the costs. Employees know their security officers and are comfortable coming to them with questions or concerns. We elicit lots of reporting following these sessions and it gives employees the chance to have questions answered in person.

The SEI realized that we had a lot of training requirements for our employees and that the old fashioned spreadsheet system was no longer working. We worked with our IT staff to create an application to track training across the institute. This application can identify specific employees for training, how often a training course should be taken, and can accept either "click to acknowledge" or uploaded certificates for validation of completion.

This has been a wonderful asset to our program and removed a huge workload from our staff in maintaining lists and following up with delinquent employees on computer-based training requirements.

Travel Support

The SEI security department has also developed a well-rounded foreign travel program, comprised of pre-travel training, support for our travelers while abroad, as well as debriefing and follow-up support upon their return back to the United States.

One hundred percent of our personnel traveling outside of the United States receive a defensive travel briefing specific to the country that they are traveling to. In some cases, especially when our personnel are traveling to an austere location, we provide a full-blown "pre-deployment briefing" focusing on the threats present within the destination country, as well as the resources available to the travelers in times of need.

The security staff also keeps a watchful eye on world events to ensure SEI personnel are kept out of harm's way. In the event of a catastrophe abroad, the security department enacts a recall process to confirm the whereabouts of all known travelers, as well as their well-being.

Finally, the security department keeps an active relationship with all travelers following their return, performing debriefings upon return, as well as government reporting when applicable.

Ease of Access

In addition to our robust training program, the security department's core values include easy and clear access to security information and staff. The security department at the SEI has its own dedicated wiki page to keep SEI staff up to date on all security related information. This allows us to post our policies and procedures for all staff to access, give information about resources and how to request clearances or report foreign travel.

Our department also writes a blog that employees can subscribe to that covers topics of security in the news, important information such as CAC expirations, and periodic general security reminders.

As part of our online presence, our security department has a service desk — just like our IT help desk. This service desk allows for a one-stop shop for employees to request clearances, access to space, and CACs, as well as submit required reporting such as suspicious contacts, foreign travel notifications, and personal status updates.

It also allows the security department to track request statuses, run reports, and create metrics. The best part is that our service desk is tied into our wiki, so as an employee searches for a request type, they can be directed to our policy page directly on the topic for more detailed instructions or answers so they no longer need to enter a ticket.

Educating our staff and providing clear guidance to them regarding security policies and procedures has led the SEI to cultivate a strong-security minded workforce. These practices help guide the SEI to provide quality work and services to our government customers.

Ultra Electronics Advanced Tactical Systems, Inc.

by Shona Nietsche
Facility Security Officer

Ultra Electronics Advanced Tactical Systems, Inc. | *Austin, Texas*

No one wins a James S. Cogswell Outstanding Industrial Security Achievement Award alone. It takes everyone working together like an orchestra. Each group, like an instrumental section, plays their part and wants to be heard.

With the facility security officer (FSO) conducting, a program can develop from a cacophonous rattle to a beautiful and harmonious symphony and, just as with music, it is easy to tell when you are hearing something special.

At the heart of the orchestra is the string section, the security team. Security professionals have to be well-educated in their craft and willing to go the extra mile. All good security people take opportunities for training, and there are many, including the Center for Development of Security Excellence and NCMS: The Society of Industrial Security Professionals.

> “Security professionals have to be well-educated in their craft and **willing to go the extra mile.**”

Training is critical to staying current with the requirements and best practices. However, this is only the basic melody. Winning a Cogswell takes layers. To add harmony — or enhancements — to the tune, a security professional must look for new ways to prove what they are doing is actually working.

For example, at our organization, **Ultra Electronics Advanced Tactical Systems**, we flipped our employee security education to a discussion-based model. Whether it is our variation on a brown-bag called “Snack Time with Security” or our annual training, our employees have to debate and discuss the material to show they didn’t just hear it, but they know it and are engaged with it.

Employees

This provides the bridge to our next orchestral section, the woodwinds, employees. Woodwinds, like employees, have a great variance in tone, can be idiosyncratic and sometimes difficult to orchestrate. When they are engaged, however, they bring a richness and color that fills out the harmony and can even provide a vital counterpoint.

It is easy, as a security professional, to say “these are the rules to obey” and forget that employees are customers with varying needs. Working with employees, letting them push the envelope and force you out of your comfort zone, looking for solutions while staying within the regulations, is what makes a cutting-edge security program.

Open dialog keeps the engagement high, which is critical to winning a Cogswell award. More importantly, having engaged voices throughout a business shows management that security is key to a company’s success.

Management

Our brass section, management, are often strident and dynamic. They are considered directional instruments, and understanding this is critical to building a harmonious relationship with the rest of the orchestra.

An award-winning security program has to be in tune with the direction that management is facing. Aligning with that direction without being overwhelmed by it is the challenge of the FSO.

Balancing the needs of the business with the requirements set forth by the National Industrial Security Program and DSS is foundational to any security program. Finding ways to make these two disparate groups perform together harmoniously is the greatest challenge, and

provides the greatest rewards. Aligning management with DSS makes beautiful music indeed.

DSS Support

DSS fills our final section. Percussion is commonly referred to as the backbone of a musical ensemble, and it is their underlying rhythm that drives the entire tune. Whether is it subtle or crisp, it is the beat of this section that keeps everyone in time with the music and provides constancy across all parts of the ensemble.

Winning a Cogswell award isn't easy. It takes a lot of people working together in every sense of the word and doing so over at least several years. From the highest level of management to the lowest ranking employee, the director of DSS to the guard at the front desk, every note has to play together in harmony.

And if you try to win a Cogswell alone, you are merely whistling in the wind.

"We are the music makers, and
we are the dreamers of dreams."
– Arthur O'Shaughnessy

SES Government Solutions

by Tammy Breeding
Facility Security Officer

SES Government Solutions | *Reston, Va.*

SES Government Solutions (SES GS) is a Foreign Ownership, Control or Influence (FOCI) mitigated company, operating under a Proxy Agreement, which provides satellite communication products and services to U.S. government agencies. One of SES GS' top priorities is to meet the mission critical deliverables for our customers while safeguarding sensitive information.

In order to build a successful security program, you must have genuine support from senior management. Our CEO's commitment to security efforts is a key enabler of our robust security program. The CEO trusts me to be proactive in meeting government security policies and directives, as well as projected future requirements and communicating those issues with solutions, in advance of facility implementation.

As a result, I've been able to ensure our program has received high marks during DSS assessments. As a result of our Superior ratings and history, DSS nominated SES GS for the 2016 Cogswell award. Competition is fierce. The Cogswell award is the most prestigious honor DSS may bestow to an industry security program. This year, SES GS was one of the companies (out of more than 13,300 cleared contractors) to receive the coveted award.

> **Competition is fierce.** The Cogswell award is the most prestigious honor DSS may bestow to an industry security program.

When I joined SES GS in 2012, previous security ratings were Commendable, but the previous security administration had not pursued the 13 new National Industrial Security Program (NISP) enhancements. Adding to this challenge was a change in our cognizant DSS office and a new DSS industrial security representative (ISR). Our controlled secure areas and sensitive compartmented information facility (SCIF) areas were required to support operations, so no downtime was permitted. And, to make things really fun, there were internal discussions about moving our headquarters office to another location in the near future.

Upon arrival, I completed a DSS Self Inspection Checklist (handbook) and invited the new DSS ISR to our facility for a "Site Assist Visit." I wanted to talk to him about elements where I felt we met the NISP requirement and obtain his guidance prior to the annual security vulnerability assessment (SVA). We had a few months to get things in order and prepare for the annual SVA and the new rating matrix with enhancements. The SES GS security team reviewed the Self Inspection Checklist and developed plans to improve weak areas and ensured SES GS met the new requirements.

The new ISR arrived and spent approximately four hours with us reviewing inspection documents and NISP enhancement qualifying elements. In the end, we were in agreement where enhancement points were earned and identified other potential enhancement areas which may require additional support. Our ISR asked thought-provoking questions for which we devised a series of solutions.

After this meeting, I developed a plan on how SES GS would meet its future security goals. This was the beginning of the journey to the Cogswell Award, and it all started with establishing a healthy communication line with the ISR, being receptive of his guidance, and a CEO who encouraged and supported the FSO. DSS helped SES GS institute an enhanced security program.

During the initial review of the SES GS security program, I took a personal approach and created:

- A security motto: "Risk accepted by ONE is shared by ALL"
- A security mascot: The SES GS Secret Squirrel, who appears on all security messages
- A security corner where many informative pamphlets are presented for easy access

SES GS worked hard to reduce known deficiencies and concentrated on meeting each NISP enhancement. I prepared a "forecast" spreadsheet which lists each NISP enhancement by category number and definition, and then added dates and event names which met category requirements. The spreadsheet has a column which allows us to document "proof of validity" and describe how each enhancement can be verified. This "forecast" is a living document updated throughout the reporting period.

Updates that impact the facility or electronic communications are shared with our ISR as soon as possible. Thanks to our transparent processes and open dialog, our ISR is aware of what is happening within the facility at all times. I believe in being very transparent with DSS regarding all updates and processes.

DSS Support

When asked, I provide the following advice to fellow FSOs: Be sure to include the DSS ISR into your discussions and keep them aware of changes in your business. This will only strengthen your security program. By executing this collaboration of tools, one will avoid choosing a bad path. Collectively, with your DSS partner, you will establish a healthy robust security program.

Each year, SES GS tries to host two guest speakers for counterintelligence and cyber security update briefings for all employees. As part of that effort, we received counterintelligence briefings from DSS CI, NSA, FBI, and a former CIA analyst. We have also shared three FBI movies with our employees.

Additionally, our DSS FOCI officer and counterintelligence special agent have a wealth of knowledge and proven strategies when it comes to assessing risks, avoiding vulnerabilities and executing an effective counterintelligence program. Their advice and training in FOCI and counterintelligence have been a life-blood to our security program and been instrumental in SES GS' pursuit of a healthy and robust security program.

Self Inspections

SES GS security staff performed several self-assessments, to include:

- Daily review of several group and filtering email mailboxes in support of identifying vulnerabilities in reference to exports, suspicious contacts, and foreign ownership, control, or influence
- Monthly information management system and DoD safe content inspection
- Monthly security keys log inspection
- Monthly personal effects inspection
- Monthly random telephone log inspection
- Monthly alarm activity report inspection
- Monthly badge reader report inspection
- Quarterly comparison of telephone bill per extension with employee telephone logs

A monthly/quarterly certification of completion for each of the above inspections is processed by the FSO and electronically archived for review during the annual DSS site visit. The SES GS Government Security Committee (GSC) uses these reports for tracking trends and uses the data from these monthly inspections as reference points. The GSC report information is used to prepare charts and graphics to assist in the analysis of past and present data trends.

Each year, I present a short review (refresher training) of the year's security events and key activities just prior to the annual SVA. The refreshers are a great time for employees to ask questions and for me to gauge employees' knowledge of security requirements and procedures.

Employees receive travel warnings and travel bulletins on a daily basis. Since we have employees who travel internationally, we provide both international and domestic travel alerts. Employees are alerted to airport delays and closings, airport strikes, blizzards, fires, health epidemics such as the measles and the Ebola virus, local unrest and riots, etc. This allows traveling employees to be armed with the latest information regarding visits to areas where a greater degree of caution should be exercised.

Monthly security messages and a Quarterly Security News bulletin are shared with employees as well. Games with prizes stimulate employee security awareness. SES GS

shares information with other security colleagues and is willing to help others when possible.

Get involved! Co-hosting security events created cross-pollination and efficiency when it comes to sharing resources. Mentoring future security officers also helps reinforce many rules and regulations. There are many ways to support others in the security community and win NISP enhancement points while helping a fellow security officer.

SES GS stores all information electronically with partitions to include accessibility to the security staff only. The company advocates for electronic storage and tracking of security documentation whenever possible.

FOCI companies must manage additional documentation not required of non-FOCI companies which can sometimes be a challenge. At SES GS, we use an electronic policy tracker to identify those who have completed or not completed security briefings.

Briefings are conducted in person and over the phone. PowerPoint presentations prove to be very effective when exams are included as employees must demonstrate mastery of the material in order to successfully answer exam questions. This holds employees accountable for learning the information.

Exams also provide feedback to the FSO on how well employees are saturated in security protocols and, the depth and breadth of your organization's security posture and culture.

The SES GS CEO and the GSC have always been supportive of our security endeavors. In the end, I love the challenge and appreciate the partnership I have with my corporate management team, as well as DSS.

Director shares his vision

By Nathan Taylor
Office of Public and Legislative Affairs

"What struck me from the start of my time at DSS was the quality of the people, and the quality of the work being done," said DSS Director Dan Payne during his opening remarks at a June 1 town hall meeting at the Russell Knox Building (RKB), Quantico Va.

"I have visited some of our field offices and I can't say enough about the quality of the people that work for this agency," Payne said during the roughly hour and a half meeting. "In my opinion, we are the ones bringing together the FBI and some of the other agencies out in the field because of our people and their expertise in what they do."

The town hall, Payne's first since becoming the DSS director, was streamed live to offices throughout the building and to DSS field offices across the country. The live stream allowed those who wanted to "attend" the meeting to do so, regardless of space or distance concerns.

According to Payne, the threat environment shows why DSS and its mission are more important now than ever before.

"I would say at least two to three times a week I read something involving the theft of information from industry," Payne said. "We see some of our adversaries teaming up to steal our secrets. They are stealing our information and making it better before it is classified."

Payne cited rapid technological development, increased globalization, the use of nontraditional collectors and foreign business practices as some of the main reasons for the increase in foreign acquisition of classified information and technology.

"We are at the forefront of protecting our secrets," Payne said. "We [the United States] are losing a vast amount of information; this cannot stand."

Payne's remarks centered mostly on what he sees as the state of the agency, his goals for the agency and where he wants to move the agency during his tenure.

As with all agencies in today's fiscal environment, DSS has had to learn to do more with less, a skill that DSS does better than anyone else, Payne said. With more than 13,000 classified facilities falling under the National Industrial Security Program (NISP), DSS has roughly one industrial security representative for every 63 sites in its jurisdiction.

Payne also addressed how policy can lag behind operations. Like most government policies, any changes to NISP policy requires a lengthy process involving different branches of government and input from various parties. For instance, the recently released NISP Operating

at first town hall

Manual (NISPOM) Change 2 took roughly two years for coordination and approval, which for Payne is far too long.

"I am concerned about the rigidity of the NISPOM," Payne said. "We, as an agency, deal with a very flexible threat. I want us to move toward a model that is focused less on a compliance-based approach and more focused on a tailored security program."

Payne cited Australia as one nation that is moving toward a more flexible, tailored program for their version of the NISPOM as an example of where he would like to head.

Payne emphasized two main points as important for the agency to focus on included a move to a risk-based model of security and closer integration between counterintelligence and security. "I want to see DSS as a more integrated part of the intelligence community," he said. "This would open up a greater amount of resources that would be available to us."

"We formulate security policy based on the threat picture," Payne said. "CI brings us what that threat picture looks like. We can't have one without the other."

Other priorities Payne mentioned included a focus on workforce development, increased top secret computer connectivity in the field, leveraging the DITMAC as a mission resource, and increased responsibilities for DSS as a part of the Defense Security Enterprise.

Payne fielded a number of questions during the event most of which focused on internal quality of life policies. He also announced an "Ask the Director" program, which allows employees to submit questions or concerns, anonymously or not, directly to him via a link on the agency intranet, drop boxes within the RKB or via representatives of the DSS Employee Advisory Council.

TOP: Fred Kollaram (left), Office of the Chief Information Office, and Dr. Carey Williams (center) and Madeline Holler, both of DSS Equal Employment Opportunity Office, listen to the director's remarks. **MIDDLE:** DSS Director Dan Payne shares his vision for the agency. **BOTTOM**: Thomas Benner, DSS Security Office, asks a question during the town hall.

A Q&A with **Troy Littles**, Chief of Staff

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

Troy Littles joined the Defense Security Service in February, 2011, as the Executive Officer to the Director. In November 2015 he was selected as the Chief of Staff and appointed to the Senior Executive Service. As the Chief of Staff, Mr. Littles exercises leadership by managing, directing, and coordinating day-to-day operations of the agency. He is responsible for interpreting and implementing higher level policies and regulations that directly shape and improve DSS operations and customer interaction throughout the agency.

As an advisor to the Director, Deputy Director and the DSS seniors and staff, he provides advice and assistance on a variety of matters that are typically complex, technical, sensitive, multifunctional and broad in scope and impact. In close coordination with the Director and Deputy Director he develops short- and long-term plans for DSS by establishing program objectives and identifying required resources in order to promote an efficient, economical and progressive organization.

Tell us about your background.

I grew up between New Jersey and Florida. I always had a desire to serve my country so I joined the Marine Corps Reserve after I graduated from high school. My mother had to sign the paperwork allowing me to enlist because I wasn't 18. The Reserve allowed me to serve my country and complete college at the same time.

While attending Longwood University, the head of the ROTC department contacted me and asked me to come see him. He explained the benefits of the Army ROTC program and convinced me to leave the Marine Corps and join the Army as an officer. After graduating from Longwood I was commissioned as an infantry officer. I served four years as an infantry officer before I moved to the Military Intelligence Corps.

Over the next 26 years I was honored to command and lead soldiers and civilians in garrison and combat. I served in the XVIII Airborne Corps, NATO and in three combatant commands, and I have had several overseas deployments in support of combat operations.

What lead you to this position?

After I retired from the Army, I began my government career as an Army civilian working in Colorado Springs as the Chief, Operations & Intelligence Support Division, United States Army Space & Missile Defense Command & Army Forces Strategic Command. The previous Director of DSS, Stan Sims, contacted me and asked me if I would be interested in becoming his Executive Officer, as he was recently selected as the Director of DSS.

I knew Mr. Sims because we had served together as soldiers on the XVIII Airborne Corps, G2 Staff. I've been asked countless times if I ever worked for Mr. Sims before DSS and the answer is no. I was, however, able to observe him daily and his leadership style and after he explained to me the DSS mission and its importance to national security, I agreed to move to Virginia to become his Executive Officer.

Prior to being selected as the Chief of Staff, you served almost 5 years as the Executive Officer. How did that prepare you for the Chief of Staff position?

Serving as the Executive Officer for the Director was a rewarding experience personally and professionally. The exposure to DoD and DSS senior level strategic thinking and decision making was unsurpassed. I think those experiences were an excellent preparation for becoming the Chief of Staff. I already had an outstanding relationship with the deputy director, senior staff, employees and our industry partners so that made the transition to the chief position very easy. Over the years I was involved in strategic discussions and decisions made by the director, deputy director and seniors on the policies, resources and personnel issues facing the Department and the agency. This personal insight has given me a unique understanding of the corporate decisions taken and the rationale behind those decisions and helped prepare me for the chief of staff position. I still have a learning curve but not as severe as I would otherwise.

What do you see as your role and that of the Chief of Staff offices?

My role as the chief of staff is to coach, mentor, and lead the staff. I see myself as the staff integrator and synchronizer. This is achieved through a comprehensive understanding of the director's vision and the development, management, prioritization, and synchronization of the processes and efforts of the agency. I work behind the scenes solving problems, mediating disputes and dealing with issues before they are brought to the director. In conjunction with the supporting offices we provide timely support and guidance to our mission directorates to allow them the flexibility to accomplish the industrial security mission by ensuring there are no roadblocks to mission accomplishment. We always work to provide the resources needed to accomplish the mission while ensuring we follow applicable rules, regulations and laws.

The Chief of Staff offices are a disparate group (i.e. Security, Acquisition, Public Affairs, Human Capital Management). What are the challenges associated with managing such a diverse group?

My challenges have been minimal and that is because I am very fortunate to have an outstanding group of senior leaders who support me. My leaders are the subject matter experts in their areas and I have confidence in their ability to do their jobs and lead their people. We have open and transparent dialogue amongst our team and this has led to a better working relationship with our internal and external stakeholders. I provide leadership guidance and direction, ensuring we are operating within the guidelines, goals and objectives set by the director.

What do you see as your role in supporting the director and his vision for the agency?

Through our DSS Strategic Plan (2020), we established short term and long term goals and objectives for the agency. This plan, along with the director's annual guidance, provide the foundation for our engagements with stakeholders. I am a key messenger and champion for his vision. I see myself as one of the principal interfaces between the director, our employees and our stakeholders. In my capacity as the chief, I interact daily with stakeholders and I am often asked about the director and his vision. Through these documents I am able to articulate a clear and consistent message concerning the director's vision for the agency.

What are your priorities as Chief of Staff? What areas do you intend to focus on?

I have to ensure the staff is prepared to support the agency goals set by the director and the senior leaders of the agency. These priorities include:

- Workforce development
- Risk-based approach
- DoD Insider Threat Management and Analysis Center
- Defense Security Enterprise transformation
- Information technology and cybersecurity

With that said, I do have some areas that I will focus on during the upcoming year. These include:

- Standing up the agency Diversity and Inclusion Council
- Improving our agency EEO processes and procedures
- Establishing the DSS Leadership Development Program.
- Improving our agency Mission Assurance Programs
- Improving our acquisitions processes and procedures
- Improving our agency anti-terrorism and force protection programs

The agency is very different from when you arrived in 2011, as is the position of Chief of Staff. What is the most notable change you've seen in the position and the agency?

DSS is a much different agency since my arrival in 2011. I believe there is recognition in the Department of the expertise that DSS brings to the industrial security mission. I remember reading a document shortly after I arrived that proposed disbanding DSS and parceling out the industrial security mission to other agencies. Today there is no such talk; we have proven our worth in the industrial security mission space. DSS interaction with our industry partners has also changed. We have come to a realization that in order to defeat our adversaries we must be united in our approach to security. We must work together to protect our sensitive technology. Our partnership with industry is much stronger and transparent than when I arrived in 2011. We work together to solve problems and our internal processes have improved greatly. For instance, National Interest Determinations, streamlining the facility clearance process, the risk management framework, the counterintelligence partnership with industry and our advise and assist visits by our IS Reps are some of the changes that have occurred. We are a different and stronger agency.

CDSE recognized with Horizon Awards

by Rachel Mongeau
Center for Development of Security Excellence

Results are in: the Center for Development of Security Excellence (CDSE) won six bronze medals in the Horizon Interactive Awards 2015 competition within the Training/E-Learning category. These products were all developed internally by CDSE staff. By earning more than four Horizon Interactive Awards, CDSE earned the distinction of being a "Distinguished Agency," which is a title given to agencies and developers who consistently demonstrate high quality work.

The Horizon Interactive Awards, now in its 14th season, is one of the most prestigious awards in the field of interactive and creative media. The competition recognizes and awards the best websites, videos, online advertising, print media, and mobile applications. Since 2009, CDSE has won a total of 43 Horizon Interactive Awards.

Entries were judged by an international volunteer panel of industry professionals with diverse backgrounds and various roles within the interactive media and advertising industries. Judges look for the best blend between creativity and functionality. Each entry was judged on the following:

- Solution creativity and originality
- Overall graphic design / appearance / user experience
- Communication of message
- Technical merit
- Effectiveness of solution

This season's competition saw over 1,100 entries from 21 different countries around the world and all 50 states.

And the winners are:

Business Structures in the National Industrial Security Program (NISP) Course

Under the terms of the U.S. government's NISP, any prospective contractor company requiring access to classified information must first be found eligible by the government for a facility security clearance. Industrial security representatives (IS Reps) help determine a company's eligibility for this facility clearance. IS Reps are responsible for examining and verifying a prospective contractor's business structure and then following the clearance requirements for that type of business. This course describes the most common business structures in the NISP.

Counterintelligence (CI) Awareness and Reporting Course for the Department of Defense (DoD)

The CI Awareness and Reporting for DoD Employees eLearning course was designed to meet a new DoD policy requirement that all personnel receive CI awareness training within 90 days of assignment or employment, and every 12 months thereafter.

The eLearning format is vital to personnel in locations where training from an experienced CI special agent isn't available. This course has been adopted by several agencies to meet their annual CI training requirement. There have been over 200,000 completions each year or 25,000 completions monthly at no cost to the customer.

Closed Area Practical Exercise

CDSE created the Closed Area Practical Exercise as part of a course for newly hired IS Reps. The exercise provides a scenario in which an IS Rep inspects a room in a contractor's facility to identify options for transforming the existing space into an area meeting the requirements to hold classified information (a closed area). The IS Rep must apply his or her knowledge of industrial security requirements to inspect the room and make recommendations.

Simulation software and audio were used to simulate the IS Rep's experience in the contractor's facility. Students first guide an IS Rep avatar through a practice inspection of the office waiting room. Next the IS Rep avatar meets with the facility security officer avatar for an orientation to the facility.

Students are then able to manipulate the IS Rep avatar to conduct a timed (40-minute maximum) inspection by placing any items of interest in a virtual briefcase. The avatar returns to the waiting room when finished, and students compile a report using the notes collected in the briefcase.

Competency Preparatory Tools (CPTs) Instructional Short

CDSE's Security Professional Education Development

By earning more than four Horizon Interactive Awards, CDSE earned the distinction of being a "Distinguished Agency."

(SPēD) Program is part of the DoD initiative to professionalize the security workforce. This program is intended to ensure there is a common set of competencies among security practitioners that promotes interoperability, facilitates professional development and training, and develops a workforce of certified security professionals.

The SPēD Program developed CPTs to provide security professionals with insight into their mastery of the facts, concepts, and principles the DoD community deems critical. These CPTs are just some of the resources security professionals can use to prepare for one of the SPēD certification assessments.

The course provides an explanation and demonstration of how to use the CPTs to prepare for SPēD certification and includes opportunities for hands-on practice and links to additional resources.

DoD Security Specialist Course

CDSE developed the DoD Security Specialist Course (SSC) for entry-level DoD and federal agency civilian, military, and contractor security professionals. The course is delivered asynchronously using a Collaborative Learning Environment (CLE) over an eight-week period.

In total, the course consists of 24 lessons bundled into seven modules. Students gain knowledge by watching pre-recorded instructor presentations, completing practice activities, and participating in discussion forums with their instructor and fellow students.

CDSE provided 24 pre-recorded instructor presentations to Horizon for judging. These presentations provide foundational course information using a visually engaging style to pique students' interest, gain their attention, and contribute to increased content retention. The video format also lets students pause and replay the content, lending to better understanding and an enhanced learning experience.

In order to apply knowledge gained from the presentations, students complete practical exercises. A sample practical exercise was also provided to Horizon for judging. The sample includes links to video tutorials created by CDSE related to operating and changing the combinations of specific locks.

National Industrial Security Program Oversight Course (NISPOC) Lesson Presentations

CDSE developed the NISPOC for newly hired IS Reps. The course is delivered using a CLE over a four to six month period. In total, the course consists of 29 lessons bundled into five modules. Students gain knowledge by taking suggested eLearning courses, reading assignments, participating in live webinar sessions, completing assignments involving on-the-job interactions, and participating in discussion forums with their instructor and fellow students.

Six lesson presentations developed specifically for the NISPOC course were presented to Horizon judges. These presentations were designed to meet several specific communication needs of IS Reps, including the ability to conduct entrance and exit briefings, prepare security vulnerability assessment reports and letters to management, and determine the effectiveness of a security program by demonstrating effective interview skills.

To learn more about CDSE award-winning products, visit **www.cdse.edu/about/awards.html**

Evolving risks, new DSS initiatives the focus of FOCI Conference

by Sara Coonin
Industrial Security Integration and Application

DSS held its 20th annual Foreign Ownership, Control, or Influence (FOCI) Conference in April 2016, for companies operating under FOCI mitigation. The conference was presented over two days, the first for Outside Directors and Proxy Holders, and the second for Facility Security Officers (FSOs).

"This conference is the primary framework for strengthening the partnership between the U.S. government and select private industry partners with foreign ownership, control, and influence," said Fred W. Gortler, director, Industrial Security Integration and Application. "Dialogue this year focused on the need to address new challenges to securing classified information and technology in the hands of our industry partners."

On the first day of the conference, DSS Director Dan Payne welcomed the attendees and shared updates to the FOCI program, and discussed the role of the agency in the context of an ever-changing, globalized national security environment.

He emphasized that both counterintelligence and security partners need to work closer together to address rapidly evolving threats. He also stressed the need for a continued partnership between the U.S. government and industry, stating that "we cannot afford anything less than a full partnership." He noted that national security information is being stolen at an unprecedented rate due to advances in technology, observing that the National Industrial Security Program Operating Manual needs to be more "nimble" to allow for quick and effective responses from the government.

Keynote speaker Maynard A. Holliday, special assistant to the Under Secretary of Defense for Acquisition, Technology and Logistics, addressed sustaining the U.S. government's technological superiority. Holliday discussed several challenges and changes to the defense industry, such as limited resources, globalization, and competitors taking advantage of some technological parity.

He then explained how to move forward with DoD innovation, stating that technological and operational advances in science, technology, engineering, and math, and open system architecture are key to fashioning a "third offset strategy." He concluded with a view toward the future, explaining that DoD initiatives like Defense Innovation Unit Experiment will work to enhance research and development capabilities, and also emphasizing the importance of recruiting and retaining new talent in the workforce.

DSS hosted three panels on the first day. The first panel, focused on delivering uncompromised products, and included Carrie Wibben, director, Counterintelligence & Security, Office of the Director for Defense Intelligence (Intelligence & Security), OUSD(I); Harvey Rishikof, senior counsel at Crowell & Moring; and Patrick Joyce, principal at Deloitte Consulting LLP. Another panel discussed risk and competition in the global marketplace, and featured David Carey, Barbara McNamara, and retired Air Force General Thomas Moorman, who discussed how their roles as Outside Directors and Proxy Holders have evolved over time. The final panel included enterprise-level directors from DSS, who explained DSS's Risk Based Analysis and Mitigation (RBAM) initiative.

During the second day of the conference the program's focus was more operational, and presentations featured DSS subject matter experts on topics including FOCI trends, policy updates, cybersecurity issues, and the Affiliated Operations Plan Guide, which has since been released to industry.

Finally, the conference featured a panel of facility security officers (FSOs): Sarah Barnhart, Carmine Mele, Nate Millsap, and James Snodgrass. Each shared insights into handling the unique security concerns and processes, procedures, and program developments they have implemented to assist with FOCI mitigation requirements.

In all, more than 300 Outside Directors, Proxy Holders, and FSOs attended the two-day event. "DSS worked with Outside Directors, Proxy Holders, and Facility Security Officers prior to the conference to ensure DSS was addressing their information needs," said Nicoletta Giordani, assistant director of the Business Analysis and Mitigation Strategy division. "DSS continues to work with industry, Outside Directors, and Proxy Holders to ensure the FOCI conference equips them with actionable items they can take back to the C-suite in order to meet DSS security requirements and achieve their operational goals."

Washington Navy Yard visit invigorates DITMAC staff

by Sara Elligson and Sarah Dent
Defense Insider Threat Management and Analysis Center

In June 2016, the Defense Insider Threat Management and Analysis Center (DITMAC) staff visited the Washington Navy Yard, the site of the mass shooting that led to the formation of the DITMAC.

The DITMAC team, accompanied by Mark Allen, Counterintelligence deputy director, met with a team of Naval Criminal Investigative Service (NCIS) special agents and analysts to receive a briefing on the events surrounding the September 2013 events.

The NCIS presentation was led by Special Agent Brian Kelley, honored by President Barack Obama as one of the 2013 "Top Cops" for heroism in saving the life of a fellow police officer gravely injured during the incident. Following the NCIS briefing the DITMAC team visited the memorial at the Naval Sea Systems Command (NAVSEA) and paid their respect to those who lost their lives that day.

In the early morning hours of Sept. 16, 2013, Aaron Alexis, a civilian contractor and prior active duty Sailor, shot and killed 12 NAVSEA employees in Building 197 at the Washington Navy Yard. Multiple federal law enforcement agencies responded to the active shooter situation, and engaged in several firefights with Alexis, who was ultimately killed by law enforcement authorities.

During the discussion and briefing to DITMAC, Kelley and other NCIS responders, who were on scene during the attack, provided firsthand context of the events, response, and investigation related to the mass shooting.

In the wake of the shooting there was a revitalized focus on safeguarding personnel, information and assets, and recognition of the need to revisit reporting mechanisms, collaboration, and information sharing throughout DoD.

In November 2013, an internal review team recommended DoD establish an enterprise insider threat management capability to "quickly analyze the results of automated records checks and reports of behavior of concern and recommend action as appropriate." A memo signed by the Secretary of Defense, dated Feb. 21, 2014, approved the recommendation to establish the DITMAC.

IN MEMORIAM: Members of the Defense Insider Threat Management and Analysis Center visit the Washington Navy Yard Memorial.

What was once an idea on paper grew into a mandate, then a plan, and is now an operational unit — the DITMAC. Incubated at DSS, DITMAC now has a staff possessing varying expertise, to include, counterintelligence, personnel security, analysis, law enforcement and behavioral science.

DITMAC's diversity provides DoD with a holistic view of insider threats. The visit to the Navy Yard reinforced the team's commitment and sense of obligation and duty to thwart future insider threat tragedies.

On the victim memorial inside the NAVSEA building, a quote from Secretary of the Navy Ray Mabus reads,

> "We memorialize as heroes those we lost and pledge that their lives and deeds shine forever bright. It was a day when ordinary people became extraordinary heroes and showed that courage lies in us all, even in the face of tragedy. Thousands returned to work just days later as a family. They would not let fear keep them away. They had a fleet to put to sea."

Leadership Development Program on the horizon

by Kim Colon
Strategic Management Office

The concept for the agency's Leadership Development Program (LDP) is continuously evolving and moving toward the launch of the pilot program in fiscal year 2017. Dr. Fred Bolton, Leadership Development Program manager, recently joined the DSS team. Bolton, along with Larry Cunningham, Leadership Development administrator, and the Leadership Advisory Board (LAB) members are working in an integrative, collaborative effort to create a viable program for DSS employees.

The LDP will change the current DSS leadership development strategy from an "employee-chosen" to an "agency-directed" landscape. In the past, there was no defined approach to leadership development; this program will provide a systematic, guided process that will be agency inclusive.

The DSS program, as well as all programs within the department, must comply with DoD Instruction 1430.16, "Growing Civilian Leaders." DoDI 1430.16 establishes policies, assigns responsibilities and describes procedures for educating, training and developing civilian leaders.

The framework for the DSS leadership program is based on DSS Values and Leadership Principles, which lay the foundation for the program's core components.

The program will be built around two tiers:

TIER 1: GG 7-13

Represents the largest group of employees in the DSS workforce talent pool at approximately 630 employees. This tier constitutes employees from entry/developmental level to full performance. These employees will be expected to implement the fundamentals/core elements of leadership and DSS-specific culture. (The Full Spectrum Leadership Capstone portion of the program is only applicable to GG 12–13.)

Tier 1 objectives are focused on the fundamental/core elements of leadership and DSS culture. They include:

- Identify good/bad behaviors and actions
- Develop communication skills
- Develop interpersonal skills
- Interact well with peers
- Adopt results-oriented approach to roles, positions
- Communicate effectively with supervisors, others
- Interacts efficiently with others

Tier 1 objectives for GG 12-13s will include implementation of the fundamental and core principles learned.

- Develop interpersonal skills, including motivation
- Apply fundamentals
- Operate effectively outside own organization
- Be responsible for results
- Know how to fail well
- Coach/mentor others
- Identify and approach challenges
- Take initiative
- Prepare/be ready to assume higher levels of responsibility

Dr. Fred Bolton joined DSS in May 2016 as the Leadership Development Program manager. Dr. Bolton comes from Averett University where he was an Associate Professor, Dean, and Associate Vice President of Distance Education.

Dr. Bolton is a colonel in the Virginia Army National Guard assigned to the Joint Chiefs of Staff, J7 in Suffolk and also serves as a faculty instructor in the Army War College distance education program.

Dr. Bolton holds a PhD from Virginia Commonwealth University as well as a Master of Public Administration from George Mason University and a Master of Strategic Studies from the U.S. Army War College.

TIER 2: GG 14-15

Represents a smaller portion of the agency population; consists of approximately 200 senior/expert level employees. This tier will focus on an enterprise-wide and global perspective.

Tier 2 objectives include, but are not limited to:

- Brief senior leadership
- Display confidence in material
- Reach across DSS directorates and agencies
- Develop enterprise perspective
- Sharpen strategic vision
- Create change
- Define/resolve challenges
- Achieve results
- Coach/mentor others
- Leverage resources
- Promote continuous development of workforce talent
- Lead/develop others

"The DSS LDP will have some of the most robust and relevant elements of any leadership development program in DoD and across the government," said Cunningham. "Our intent is to deliver a program that is supported by solid research and valid data.

"Our program will provide the training and education, activities, opportunities and experiences that will shape individual leaders and impact collective leadership," he continued. "I look forward to seeing our vision take form as the LDP is launched and we begin a new era of adding to, and developing, great leaders in DSS, for DoD, and across government service."

The LDP is looking for individuals who are interested in becoming a "leadership ambassador." This person would be involved in actively supporting the LDP within their respective directorate, region, office, etc. If interested in participating in the LDP pilot program as a candidate and/or as a "leadership ambassador," please reach out to either Bolton or Cunningham for more information.

Leadership in DSS

In DSS, being a leader is more than a title. It is a responsibility and significant role in achieving organizational goals and mission success. Leadership is the ability to influence actions and provide purpose, direction, and motivation in leading yourself and others toward results. A leader's behaviors, actions and words should exemplify DSS values and principles.

LDP Core Components

Facilitated Leadership Development Workshops

Behavioral Style Self-Assessments

Leadership 360 Degree Assessments

Executive Coaching

Full Spectrum Leadership Capstone

Speaker Series

Periodic Webinars/Brown Bag Discussions

E-Portal

Leadership Development Conference

Reading Assignments

Catalog of Leadership Development Topics

Shadowing/Rotational Program

Individual Development Programs

DSS Values

Our guiding principles of conduct give life to the DSS Mission and Vision and drive organizational success. Understanding, modeling, and communicating them are daily requirements for every member of the DSS team.

- Dependability
- Integrity
- Collaboration
- Respect
- Agility
- Accountability

DSS Leadership Principles

Leadership principles include actions, traits and behaviors. Our principles serve as a compass to guide and stay the course in fulfilling the DSS Mission and Vision. Everyone is a leader in DSS.

- Results-oriented
- Strategic actions
- Investment in self and others
- Influence
- Continuous development
- Communication

Partners in Education:

Building a relationship between CDSE and CI

by Melanie Stagliano
Counterintelligence directorate

"The improvement of understanding is for two ends: first, our own increase of knowledge; secondly to enable us to deliver that knowledge to others."

– John Locke

Education is a cornerstone of the DSS mission. Through the Center for Development of Security Excellence (CDSE), DSS provides a valuable service to its employees, government customers, and industry partners. The DSS Counterintelligence (CI) directorate teams with CDSE in the development and maintenance of CI awareness, insider threat, and cyber security training for government and industry professionals.

By working together to provide a cohesive set of CI courses, CDSE and the CI directorate create more knowledgeable industry security professionals who can pass their knowledge on to the workforce at their facilities. Increased CI awareness is an integral part of protecting critical technology and information in the hands of cleared facilities.

Working with CI subject matter experts, CDSE has developed a wide spectrum of CI training tools to assist cleared contractor employees. These courses integrate CI into industrial security programs and emphasize the reporting of suspicious activities. These courses include:

- Thwarting the Enemy
- Sensitizing Facility Employees to CI Concerns
- The Relationship Between CI and Security
- Protecting Your Facility's Technology
- CI and Security Briefing

These courses were designed to help cleared employees recognize potential threats and emphasize National Industrial Security Program reporting requirements. CDSE recently added three new CI e-learning courses, which brings the total number of CI courses to 14.

CDSE combined several of these courses into a Counterintelligence Awareness Curriculum, which allows students who complete all the courses to receive a CI Awareness Curriculum Certificate. This program provides facility security officers (FSOs) the opportunity to show additional steps they are taking to integrate CI into their security program.

Another way CI supports CDSE is serving as adjunct faculty and briefing blocks of instruction during the FSO Getting Started Seminar. This puts the local supporting CI special agent face to face with the new FSOs working within his/her area.

The more the FSO understands about CI, the more capable they will be in establishing an effective CI program at their facilities. This, in turn, creates an environment of trust and strengthens the partnership between industry and DSS.

In addition, new industrial security specialists receive training through CDSE on CI-related topics to prepare them to work with cleared industry on improving facility security posture. This collaboration prepares DSS field personnel to best support cleared industry.

In addition to eLearning courses, CDSE has hosted 16 CI webinars, to include an unclassified threat webinar. A DSS CI subject matter expert serves as the guest presenter for each of these webinars which cover such topics as:

- Counter Proliferation
- Elements of a CI Program
- Recognition and Reporting of CI Anomalies
- Supply Chain Risk Management

CDSE has also produced more than a dozen Job Aids, many of which are insider threat case studies, which are useful for informing industry and government partners

about the persistent threat from those with access to sensitive or classified information and technology.

CDSE is recognized as a valued source for obtaining CI training. An increasing emphasis on the integration of CI and threat awareness into cleared contractors' security programs is a crucial step in creating a trusting open relationship with industry partners. Reporting from industry is critical to the success of DSS' CI mission and there has been a noticeable increase in reporting from industry as new courses are released.

Fun Fact: In calendar year 2015, there were over 454,000 completions of CDSE CI awareness training

See all the CDSE Insider Threat courses, job aids, and other related information at: www.cdse.edu/catalog/insider-threat.html

CI Awareness Certificate Curriculum

Designed for DoD military, civilian, and contractor security professionals, the Counterintelligence Awareness Certificate Curriculum addresses awareness and reporting, insider threat awareness, the integration of CI into security programs, CI concerns in personnel security and foreign travel, research and technology protection, and threats to defense industry.

The curriculum includes nine CI eLearning courses and three CI shorts. There is a final comprehensive exam that covers all of the material in the course. All of the courses and exams are available in the STEPP learning management system.

Director hosts fifth annual Memorial Day Wreath Laying Ceremony

by Nathan Taylor
Office of Public and Legislative Affairs

The Marines stood silent. On cue from the narrator they came to attention, grasped the wreath stand in their crisp, white gloves and marched slowly toward their destination, just as they had practiced so many times before. The final note of Taps slowly faded away, the narrator thanked those in attendance and the ceremony was over.

The ceremony was the fifth annual DSS Memorial Day Wreath Laying Ceremony held in the quad of the Russell-Knox Building in May 2016, and hosted by the DSS Director Dan Payne.

During his remarks, Payne emphasized the importance of Memorial Day and how the United States is unique in how we honor those who have served in our military.

"America is unique in that we have two specific holidays set aside to honor those who have put their lives on the line to defend our freedom," Payne said. "There is Veterans Day, where we say, 'thank you,' to all of our fellow countrymen and women who have put on the uniform and stood between us and adversaries during both peace and war. But on Memorial Day, we reserve our thoughts for those who made the ultimate sacrifice for our nation."

The origins of Memorial Day can be traced back to the aftermath of the Civil War. Survivors of both the Union and Confederate militaries paid tribute to those who lost their lives in the conflict by leaving flags, flowers, and wreaths at their burial sites and at the sites of battles.

Eventually the practice caught on and was expanded to pay tribute to all military members who died in combat.

According to Payne, the wreath symbolizes the spirit of those that, as President Abraham Lincoln said, gave "the last full measure of devotion," in defense of our country.

Though the day was hot and muggy, turnout was high. Onlookers packed the RKB quad, eager to show their respect and to honor those who gave their lives in defense of our nation, a point Payne emphasized in his speech.

"As we lay this wreath today, let our thoughts go to all Americans who have fallen in the line of duty so that we may stand tall and free," Payne said. "Additionally, let us not forget their families. We must let them know that they are not alone in their sorrow and that their loss is also a loss to the nation."

AT LEFT: Marine Corps Base Quantico Honor Guard members Sgt. Darius Wright (left) and Lance Cpl. Nicholas Gallante assist DSS Director Dan Payne (right) in placing the wreath in front of the U.S. flag in honor of Memorial Day. **BELOW:** DSS Director Dan Payne provides remarks at the DSS Memorial Day Wreath Laying Ceremony.

Management support key ingredient to successful security vulnerability assessments

by Gary Layne
Virginia Beach Field Office
Industrial Security Field Operations

Editor's Note: *The below article is a personal account by a senior industrial security representative about the importance of having senior management attend entrance and exit briefings during a security vulnerability assessment.*

It was a warm August day in 2005, and sweat was beading down my temples. I kept thinking: "Is my tie straight?" "Did I get the cat hair off of my suit?" and "Why on earth am I sweating so much in this air-conditioned building?"

In retrospect, it was probably because I, a young DSS industrial security representative (ISR), was about to meet the president and chief executive officer of the largest cleared facility in Virginia. No matter how much time and effort I'd put into preparing for this meeting, his presence still had me questioning whether I was truly prepared for the entrance briefing.

As a DSS ISR, I was about to lead a team security vulnerability assessment (SVA) at a company with more than 15,000 cleared employees. Once the SVA was over, after five days of team interviews and security checks, I began feeling the same anxiety-inducing worries that I had before the entrance briefing, only this time it was to complete the exit briefing.

My anxiety level might not have been so high had I not planned to meet with senior key management personnel (KMP). But I learned that senior KMPs can have long-lasting impacts on the industrial security program; therefore, including them in entrance and exit briefings directly correlates with the effectiveness of the SVA.

One of the prime lessons we learn from the corporate world is that first impressions can last a lifetime. It is essential to enter each facility fully prepared, both physically and mentally. This includes dressing professionally, completing thorough research, and preparing your mind for the SVA.

> "As the builder of U.S. Navy nuclear-powered aircraft carriers and submarines, I believe our people, our products and our facilities are all national assets. Providing a safe and secure infrastructure is paramount, while also being compliant with the National Industrial Security Program Operating Manual. The SVA entrance and exit briefings with DSS allow for an exchange of information about our protective measures of classified information, and it gives us a better understanding of DSS' concerns, priorities and expectations. It is through these candid conversations that we are able to continually grow, develop and learn new ways to strengthen our security compliance program."
>
> – **Matthew Mulherin,** President, Newport News Shipbuilding

Management immersion is not only vital to the success of the industrial security program, but in my experience, I have observed this support is in fact the key ingredient

SETTING THE SCENE: Susie Miller (left), ISR in the Virginia Beach Field Office, conducts a mock entrance briefing with Ann Gardner (center), AMSEC LLC director of administration, and Sharon Bishop, AMSEC LLC corporate security manager.

that separates those rated satisfactory or lower from those rated commendable or higher.

Through my 16 years as an ISR, I have made it my mission to express to FSOs the significance of senior management participation in briefings. Occasionally, senior managers are not available at the time of the SVA. This is why it is vital to establish a relationship from the very beginning of the facility clearance process.

I suggest when you have a new cleared facility or one that you are recently assigned, you insist that the senior manager participates in these briefings during the first SVA. Phone conversations with FSOs are great from a communication standpoint, but when going to a new facility to conduct an SVA, I highly recommend that the senior manager attend.

If he or she is unavailable for the date you set, consider changing the date to a more convenient day and time. This is the time for you to build a rapport with the person that truly manages and has total control of the day-to-day operations of the cleared facility. This is the time for you as the ISR to represent DSS by explaining the essential roles of our services.

Our mission is critical to national security, and senior managers must understand the role of the FSO and the support system the FSO needs to maintain an organized and effective industrial security program.

Senior managers should also understand that if the rating of their SVA falls below satisfactory, it can jeopardize the facility clearance, which in turn affects their ability to perform on present and future government contracts.

I always try to hold an entrance and exit briefing with senior management. In fact, if I miss the senior manager for the exit briefing due to scheduling conflicts and everything is satisfactory or higher, I usually call the senior manager to ensure closure on the SVA. Why? I am simply maintaining communication with the person

The following is an example of an entrance briefing I conducted with my colleagues: Information Systems Security Professional Dustin Sievers and CI Special Agent Colin Glover.

The briefing was with the president/chief executive officer of an engineering and architectural firm that works on embassies all over the world.

I opened the briefing with routine introductions, followed by Sievers' comments about classified systems and the Risk Management Framework. Next, Glover spoke about suspicious contact reports and the continuous cyber-attacks our nation's companies deal with.

At the end of this SVA, having done so many, many SVAs in my career, I had goose bumps because I was privileged to witness one of the best entrance briefings I had ever attended.

I'm continually impressed by DSS personnel — we know our jobs, we contribute to national security, and most of all, our agency has positioned itself to garner respect as it relates to the protection of classified information and security education.

> Entrance and exit briefings are important because DSS informs senior leadership what to expect, what will be assessed, etc. Senior leadership often does not have a deep understanding of the assessment, and the more involved they are the better for the overall security program itself.
>
> While it is the FSO's responsibility to brief their leadership, hearing it directly from an agency representative reinforces the importance of maintaining a vigilant program.
>
> **– Tammy Watts,** FSO BAE Systems

who can either support the program or potentially cause future challenges at the cleared facility.

From the onset, establish with your FSO that senior management participation is important and crucial to the overall success of a robust industrial security program.

You can provide examples to the senior managers on how they can support the FSO. For example, encourage them to hire an assistant FSO if the program has grown rapidly, invest in security education to protect their assets, and allow the FSO to attend professional security working groups. Most of all, emphasize the importance of senior management communication to the workforce clarifying the role of the FSO and the importance of following the security policy and procedures established by the facility as set forth in the NISPOM and other requirements.

With this type of backing from management, the SVA usually goes well, the FSO is content, and most of all, you as the assigned ISR, have established a rapport with the company's decision makers.

Today in DSS, we are focusing on risk management principles and practices. I truly believe one risk is not knowing who the senior KMPs are at cleared facilities. I know my fellow ISRs recognize when management is "all in," partially in, or not at all in with DSS, but this only occurs if you meet them in person.

As a new DSS ISR it can be intimidating, as a mid-level ISR it can be routine, and as an experienced ISR you may think it's useless because you know everything — not true.

Try to stay connected to the senior KMPs and continue to dress the part, straighten your tie, remove the cat hair, and do the best entrance and exit briefing you can do because it will certainly pay off in the long run.

Be proud that you are a special agent working in the industrial security arena and convey to senior management the importance of our program during these entrance and exit briefings. Regardless of the size and complexity of each facility, meeting senior management is essential.

Field office continues tradition of partnering with industry

by Kathryn Kimball
Andover Field Office,
Industrial Security Field Operations

Andover Field Office hosted the 3rd Annual Partnership with Industry Day on July 6, 2016. To host the event, office personnel collaborated with its leadership, Personnel Security Management Office for Industry, Center for Development of Security Excellence (CDSE), and Northern Region Counterintelligence.

The event was orchestrated by Clement LaShomb, Andover Field Office industrial security representative, with logistical support from three cleared contractor facilities.

The day-long event, which originated in 2014, is intended to provide relevant DSS information and guidance to the security staff of smaller cleared contractor facilities. This year more than 70 security personnel, representing approximately 65 cleared facilities from Massachusetts, Maine and New Hampshire, attended.

The topics for this year's presentations were determined by feedback from the 2015 event, as well as the recent implementation of the National Industrial Security Program Operating Manual Change 2 requirements.

Andover Field Office Chief Sean Donnelly welcomed the group and provided information on recent DSS leadership changes, the Risk Based Analysis and Mitigation model, and upcoming DSS priorities driven by rapid technological changes and globalization.

During the day, presentations were provided on Risk Management Framework, CDSE courses and products, personnel security, and insider threat. The NCMS New England Chapter Chair and Vice Chair also spoke at the event.

The day concluded with a DSS "Open Panel" consisting of field office personnel and DSS presenters. The event received positive feedback, with several asking that the DSS/Industry Day continue on an annual basis.

Larry Paxton, Personnel Security Management Office for Industry, speaks to industry security professionals during the Andover Field Office Partnership with Industry Day.

Quotes from our Partners in Industry:

"

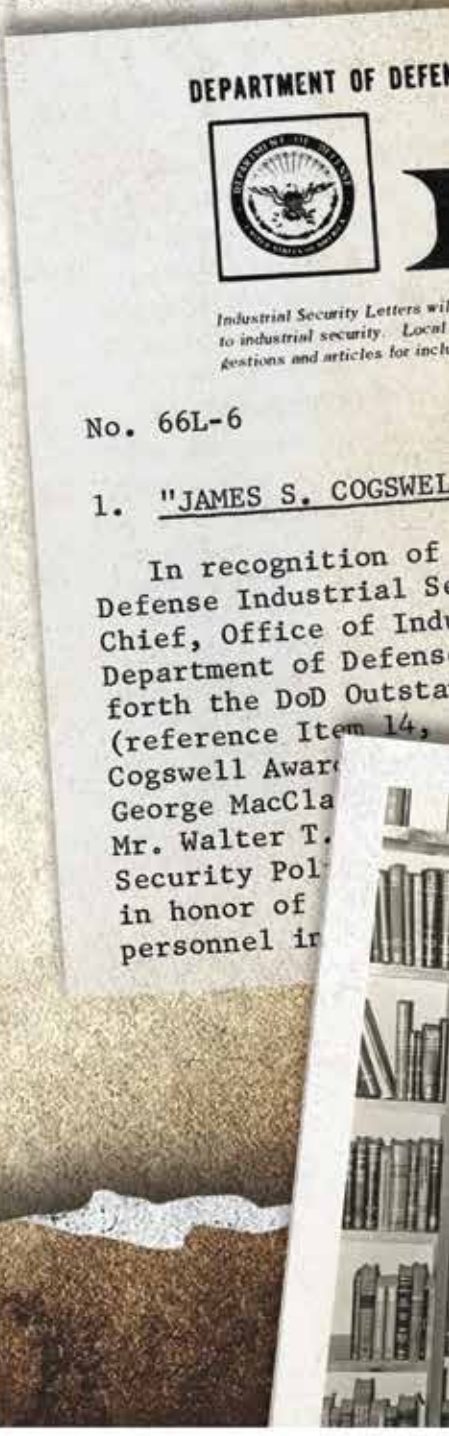
I thought the CDSE presentation was very helpful in showing me how to navigate through the different course offerings. I found the RMF to be quite interesting as well.

I found the insider threat presentation to be very interesting and informative. I will also be bringing back some good ideas on security education and training.

All of the presentations were very informative and packed with a lot of new information. The RMF piece was very helpful for FSOs that are not Information Systems Security Managers to understand the process. Please continue to have this event annually.

"

Defense Security Service



DEPARTMENT OF DEFE

Industrial Security Letters wil
to industrial security. Local
gestions and articles for incl

No. 66L-6

1. "JAMES S. COGSWEL

In recognition of
Defense Industrial Se
Chief, Office of Indu
Department of Defens
forth the DoD Outsta
(reference Item 14,
Cogswell Awar
George MacCla
Mr. Walter T.
Security Pol
in honor of
personnel in