



ASIS Councils NEWSLETTER

Defense and Intelligence Council Members

COUNCIL CHAIR

Marshall Sanders

COUNCIL VICE CHAIR

Mary Rose McCaffrey

MEMBERS

List included



Defense and Intelligence Council

January 2011

A QUICK LOOK

The Defense and Intelligence Council (D&IC) successfully completed its bi-annual meeting at the Annual Seminar in Dallas, Texas. Members of the D&IC vigorously engaged in 2010 recaps and 2011 planning. The D&IC is proud of its 2010 accomplishments to include sponsoring 8 education sessions at the Annual Seminar, conducting an ASIS webinar, and adding new members.

In this Issue:

- DSS Presents a New Leader
- Good to Great – D&IC Webinar
- Enterprise Protection Risk Management
- Meet our Members
- Items of Interest
- Our Members

DSS PRESENTS A NEW LEADER



After more than four years as the Director of the Defense Security Service (DSS), Ms. Kathleen Watson retired from government service to accept a position in the private sector.

Effective Dec. 5, 2010, Mr. Stan Sims became the Director of DSS. Prior to this appointment, Mr. Sims served as the Director of Security within the office of Deputy Under Secretary of Defense for HUMINT CI&

Security, exercising policy oversight of DSS. He was responsible for the development of necessary policy changes improving the ability of DSS to operate effectively in a complex operational environment.

Mr. Sims brings with him over 31 years of military and civilian experience having served in a variety of intelligence, operations, command and staff positions at every level. He is a member of the Defense Intelligence Senior Executive Service and is a decorated combat veteran with a well-deserved reputation as an extraordinarily competent manager, bridge-builder, and communicator.

GOOD TO GREAT

The D&IC produced the webinar Good to Great: Building High Performance Security Programs on November 17, 2010. Today's competitive and high-threat world challenges global security leaders at all levels with building and maintaining top-tier performance programs. NSA, CIA, Northrop Grumman, and BAE have all built high performance security programs to protect and enable their businesses. In the 90 minute segment, the contributors shared how they tackled the challenges of continuous improvement and how they organize, measure, manage, and lead their security programs. They revealed best practices, keys to success, and pitfalls to avoid. Most importantly, they addressed how others could transform their programs from "Good to Great".

The presenter included the following:

Edward P. Halibozek has been with Northrop Grumman Corporation for 25+ years and is currently the vice president of Security, Flight Operations, and Administration and the chair of the Northrop Grumman Security Council. He has coauthored five books on security, holds a MS in criminal justice from California State University and an MBA from Pepperdine University.

Tom Langer, vice president of security for BAE Systems, Inc., is responsible for the overall security program for the North America companies and the company's compliance with the Special Security Agreement between BAE Systems, Inc. and the U.S. Government. Tom received his Bachelor of Science degree in criminal justice from St. Anselm College in Manchester, New Hampshire.

Charles S. Phalen, Jr. joined the Central Intelligence Agency in 1981 and has served tours in both the United States and abroad, as well as executive assignments to the National Reconnaissance Office and the Federal Bureau of Investigation. He was named Director of Security for the CIA in April 2007. Mr. Phalen received a B.S. in Law Enforcement and Criminology from the University of Maryland.

ENTERPRISE PROTECTION RISK MANAGEMENT (EPRM)

Enterprise Protection Risk Management (EPRM)—Convergence on Hyperdrive
By Jim Shames, US Air Force Senior Advisor, Security Policy and Oversight

If it's hard for you to address the myriad of risks associated with protecting your organization, imagine what it would be like for the leader of your company or government organization. Of course, you want to get support for your security needs, but your needs have to be stacked against those of other stakeholders, and all the needs have to be measured against the mission, strategy, budget, and risks of the organization overall. What's compelling about your needs compared to others' and how can you show your recommendations provide the best return on investment? To answer this question, Air Force Information Protection Directorate officials have begun work on an iterative, 7-step process, to help leaders and their staffs to more effectively and efficiently assess threats, vulnerabilities, and countermeasures. A few of the highlights of this initiative were shared at the 2010 ASIS International Seminar

and Exhibits during a presentation entitled, “The Security Metrics Challenge: You’re the CEO - You Decide Which Metrics Would Score for Your Boss.” EPRM is defined as the collective policies, processes and application of risk assessment and countermeasures instituted to mitigate the compromise, loss, unauthorized access/disclosure, destruction, distortion or non-accessibility of mission-related assets—information, technology/equipment, facilities, and people. Its purpose is to achieve effective risk-based protection of key assets across the enterprise. This approach is both broad in view and detailed in application, requiring collection of key information and analyzing and presenting the situation and prospective solutions in ways that will enable meaningful decisions. The conceptual framework for the approach has been developed and will be supported by an automated decision support tool. The concept recognizes the increasingly important and complicated nature of security issues, and it enables security and other professionals to collaborate to assess the risk to their operations and develop a cost effective mitigation strategy. The gains from this initiative are far-reaching and extremely important to increasing security analysis capabilities and professionalism, and most importantly to enable huge improvements in effective decision-making for protection of assets across the full scope of an enterprise.

EPRM Process



The EPRM process increases threat-based situational awareness and motivates effective action. While the process employs a decision support tool, critical thinking and collaboration among staff, supervisors, and senior leaders are key to successful assessments, identifying the most beneficial countermeasures, and achieving effective implementation. EPRM also eases and simplifies data collection, analysis and presentation for decision-making, performance assessment and action tracking; in essence, it enables more time for thinking and implementing by reducing administrative requirements.

In summary, risk management has been difficult to perform due to the extraordinary number of interrelated and complex security matters as well as interdependent organizations spread across numerous corporate, government, and functional entities. To help correct this long-standing issue, EPRM implementation intends to provide leadership with an effective, holistic, standardized risk management capability and decision support tool. Implementation of the EPRM concept is considered a major step toward ensuring protection of an organization’s most important assets.

MEET OUR MEMBERS

Featuring: Michael J. Porturica



Michael J. Porturica is the Director of Security for ITT Defense and Information Solutions. He is responsible for the planning, execution, delivery and reporting of all aspects of the ITT Defense Security program. He provides oversight and leadership to ITT Defense value center security managers to ensure full compliance with Department of Defense security regulations and other customer specific regulatory requirements. Prior to his current position, Porturica was with the Raytheon Company, where he served as the Security Manager for their Mission Integration and Development program. He also held a 15-year career as a United States Navy civilian assigned as a Program Security Manager to the National Reconnaissance Office. Porturica served in the United States Air Force from 1983-1987, from which he received an honorable discharge. He currently serves on the Federal Bureau of Investigation, National Security Business Alliance Council (NSBAC) and the Aerospace Industry Association (AIA) security committee. He is an active member of the American Society for Industrial Security (ASIS) Defense and Intelligence Council, National Classification Management Society (NCMS), Operations Security Society, and the Industrial Security Working Group (ISWG). Porturica holds a Bachelor of Science in Management from National-Louis University in Chicago, Illinois.

1. Briefly describe how you first started in the defense/intelligence business?

During my career in the United States Air Force, I was granted a Top Secret clearance with access to Sensitive Compartmented Information. I performed quality assurance duties in the Presidential Fuels Laboratory at Andrews Air Force Base. Assigned to serve “Air Force One” during the Reagan administration was a tremendous experience. It is there that I had my introduction to asset protection, physical security, and operations security. After four years in the military, I began an occupation as a Navy civilian. I worked for the Director Naval Intelligence as a document control clerk at the Pentagon. Promoted, I moved to Defense Advanced Research Project Agency where I began working as Program Security Officer performing first level adjudication and assisting on security audits. The projects and programs were amazing. My final assignment in Civil Service was as a Program Security Officer for the National Reconnaissance Office (NRO). This assignment was very rewarding. A group so exceptionally dedicated to customer, internal and external, and functional excellence. The leaders of the NRO security office still motivate me today. Ten years ago I made the transition to industry, first with Raytheon and now the ITT Corporation. Today, I still reach out to the relationships that I had made earlier in my career. The ASIS Defense and Intelligence Council has allowed me to maintain connectivity with security professionals that over the years I have come to so greatly admire.

2. What are your major challenges in the defense/intelligence community?

As a Navy civilian, accustomed to performing two inspections each year on the condition of our contractor’s security program, I was placed on a team to bring together the different security factions at the NRO and develop an “assessment”

program. There were many cultural differences in this group. Everything from titles and pay grades to a language disparity of each organization. We soon found out that the diversity of our group was not as much a challenge but as an undeniable strength. We built a very good program. One built on years of trust between government and industry, and one that provided a level of responsible governance. Today, we face a similar challenge of consistent implementation of our regulatory requirements, and smartly working together as partners.

3. What are your most prevalent opportunities in the defense/intelligence community?

The opportunity to lead the industrial security program at ITT is a privilege. Traditionally security leaders have focused on being their corporations' security subject matter expert. Today that is not enough. To augment my business acumen I attended the ASIS sponsored, "Security Executive Development Program" at the University of Pennsylvania, Wharton School. My job is to be fully immersed in our company strategies and key initiatives, understanding and anticipating existing and emerging risks and driving the solutions to address them. My position directly correlates with the success of the strategic business initiatives. I must influence across organizational functions and drive my own staff not only to functional excellence but to provide a business advantage.

4. What types of changes have you personally developed and implemented?

ITT Corporation has a long rich history. A history that reads like a "who's who" of corporations. As a holding company ITT had many successful business lines. Though our current security model is only three years old we are progressing with the implementation of security-related initiatives designed to enhance critical functions. Improvements have been made in the exchange of security best practices, exchange of training resources and the adoption of new corporate security policies.

5. What is your vision for the company/agency?

At the ITT Corporation we like to say, "COMMIT, CREATE, and CONNECT". ITT leadership COMMITTS to a sustainable, premier security program by building an effective security function with adequate resources, formal corporate security policy, and a strong internal audit program. The ITT Security Program continues to CREATE a strong reputation by providing competent security professionals that promote an environment of functional excellence. The ITT Industrial Security Program is CONNECTED to customer centricity by being aligned with the ITT corporate strategy, and maintaining compliance while enabling business success.

6. What keeps you enthused about your career?

I have been affiliated with our nation's defense for nearly three decades. My dad proudly served this country for four decades. The security profession is a noble one. At ITT we are very proud of what we do for the men and women in uniform. In each presentation that I give I speak to the privilege of classified access and the responsibility needed to be good stewards of classified material. I welcome the challenge of managing threats, globalization, the collaboration between our commercial and defense business and our continued obligation to protect our people and corporate assets. I am very grateful for this opportunity.

7. What is your leadership style?

My leadership style is people-oriented relationship driven. I have learned so much from others and I am continually impressed by what groups can accomplish.

8. What lessons have you learned throughout your career that still inspires you today?

I have worked with several leaders, and known many others, whom by their actions have inspired me. I have often been challenged to ask questions but bring solutions. A security director at the Naval Research Laboratory taught me to care for your customer. Your customer is each person that you support, each person that calls you, each person standing at your desk when you get to work. Fostering great relationships in life and at work are critical to ones success.

ITEMS OF INTEREST

New Technology, New Threats

It is difficult to remember the days before the Internet, Facebook, ipads and smartphones. But recent advances in technology and wireless capabilities pose new security threats and vulnerabilities to employees and their families. Several social media sites to include Facebook and twitter along with access to those sites on iphones or other smartphones have the capability of divulging your location (known as geotagging). Although this may seem harmless at first, it has been the means for increased break-ins and revelation of military unit locations abroad.



A recent Army publication defines geotagging as "the process of adding geographical identification to photographs, video, websites and SMS messages. It is the equivalent of adding a 10-digit grid coordinate to everything you post on the internet." The publication also states that pictures taken with smartphones and loaded to the Internet automatically geotag their photos and when uploaded to the Internet, it allows people to track your location and associate it with other information.

Many soldiers located in both public and classified areas are cautioned against posting photos on social networking sites since they are tagged and can be detrimental to a mission and risk lives. Facebook elevates geotagging to the next level by its new feature that allows people not only to see the location of your photos, but the location of your access to the internet. Another government threat advisory states, "Tactically, this FACEBOOK feature can be employed by an adversary to refine targeting and corroborate intelligence on specific sensitive locations and/or exploitable personnel." There are several areas within Facebook where an individual must disable these features (see references below).

The important thing is for people to remain vigilant and aware that their actions on social networking sites can impact the security of their families and our nation. Some measures to avoid this form of geotagging are to turn off the GPS functions in your phones and set the highest security measures on internet sites. Be cognizant of the types of information you are divulging (gone on vacation, posting pictures while on vacation, leaving for an extended period of time, or your military installation). Employees practicing Operations Security (OPSEC), the process of identifying

potentially harmless information that can be observed and used by an adversary and finding mitigating measures to prevent that adversary from exploitation of the information, should reduce the risk of exposure of critical data.

Always remember to use caution when posting information on social networking sites!



For more information on these topics visit the following site:
<http://yongsan.korea.army.mil/pdf/socialmediasafety.pdf>.

Smartphones Collect Data



Every time you download apps on your smartphones do you think you are alone? Recent investigations indicate that your apps may be transmitting data about you and your phone to outside vendors and companies. These phones are submitting information such as location, zip codes and sometimes the person's age, gender and phone identifier. Not something you'd like to share with others? Despite Apple's efforts to review every app before

posting on their store, the manner in which their privacy policies are enforced and monitored are not discussed by Apple. Google neglects to review their apps and shift the responsibility to the user; if the user has issues with the data that will be transmitted, they can refrain from downloading the app. These companies are leaving the security up to you. Therefore be cautious when downloading apps to your phones. For more information on applications, visit [Your Apps Are Watching You](#).

D&IC MEMBERS

Paul Bailey
Jeff Berkin
Jay Carroll
Mike Clancy
Deborah Russell Collins
Cindi Conlon
Shawn Daley
J C Dodson
Lee Engel
Mike Frazier
John Fitzpatrick
Jack Forsythe
Karl Glasbrenner
Ed Halibozek

Allison Hall
Dennis Hanratty
Bob Harney
Mike Harris
Vince Jarvie
Alvina Jones
Kerrie Kavulic
Mike Laverdure
Bob Lilje
Mary Rose McCaffrey
Ryan McCausland
Dan McGarvey
Tim McQuiggan
Ray Musser

Charlie Phalen
Mike Porturica
Don Reid
Rob Rogalski
Marshall Sanders
Dan Schlehr
Jim Shamess
Jim Snodgrass
Bob Trono
Deed Vest
Dick Williams
Drew Winneberger
Wes Wong
John Young

Next Issue: April 2011

Links:

Defense & Intelligence Council – <http://www.asisonline.org/councils/GOVT.xml>

ASIS International – <http://www.asisonline.org/>

Defense & Intelligence Council Newsletter – Kerrie Kavulic – kavulick@saic.com