



Defense and Intelligence Council Members

COUNCIL CHAIR
Ed Halibozek

COUNCIL VICE CHAIR
Mary Rose McCaffrey

- MEMBERS**
- Paul L. Bailey, CPP
 - Jeffrey J. Berkin
 - Jay A. Carroll, CPP
 - Michael H. Clancy, CPP
 - Deborah Russell Collins
 - Cynthia P. Conlon, CPP
 - Shawn S. Daley
 - J.C. Dodson
 - Richard L. Engel, CPP
 - Michael W. Frazier, CPP
 - Jack L. Forsythe
 - Karl C. Glasbrenner, CPP
 - Dennis P. Hanratty
 - Bob Harney
 - J. Michael Harris, CPP
 - Vincent Jarvie
 - Alvina E. Jones
 - Kerrie L. Kavulic
 - Thomas J. Langer
 - Michael L. Laverdure
 - Robert O. Lilje, CPP
 - Daniel A. McGarvey
 - Timothy J. McQuiggan
 - Ray Musser, CPP
 - Charles S. Phalen, Jr.
 - Michael J. Porturica
 - Donald R. Reid
 - Rob W. Rogalski
 - Marshall C. Sanders, CPP
 - Daniel E. Schlehr
 - Jim Shames, CPP
 - Jim Snodgrass, CPP
 - Bob Trono
 - Deed Vest
 - Richard F. Williams, CPP
 - Drew R. Winneberger
 - Wesley Wong
 - John J. Young

Defense and Intelligence Council
April 2010

A QUICK LOOK

The Defense and Intelligence Council (D&IC) successfully completed its bi-annual meeting in January 2010. Members of the D&IC vigorously engaged in 2010 planning. Moreover, the meeting allowed other representatives from government and industry to participate in order to address key issues facing today's security professionals. With the addition of new members and potential educational sessions to the 2010 Annual Seminar, the D&IC started 2010 with energy, enthusiasm and a robust action plan.

In this Issue:

- Council Corner
- New Members
- Meet our Members
- Annual Seminar 2010
- Items of Interest

COUNCIL CORNER

The Defense & Intelligence Council (D&IC) has been hard at work this first quarter. With the continued dedication and efforts of its members the council has set forth aggressive goals for 2010:

- Increase CI Awareness information availability.
- Provide educational sessions for the 2010 Annual Seminar.
- Present 'Return on Security Investment' webinar.
- Present 'Good to Great – High performance Security Programs' webinar.
- Support the Trusted Information Provider project.
- Support the DoD PERSEREC Cyber Vetting Policies and Procedures effort.
- Continue to promote and expand the Associate Council Member program.
- Continue outreach to ASIS Chapter, Councils, legislative liaisons, and the MOU.
- Participate in the NISPOM re-write.

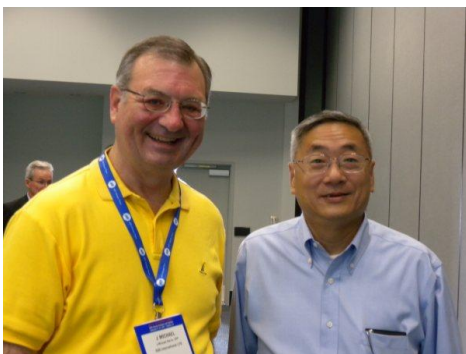


The D&IC is extremely proud of their 2009 accomplishment which include:

- D&IC article in *Security Management*
- Creation of a SharePoint site
- Distribution of survey to identify potential webinar topics
- Support of the Trusted Information Provider project
- Addition of several new members to the Council
- Reach out to other Councils and Chapters

Annual Seminar 2009:

The 2009 seminar annual seminar in Anaheim, CA was another accomplishment for the D&IC. The D&IC held their semi-annual meeting as well as proudly sponsored 6 educational sessions. We are actively gearing up for the 2010 seminar.



NEW MEMBERS

- The D&IC has the honor of welcoming several new members into the group.
 - Jay A. Carroll, US Nuclear Command and Control System Support Staff (NSS)
 - Deborah Russell Collins, NSTI
 - Jack L. Forsythe, NASA
 - Robert O. Lilje, MacAulay-Brown, Inc.
 - Michael J. Porturica, ITT Defense
 - Drew R. Winneberger, Defense Security Service

MEET OUR MEMBERS

Featuring: Deborah Russell Collins



As part of the D&IC newsletters, we will highlight an existing member. Members will share past experiences as well as their vision and expectations for current industry trends. This quarter, we will focus on Deborah Russell Collins (deedee), Executive Director of the National Security Training Institute.

Mrs. Deborah Russell Collins, Executive Director of the National Security Training Institute, has almost thirty years of experience in a wide array of fields to include training, organizational consulting, facilitation, and industrial security management. Deedee is nationally recognized as an expert in the design and delivery of motivational security awareness programs throughout the intelligence community and has worked with a variety of clients throughout the US Government and industry. Her clients include DIA, NRO, CIA, NSA, DoD, DARPA, as well as several corporations. Prior to establishing her own consulting business, Deedee was a senior manager with ESL/TRW for 15 years and responsible for new business development, community affairs, professional security staff training and development, security awareness and managing corporate security services.

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

I was fortunate to be exposed to the work of the intelligence community at a young age. Both of my parents had careers with the Central Intelligence Agency (CIA) and I lived overseas most of my childhood. While in college, I was given the opportunity to intern with the CIA for two summers in the security organization. It was an exciting environment to work in and I found the people I supported to be dedicated, professional and true patriots! Upon graduation from college, I was offered a security administrator position at a defense contractor, Electromagnetic Systems Laboratories (ESL), a subsidiary of TRW. The management of ESL was progressive even in 1980 because they saw to it that I worked in every major discipline of our profession within the first three years of my employment. It was rewarding and challenging in so many different ways. Within ten years, I was a senior security manager with the company.

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

In the late 1980s, I was approached by a colleague, Joe Cooper, who wanted to develop and deliver special security officer training to industry. No one had ever done it before. We embarked on a journey that now, twenty-one years later, has provided professional security training and development to five generations of special security officers in this profession.

The greatest challenge we face in the security profession is one of attracting and retaining qualified and gifted individuals to join our ranks. One of the first things to be cut in our budgets is training dollars. Unfortunately, the measure of most security programs falls to “nothing happened,” or, “security is a paradox: the more it succeeds the less important it appears.” It is difficult to articulate the value-added from professional development and training for our security staff.

After serving as Executive Director of NSTI for the past five years, I feel fortunate to be part of an organization that continues to provide premiere training and professional development to security professionals in government and industry. To further our profession, we must do all we can to equip, encourage and mentor the future generations in the security field.

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

I have been blessed to have the “privilege of the platform” for almost thirty years in this profession. I have been able to use a passion for the security profession coupled with a love for public speaking to find my greatest opportunities in the classroom, security conferences and mentoring 1-1. In my work I daily meet the next generation of security leaders in our profession. It’s a joy to guide, encourage and mentor all those who choose this great profession as their calling.

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

To be given a platform to do what God intended me to do in this career field has been one of life’s greatest gifts. The early part of my career focused on security awareness. It is still at the core of my contribution to the security community. In recent years, based on surviving a mass workplace violence shooting in 1988 at ESL, I have been able to work with several government agencies and corporations to establish programs to address this epidemic in our country. In several instances our work has prevented the loss of life. I feel I honor the lives lost at my company every time I speak on the subject around the nation.

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

The National Security Training Institute (NSTI) is a not-for-profit corporation dedicated to the advancement of the security professional through the presentation of courses and seminars in the national security arena.

6. What keeps you enthused about your career?

Every day is a gift and I am doing exactly what I was meant to do! It is rare in this life to find you are using every gift God gave you. I tell my security management classes often that life is more than a job title or position, it is who you are that matters. I have been offered security director positions throughout my career. I have turned them down because, while they were great opportunities, I would only touch lives in one organization. The platform I have been given allows me to teach and speak before government agencies, defense contractors as well as all the security professional organizations.

7. What is your leadership style?

Participatory, Innovative and Fun! I find more joy in collaboration than I do working alone.

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

My principal mentor in this profession was my first security director at ESL, George Bessey. We lost George last year. Here is some of what he taught me...

George Bessey will always be one of the most influential people in my life. He gave me a career that I could have only dreamed of. He believed in me and let me have every opportunity to grow and succeed in the security profession. I will celebrate my 30th year in this industry next fall and it all started with a job working at ESL in his security department. He taught all of us so much – far more than the business of security.

What I will remember always is that he inspired us to think “outside the box”, to question conventional wisdom and to seek to make a difference in all that we did at ESL. I have carried his teachings with me throughout my career. George gave me the platform of security education which uses every skill God blessed me with. George saw those traits in me far before I had the confidence to believe I could deliver that mission for ESL. He did that for everyone who worked for him – stretched us, developed us and made us the best we could be!

I've been blessed by many other mentors since --- Joe Cooper, Bill Kotapish, Raymond Falcione, my parents and my husband.

The greatest lesson in all of this is to celebrate those who have been placed in your life and learn from them! I feel fortunate to be a part of the Defense and Intelligence Council of ASIS which is comprised of the finest leaders of our industry. I have been blessed to have had a career and platform that has been rewarding every day and I never take that for granted!

ANNUAL SEMINAR 2010

The ASIS International Defense and Intelligence Council is committed to serve as a credible and progressive source of security information on issues affecting the U.S. defense and intelligence communities. In order to deliver high-quality educational security programs on relevant issues, the council is proud to sponsor nine presentations* during the 2010 ASIS International 56th Annual Seminar and Exhibits, October 12th-15th, in Dallas, Texas.

In an attempt to address increasing cyber security threats, many organizations are unwittingly wasting money and increasing operating costs by duplicating security functions. Security directors are being left on the sideline while Information Technology (IT) leaders independently develop investigative procedures, cyber security policy, sanctions, and executive management briefings on threats. Within the seminar “***Building an Effective Information Systems Security Program,***” attendees will hear how one organization accomplished their ultimate goal of effective IT security through collaboration and streamlining of functions. The power of this seminar will help discuss techniques you can use to maximize effectiveness,

capitalize on existing practices, and multiply the efficiency of your cyber security program.

How do you present to senior business and government leaders the security risk management and performance measures needed to reasonably assure protection while also maintaining an effective return on investment? We'll address this challenge facing today's security professional during "***The Security Metrics Challenge—Best of the Best—You're the CEO; You Decide Which Metrics Meet Your Bottom Line***" seminar. Top security professionals within the commercial and government sectors will demonstrate their proven methods to devise risk-managed proposals to help their top managers make key security budgeting decisions affecting their businesses and missions. See how security leaders measure the effectiveness and efficiency of security measures in order to demonstrate a meaningful return on investment.

Are you prepared to counter the myriad of threats to our people, facilities, and operations in an effective and efficient manner? How do you get the interest and resources needed to combat the threat? Without the right education and training, you don't. Through the ASIS Defense and Intelligence Council's "***Advancing DoD Security Capabilities through Professionalization and Certification***" seminar, you'll see how a recent initiative has been structured on scientific assessments and the educational and certification requirements are being used to ensure the DoD has the best security professionals in the world.

During "***The "Dongfan "Greg" Chung Economic Espionage Case***" seminar, attendees will be exposed to the shocking details of how Dongfan "Greg" Chung, a Boeing/Rockwell engineer for 30 years, illegally provided information to China since 1979. Chung was arrested in 2008, and information recovered included trade secret documents relating to programs regarding the Shuttle Phased Array, Delta IV, C-17, and civilian aircraft and helicopters. In a precedent setting trial, Chung was convicted in July 2009 for conspiracy to commit economic espionage, six counts of economic espionage to benefit a foreign country, one count of acting as an agent of the People's Republic of China and one count of making false statements to the FBI. This is one seminar that every security professional should attend.

Currently, there is no comprehensive baccalaureate degree that covers all aspects of the security discipline as practiced by the U.S. Government and supporting contractor industry. Through the "***Attracting the Next Generation of Security Professionals: Security Operations Baccalaureate Degree***" seminar, presenters will demonstrate how the Federal government, contractor industry and academia are teaming together to mitigate the exodus of experienced security professionals over the next five to ten years and "grow our own talent" through this much-needed education initiative. This presentation will inform participants of current methodologies, identify obstacles they have scaled and those that still exist while outlining the next steps which are being undertaken in order to turn this concept into a reality.

The Defense Security Service (DSS) supports the U.S. national security and the warfighter by securing the nation's technological base and overseeing the protection of U.S. and foreign classified information through the National Industrial Security Program. The "***Defense Security Service – Report to ASIS***" seminar will continue to highlight the symbiotic relationship between DSS and ASIS International. During the presentation, a senior DSS leader will explain current activities and issues with a

look into how DSS policies and practices will affect industry. This is a “must see” seminar for any industrial security professional who is currently supporting U.S. classified contracts or those whose companies are soon going to be!

Online social networking sites can be productive sources of information for pre-employment vetting and post-hiring monitoring. But is it valid? These sites can disclose sensitive, embarrassing and inaccurate information. Do you have a clear policy for collecting and using online information during recruiting? What is your policy on the use of social media sites and guidance on what employees should not post? What is the impact or liability of pre- and post-hire cyber vetting? There are significant legal, privacy, effectiveness, accuracy and fairness concerns. Through the “**Cyber-Vetting – the On-Line Persona of You and Others**” seminar, hear the latest results of a study of this cutting edge issue along with recommended guidelines.

And finally, time is money and every second counts! Today’s corporate security programs must offer security education and awareness information in a cost-effective manner in order to deliver the greatest results. Through our “**Excellence In High-Impact Security Education Training**” seminar, you will garner valuable insight into designing high-impact / high-return security education and awareness training programs that are responsive, serve the business and fosters an environment that protects our nation's secrets. Learn best practices that have been proven to help you effectively communicate and involve your management and employees in efforts that will deliver positive results each and every time! This presentation will offer a variety of tools essential to any security professional’s toolkit and will assist in delivering lasting security messages guaranteed to deliver positive results with your employees.

The ASIS International Defense and Intelligence Council looks forward to seeing you at this year’s annual seminar and exhibits. In addition to the proposed conference sessions outlined above, we encourage you to stop by our council booth to find out more about our goals and objectives, as well as how our council can better meet the needs of your ASIS chapter, government agency or private organization.

ITEMS OF INTEREST

Is Your Computer Really Infected?

Has this ever happened to you? While browsing a website, you are suddenly presented with a pop-up alert warning.

Don’t be fooled. Such alerts are almost never real, and if not careful, you will end up with an infected system, just like the 30 million computer users that have fallen prey to this very scam, according to IT security provider Panda Security. One of the biggest trends in malware attacks takes advantage of people’s lack of awareness of security threats. Hackers and scammers use a heightened fear to get users to install bogus antivirus and antispyware programs. Sometimes the point of the scam is to entice you to purchase their useless software, after which the scammer can use your credit card information for other nefarious purposes. More frequently, though, the downloaded software is actually malware disguised as an antivirus or antispyware program. Many of these programs run in the background of the infected system and can steal passwords or financial data, email thousands of spam messages, or lie in wait, ready to be given further instructions by a malicious remote server. This server sometimes instructs the infected computer to attack other systems on its behalf as part of a distributed denial-of-service attack. Most of these phony pop-up alerts and

their dangerous malware are spread by visiting compromised websites. If you encounter an alert while browsing the web, the best course of action is to close all of your browser windows. However, you still have to be extra careful when doing this since some threats use deceptive “close” buttons to get you to install the software.

Here’s the correct method to close your browser windows:

- On Windows systems, right-click on the browser icons on your task bar, and select “close” for every instance of the browser you see;
- On Mac systems, right-click on your browser icon on the dock, and select Quit;
- On Linux systems, use Control-Q to close all Firefox windows.

Some phony pop-up alert messages are spread via spam email. The best defense against them is not to use a preview pane in your mail program, never render email as HTML, and never click on attachment links that you weren’t expecting. If you believe your system may have been exposed to malware, you are encouraged to promptly report any incidents immediately to your appropriate company representative.

Cyber Update: SF-86 Questionnaire for National Security Positions

The U.S. Government has been working to streamline and enhance the security clearance process. At the same time, it is evident that more focus is being placed on proper behavior in the cyber security area. The DoD Standard Form 86, Questionnaire for National Security Positions, has been revised to include new questions and sections (on both the hard copy and the eQIP online form). The newest section is Use of Information Technology Systems, which includes questions on misuse of computers and data used for the communication, transmission, processing, manipulation, storage, or protection of information. When the form is completed or updated, you are required to answer the questions fully and truthfully, and your failure to do so could jeopardize your ability to obtain and/or maintain a security clearance.

The new questions are:

- In the last seven years, have you illegally or without proper authorization entered into any information technology (IT) system?
- In the last seven years, have you illegally or without authorization modified, destroyed, manipulated, or denied others access to information residing on an IT system?
- In the last seven years, have you introduced, removed, or used hardware, software, or media in connection with any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations?

The concern:

Naturally, there are specific reasons why these questions have been added to the SF-86. Noncompliance with rules, procedures, guidelines, or regulations pertaining to IT systems may raise security concerns about an individual's trustworthiness, willingness, and ability to follow security procedures, and may subsequently place systems that contain sensitive or classified information at risk.

In addition to the above questions, behaviors that could raise a security concern and may be disqualifying include:

- Use of any IT system to gain unauthorized access to another system or to a compartmented area within the same system;

- Downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or IT system;
- Unauthorized use of a government or other IT system;
- Negligence or lax security habits in handling IT technology that persists despite counseling by management;
- Any misuse of information technology, whether deliberate or negligent, that results in damage to national security.

Tips to avoid the dangers of social networking sites

DO NOT share your password with anyone. They may not be as careful about its protection as you are, or they may use it without your knowledge.

DO NOT use the same password for multiple sites. A hacker who steals it may use it to log into other web sites.

DO NOT click on links or download files, whenever possible. You never know if they are safe or not.

DO NOT post anything you would not want to have distributed publicly.

DO NOT use untrusted third-party applications or add-ons. Sometimes these "apps" are developed with the intent to distribute malware.

DO NOT allow unknown individuals to join your "friends list." They may be criminals trying to steal your personal or work information.

DO NOT use your work or home email address. If possible, set up a separate email account to use for social networking sites or online purchases.

DO NOT share company sensitive or classified information that is not approved for public release, or any information which requires protection under the International Traffic in Arms Regulation (ITAR).

DO adjust your profile until you are comfortable with the amount of protection provided, in order to maximize security to your information.

DO choose your screen name carefully; it should be professional and nondescript (i.e., "Labresearcher" may provide too much information to others).

DO mark your profile "private" and not open to public view, so you keep malicious persons away from your personal information.

DO make sure the "Remember me" check box is not checked before you click the Login button; otherwise others may be able to log into your account if you walk away from your computer.

DO log off the site when you are finished.

DO cancel unused accounts. They may provide others with small pieces of information that can be assembled like a puzzle in order to launch a phishing attempt against you.

DO be careful posting any pictures; they can be altered and re-posted anywhere on the Internet.

Items of Interest information provided by: *Security Digest*, MIT Lincoln Laboratory

Next Issue: October 2010

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