



Defense and Intelligence Council

June 2009

Defense and Intelligence Council Members

COUNCIL CHAIR

Ed Halibozek

COUNCIL VICE CHAIR

J. William Leonard

MEMBERS

Paul L. Bailey, CPP
Jeffrey J. Berkin
Michael H. Clancy, CPP
Cynthia P. Conlon, CPP
Shawn S. Daley
J.C. Dodson
Richard L. Engel, CPP
Michael W. Frazier, CPP
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
Mary Rose McCaffrey
Daniel A. McGarvey
Timothy J. McQuiggan
Michael Morehart
Ray Musser, CPP
Charles S. Phalen, Jr.
Donald R. Reid
Rob W. Rogalski
Marshall C. Sanders, CPP
Daniel E. Schlehr
Jim Shames, CPP
Jim Snodgrass, CPP
Glenn Sweigart, CPP
Bob Trono
Deed Vest
Richard F. Williams, CPP
Wesley Wong
John J. Young

A QUICK LOOK

The Defense and Intelligence Council (D&IC) successfully completed its bi-annual meeting in January 2009. Members of the D&IC vigorously engaged in 2009 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 2009 Annual Seminar, the D&IC started 2009 with energy, enthusiasm and a robust action plan.

In this Issue:

- New Members
- Membership Criteria
- Meet our Members
- Topics of Interest

NEW MEMBERS

- The D&IC has the honor of welcoming several new members into the group.
 - Paul L. Bailey, USNORTHCOM
 - Jeffrey J. Berkin, CACI
 - Michael H. Clancy, General Dynamics
 - J.C. Dodson, BAE Systems
 - Bob Harney, National Reconnaissance Office
 - Michael Morehart, Federal Bureau of Investigations
 - Vincent Jarvie, L-3 Communications
 - Alvina Jones, National Geospatial-Intelligence Agency
 - Daniel A. McGarvey, Department of the Air Force
 - Daniel E. Schlehr, Raytheon
 - Jim Shames, 5D Pro Solutions

The Defense & Intelligence Council strategically continues to recruit new members. Since the 2008 Annual Seminar in Atlanta, Georgia, the Council has expanded its membership to include active leaders in the defense and intelligence arena. The new members represent industry partners as well as security representatives from the intelligence community. The D&IC welcomes their new members and looks forward to their experience and contribution.

In addition to admitting new members, the D&IC adopted a tiered membership structure to allow associate membership. The D&IC welcomes Michael W. Frazier from Booz-Allen-Hamilton as its first associate member. Other ASIS members interested in the defense and intelligence should read through the membership criteria to determine which level would fit them best.



The new members inserted themselves into working groups, serve as chapter liaisons and represent the council in other organizations. The D&IC seeks to continually provide assistance and knowledge to both external customers and internal to ASIS.

MEMBERSHIP CRITERIA

- **Principal Member:**
 - Full Council voting member eligible to hold council office and participate in all council meetings and activities. A Principal Member would usually be the senior security representative within an agency or company.
 - Exceptions may be granted by a majority Council vote and approval of the Council Chair.
 - Principal membership would be “grandfathered” for existing Council members who as of the date of the adoption of this proposal are not the senior security representatives within their agency or company.

- **Associate Member:**
 - Associate Members would be defined as high potential mid-level security professionals identified and sponsored for Associate Membership by a Council Principal
 - Associate Members if approved for membership would serve as full Council members eligible to participate in Council meetings but would not be eligible to hold Council office or to vote in Council elections.
 - Associate members must be continuously sponsored by a Council Principal Member.
 - Associate members would serve for a two calendar year appointment beginning January 1st each year.
 - During their two year term Associate Members must actively serve on a Council Working Group.
 - At the end of the their two year term an Associate Member would be eligible for a second two year term with their sponsors nomination and majority approval vote of the Council Principals and the concurrence of the Council Chair.
 - At the end of each term year each Associate Member must submit in writing to the Council Chairman and their Working Group Chair a summary of their work, contributions and initiatives completed in support of the Council for the past year.

MEET OUR MEMBERS

Featuring: **Edward P. Halibozek**



As part of the D&IC newsletters, we will begin to 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 Edward P. Halibozek (Ed), Corporate Vice President of Security for Northrop Grumman Corporation.

Ed currently chairs the Northrop Grumman Security Council which among its many objectives, focuses on security issues, compliance with government regulations, and formulates security strategies for the Corporation. Ed answered a series of questions, to provide insight and challenges within the defense and intelligence industries.



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

After serving in the U.S. Army Military Police Corps, I had an interest to move from law enforcement to security. I was particularly interested in the defense industry and as luck would have it, I had friends who worked in the industry and offered me the connection I needed to move from commercial security to defense industry security.

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

At this point in time, there are three:

1. The rapidly changing cyber environment and the ever present threat to information systems and networks stands out as perhaps the most important security issue facing security professionals today. Company information is created, processed, transmitted and stored on information systems. Attacks on, and vulnerabilities to, information systems put our information (intellectual property) at greater risk. Security professional, charged with protecting information, must develop and implement effective measures of protection without disrupting or inhibiting business processes. This is a difficult challenge.

2. Delivering security services and products in such a way as to be both compliant with policy, regulation and laws and do so in efficient business ways.

3. Ensuring our profession (security) attracts and retains capable new talent. What must any organization do to attract and retain the best future security professionals we can? Particularly, when there are many opportunities for them in environments less constrained by policy and regulation.

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

One continual opportunity is the quest to continue to find ways to become more efficient in the delivery of security products and services. I think of it as efficient compliance. Furthermore, I struggle with finding better ways to measure efficiency and effectiveness in the security field. I think there is real opportunity for developing better performance measures.

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

In order to better utilize resources and improve efficiency while delivering security products and services, I've migrated to more shared services and in some cases, greater use of service providers. Essentially, taking advantage of core competencies offered by outside service providers (background investigations, security officer services, etc.) and creating centers of excellence within the company to increase efficiency in the delivery of security services and products.

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

To be the most trusted and efficient provider of security services and products possible.

6. What keeps you enthused about your career?

The seemingly never ending new challenges I'm confronted with regularly. Just when I think I've not seen a new problem, one presents itself. Also, watching young security professionals enter our profession seeking to take on security challenges both known and unknown is motivating. "New blood" brings energy and enthusiasm to the work place and to our profession.

7. What is your leadership style?

I like to think it is a participative or collaborative style.

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

The role of the security professional continues to grow. Years ago, security was often perceived, to put it simply, as guns, guards and gates. Today's security professional is often involved not only in complex security processes associated with personal, physical and information security but with related areas such as crisis management and business resilience.

Watching the scope of the security professionals role grow is inspirational, particularly, when I see security professionals rise to the challenge and achieve significant successes. Where security used to be a supporting function, it has risen to the status of a business partner. This is good.

Ed has maintained a distinguished career in the defense and intelligence industry. His leadership and influence has been paramount. In addition to his many roles, he has coauthored several books to include, "Security Metrics Management." Furthermore, not only is Ed an integral part of his corporation, he also serves as the Chair for the Defense and Intelligence Council. Under Ed's leadership, the council continues to excel and increase it's visibility within the defense and intelligence communities.

TOPICS OF INTEREST

Trusted Information Provider Pilot Program

By: Bill Leonard

Currently, many elements of pre-employment background screening employed by contractors to the Federal government are subsequently repeated by the government when investigating a contractor employee for access to classified information, for access to federally controlled facilities and information systems or otherwise determining eligibility to perform on a contract or in a position of trust. Such duplication of effort is both costly and time consuming. In that vein, the Defense and Intelligence Council of ASIS International has entered into an collaborative effort with the Federal government's Joint Security Clearance and Suitability Reform Team (JSCSRT) to examine the feasibility of establishing standards-based policy and procedures for inclusion of pre-employment screening checks conducted by the private sector prior to submitting requests for government-sponsored background investigations for suitability or security. Under this concept, when a Federal contractor elects to adhere to such standards and chooses to act as a "trusted information provider" (TIP), such pre-employment screening would then be accepted by the Federal government in lieu of the government conducting redundant checks. It is envisioned that such standards would be promulgated as an appendix to the existing *ASIS Preemployment Background Screening Guideline*.

In order to provide a proof of concept, a short term pilot is being undertaken under the auspices of the JSCSRT, an interagency effort under the joint direction of the Director of National Intelligence, the Under Secretary of Defense (Intelligence) and the Director, Office of Personnel Management (OPM). This pilot program entails contractors, on a voluntary basis, submitting the results of specified pre-employment checks (if conducted) in an agreed to "TIP format" when submitting an employee for a personnel security investigation. OPM would continue to conduct all routine checks as part of the government's investigation. The results of the government's investigation would then be compared to the "TIP" submission to ensure equivalent results. A proposed consent form has been developed for this program. All information provided will be stored solely on secure, government computers and will be used solely for the purpose of this pilot program. Information provided will not serve as the basis for any government adjudicative decisions.

The long run objective is to eliminate duplication of record checks and reference interviews and to automate front-end data entry fields in an end-to-end approach. Such a result should present an opportunity for savings of time and money to both the contractor and the government.

Next Issue: September 2009

