



ASIS Councils NEWSLETTER

LAW ENFORCEMENT LIAISON COUNCIL
April 2008



LEADERSHIP 2008

Chairperson:
Mr. Richard E. Chase,
CPP

Vice-Chairperson:
Oksana Farber

COMMITTEES:

Chairperson

Annual Seminar

Mr. Michael D. Gambrill

Book Reviews

Mr. James T. "Tom"
Roberts, Jr. CPP

Council Certification

Mr. Walt Smith

Guidelines Committee

Ms. Gail M. Simonton

Esq.

Membership Committee

Mr. James W. Birch

Publications Committee

/Newsletter Editor

Mr. James H. Fetzer, III

CPP: jfa@tds.net

P3 - Private/Public

Partnership Strategy

Mr. Robert E. Lee

Session Reviewers

Mr. Robert F. Graham,

CPP

Subject Matter Experts

Mr. Ira S. Somerson,

CPP

School Violence

Mr. Jeffrey Roehm & Mr.

Michael Scala, CPP

Transitional Training

Mr. James Birch, Ms.

Stacy Irving, Mr. Walt

Smith

Web Master

Mr. Mark Competello

SEE:

"ASIS Dynamics"
for leadership
contact
information.

LELC: OPENING REMARKS

From the Desk of Oksana Farber, Vice- Chairperson

Happy Spring to everyone!

The Law Enforcement Liaison Council and the ASIS executive leadership team have made remarkably productive strides in fostering communications to better achieve partnering initiatives in many areas.

New global leaders will not be found nor developed by looking in conventional places, nor will they act in the conventional take-charge way. There is an increasing need to seek individuals who know how to lead from behind.

Through our Council's collective activity, we've created a culture in which other people are able to lead, much like a shepherd leads his flock from behind. We have not abrogated responsibility because leading from behind is hard work, involves judgment calls and articulates values. Collectively we've learned how to decide when to be supportive, when to improvise and when to impose a structure. The LELC has taken the initiative to exercise that function by actively promoting the joint collaboration between the IACP and ASIS International. The meeting that took place between the executive directors of both organizations on Wednesday, February 28, 2008 was a significant first-step in the facilitation of emerging strategies that will hopefully provide some valuable insights into a long-term and proactive communication.

ASIS President, Tim Williams will be scheduling a meeting with the Major City Chiefs' President through the efforts of Chief Steve Harris. President Williams, a former member of the IACP PSLC, recognizes the efforts of the LELC and understands how the development of rapport between organizations can be beneficial to both.

Our Council's committees continue to systematically provide information and resources that benefit communications between policing organizations and the private security sector in many different ways. Whether we need to focus on quality membership, publications, Operation Partnership, the Transitional Training Program or other important dynamics that keep our group effective, all of the committees offer marked contributions.

Nominations for the Roy N. Bordes Council Member Award of Excellence should be submitted as soon as possible. The deadline for completed submissions is Friday, May 9, 2008.

Once again, our Council will be represented at the ASIS NYC Chapter's annual Trade Show at the Jacob Javits Center on Monday, May 12, 2008 in Manhattan. We are very grateful that Susan Powers will be back in New York to help "man" our booth and spread the word about the LELC's good work.

On May 22, 2008, panelists from the Nassau County Security / Police Information Network (SPIN) will discuss the development of SPIN, its impact on crime, business continuity and homeland security at the National Academies Security Symposium's "Fostering Public-Private Partnerships", which will take place at James Madison University. If you are interested in attending the symposium, I'll be happy to provide you with more information.

Inspector Matt Simeone, Publications Committee, will be temporarily unavailable so that he can address health issues. We would like to extend our earnest prayers and heartfelt wishes for a very speedy recovery. Your dedication and hard work on this Council make significant impacts on our mission. Thank you for setting such high standards and for all of your efforts.

"Mountains appear more lofty the nearer they are approached,
but great leaders resemble them not in this particular."

M. Blessington (1789-1849)

REGIONAL COMPUTER FORENSIC LABORATORY (RCFL)

Michael Scala, CPP Member Law Enforcement Liaison Council

Many of today's criminals use a computer...not a gun, knife or the usual burglary tools. Unlawful offenses such as child pornography, financial crimes, fraud and acts of terrorism are committed everyday with the use of an office or home computer. In an effort to combat these types of crimes, law enforcement is joining forces and creating Regional Computer Forensic Laboratories (RCFL).

RCFL are dedicated to the examination of digital evidence in support of criminal investigations. Presently, there are 14 RCFL throughout the United States. In addition, the RCFL are instructional centers for law enforcement to teach proper, standardized- techniques for the purpose of collecting and seizing evidence and cataloging and storing digital evidence.

The RCFL program is built on partnerships between the FBI and other law enforcement agencies at the federal, state and local levels within a specific region or geographic area. Typically, the lab consists of 15 examiners and support staff members. The labs have the ability to locate deleted, encrypted or damaged files on computer hard drives, and use this data as evidence in a criminal investigation. In addition to computer

hard drives, the labs have the ability to examine cellular phones, digital media, video cameras and personal digital assistants (PDA).

Noteworthy Computer Crimes and Digital Forensics

Financial Crime: One of the most egregious acts of financial fraud was the Enron Energy Company. At its height in 2001, Enron employed 22,000 people and claimed revenue of \$111 billion. (Yes, that's a "B"). The accounting fraud and deception was carried out by individuals, but the crime was aided by computers and technology. However, it was these same computers that prosecutors, with the aid of digital forensics, used against the defendants to obtain guilty verdicts.

Computer Virus: In 1999, David L. Smith unleashed the Melissa computer virus, causing millions of dollars in damage and infecting millions of computers and computer networks. The Melissa virus was disguised as an email from a friend. It was designed to send an infected email to the first 50 email addresses on the user's mailing list. The virus spread automatically and rapidly, subsequently inundating email servers. Smith ended up serving 20 months in a Federal prison.

Computer Hacker: In the 1990's, Kevin Mitnick hacked into computers at Nokia, Motorola, Sun Microsystems and Siemens. Mitnick exploited weaknesses in the security of these networks and systems. There is somewhat of a controversy surrounding the severity of Mitnick's intentions. His supporters say that he merely hacked into the computer networks to flaunt his computer skills...not with any criminal intent. However, prosecutors had a much different opinion and Mitnick was sentenced to five years. Regardless of what side you are on in this incident, the activities of Mitnick exposed the company's protected information, as well as, compromising their trade secrets and tarnishing their reputations.

An issue with members of RCFL is their efforts to avoid the disruption of a company's operation while an investigation is ongoing. The mission is to obtain the digital evidence quickly, in an efficient and methodical manner. Every attempt is made to secure a digital image of the evidence, permitting the computer and related hardware to remain at the scene. Consequently, this action allows the company to seamlessly continue their operation and activities. However, if this is not possible for the integrity of the criminal investigation, then the computer and related evidence is removed.

Is There A RCFL Near You?

Buffalo, New York
Centennial, Colorado
Chicago, Illinois
Dallas, Texas
Dayton, Ohio
Hamilton, New Jersey
Houston, Texas
Kansas City, Missouri
Louisville, Kentucky
Menlo Park, California
Philadelphia, Pennsylvania
Portland, Oregon
Salt Lake City, Utah
San Diego, California

“The Integration of Virtual Public-Private Partnership’s (VP3s) into Local Law Enforcement to Achieve Enhanced Intelligence-Led Policing:” Part 6

Masters Degree Thesis: Naval Postgraduate School, Monterey, CA Center For Homeland Defense & Security. Inspector Matthew Simeone, Nassau County New York Police Department, LELC member

In this, the sixth installment in this series, we will excerpt from Chapter 7, entitled VP3-ENHANCED INTELLIGENCE-LED POLICING: A NEW MODEL.

STARTING WITH A PRIVATE SECURITY PARTNERSHIP

With the pressing homeland security need to protect critical infrastructure, and with most critical infrastructure under private control, private security is a good place for a law enforcement agency to begin building a partnership. With private security comprising nearly three-quarters of the protective workforce, a police-private security partnership can provide a solid platform from which the scope of the P3 can be expanded at a later point.¹

Before beginning, getting input into the needs of prospective partners can help set the tone for a successful partnership. To do this, a liaison should consider reaching out to local security directors and organizing a meeting to discuss the idea of a partnership before it is launched. The purpose of assembling this group is more than just getting their “buy-in,” but is also to learn precisely what a group of knowledgeable and experienced security professionals would like from a partnership.

. . . In many places, the local chapter of ASIS International can serve as a great umbrella organization and as obliging partners in helping to organize this type of meeting. This strategy was utilized with great success in starting Nassau County SPIN as it established from the beginning that the new initiative was going to be a partnership, and that the views of private sector partners were important.

To facilitate the sharing of information that may be labeled *For Official Use Only* (FOUO), or other sensitive information, an agency should consider vetting its private security directors through an application process. This process will help to create a more trusted environment within the group and, in addition to receiving basic pedigree information, provides the law enforcement agency with an opportunity to obtain details about the responsibilities of the applicant, as well as the number of security and non-security personnel in the company. This information will give the agency better insight into the potential leverage offered by the applicant. In addition, if the agency administers a secure web-portal, a process for establishing a user name and password must be developed.

THE VP3 AND THE INTELLIGENCE FUNCTION

Leaders planning to implement a VP3 will need to decide where in the organization to house the partnership. To the extent possible within the logistical constraints of the department, agency heads should approach public-private information sharing with the mindset that a VP3 should be closely tied to the centralized intelligence function, have real-time access to information regarding the agency's operations, and that conceptually, data sharing with the private sector should be just an extension of the internal system used to move information within the agency. In larger departments, that may mean that the VP3 should be made part of an intelligence center, where data and crime analysis occurs.

Embedding a VP3 within the centralized intelligence function has many advantages. With information and intelligence readily accessible, both the quality and timeliness of network content will be enhanced. This type of functional consolidation within an intelligence center will streamline the flow of information and dramatically enhance the value that the VP3 offers to private sector consumers. Enhanced value to consumers is likely to result in a more informed and engaged private sector, which is then better able to prevent crime and terrorism.

Intelligence analysis lies at the core of intelligence-led policing, and, as a result, analysts play a critical role in influencing the direction and deployment of police resources. In terms of the 3i Model discussed earlier, analysts do this by *interpreting* the environment and creating intelligence products that can *influence* decision makers. These decision makers, having been influenced by intelligence, can then *impact* the environment.

Instilling a culture that will support information sharing within the agency and with the private sector will be a major factor in determining the success of any partnership. In describing the importance of addressing cultural concerns, David Carter writes:

One of the greatest weaknesses in the organizational culture of intelligence units is the unwillingness to share information. Police leadership must ensure that intelligence is proactively shared with the people who need the information, both inside the organization and with external agencies. Too many times, intelligence units act as a sponge, absorbing information from diverse sources, but are reluctant to share what they have gathered and learned. This gate-keeping practice is dysfunctional, wastes resources, and contributes to the reluctance of field personnel to submit information.²

Establishing information sharing policy and guidelines which hold members responsible for delivering information and intelligence products to those who need it, can assist in addressing this problem and can help shape the culture of a new VP3. Policy of this type should attempt to balance the need to protect information — that, if released, could jeopardize officer safety or an ongoing investigation — with the need to “provide the right information to the right people at the right time.”³

ENDNOTES




¹ William C. Cunningham, “U.S. Private Security Trends,” Presentation (Amelia Island: Hallcrest Systems, February 2003): 4.

² David L. Carter, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies* (Washington, DC: Office of Community Oriented Policing Services, November 2004) 62.

³ Robert S. Mueller III, Director, Federal Bureau of Investigation, Address to U.S. Chamber of Commerce, Washington, DC, January 19, 2006, *Vital Speeches of the Day* (New York: February 15, 2006) Vol. 72, Iss. 9: 258.

The IACP "CHIEF MICHAEL SHANAHAN AWARD" FOR EXCELLENCE IN PUBLIC/PRIVATE COOPERATION

from the IACP Police Chief Magazine

International Association of Chiefs of Police	
 IACP	
 global leadership in policing	<input type="text"/>
<input type="button" value="Submit Query"/>	

[FAQs](#) | [Contact Us](#) | [Other IA](#)

- [Awards & Campaigns](#)
- [IACP Home](#)
- [About IACP](#)
- [Policing](#)
- [Awards](#)
- [Memberships](#)
- [International](#)
- [Conferences](#)
- [Leadership](#)
- [Calendar](#)
- [Training](#)
- [GOAL](#)
- [Links](#)

The Michael Shanahan Award for Excellence in Public/Private Cooperation

The award seeks to recognize outstanding achievement in the development and implementation of public/private cooperation in public safety. This award recognizes agencies who have demonstrated outstanding achievements in cooperative efforts in public safety.

Research

AWARD OVERVIEW

Foundation

This award, in honor of Chief Michael Shanahan (Retired), who served the University of Washington Police Department for 24 years before retiring in 1995, seeks to recognize outstanding achievements in the development and implementation of Public/Private Cooperation in the Public Safety. Chief Shanahan made significant contributions to world wide public safety serving as the Co-Chair of the IACP Private Sector Liaison Committee (PSLC) from 1985 to 1999. Under his leadership the PSLC focused on solutions to critical public/private sector issues such as product tampering, drugs in the workplace, guidelines for non-sworn responders to alarms, workplace and school violence, and hiring and training guidelines for security guards. Chief Shanahan was the chair of the IACP's State Association of Chiefs of Police (SACOP), 1983-1989. He remains a highly respected national leader, innovator, and advocate, who recognized the critical importance of public/private partnerships in enhancing an individual community's public safety and the accumulative positive impact such collaborative actions have on protecting the vital interests of a community.

ELIGIBILITY

- The award will be presented to full service law enforcement agencies and private security organizations that work together to solve local problems that result in increased public safety. Note: This is a joint award. Individuals are not eligible.
- The program must have been initiated no later than one year prior to submission for consideration.
- The program must have been in operation during the January 1, 2007 to December 31, 2007 time frame.

EVALUATION CRITERIA

Division...

Nominees will be evaluated based on the following criteria:

- The significance of the contribution to the advancement of joint cooperative efforts geared to increasing public safety;
- Issues and problems identified, and the methodology used for problem resolution;
- Level of participation, partnering, collaboration and mutual-cooperation;
- Initiative and innovation;
- Permanency of the program;
- Development of quality assurance and performance metrics;
- Level, type and quality of communications established among participants;
- Executive leadership demonstrated; and,
- Resolution of problems identified.

APPLICATION GUIDANCE

The application package must include the following:

- Application form (**signed by the chief executive of both the law enforcement agency and the private organization**).
- Narrative summary (no more than three pages).
- Detailed project description addressing the specific circumstances involving distinguished public/private achievement as outlined by the evaluation criteria.
- Supplemental material such as departmental citations, letters of commendation, and newspaper clippings will be accepted. Videotapes, DVDs/CDs, and photos are welcome.

The complete award application must be postmarked no later than May 31, 2008 and mailed to:

IACP – Shanahan Award
Attn: Nancy Kolb
515 N. Washington Street
Alexandria, VA 22314

SELECTION PROCESS

The IACP's Private Sector Liaison Committee will be responsible for reviewing all applications and selecting the winning program. The selection committee will include members from ASIS International's Law Enforcement Liaison Council.

AWARD PRESENTATION

The award presentation will be made at the 115th Annual IACP Conference in San Diego, California. Travel expenses to the conference will be provided for the winners (one representative from the private security organization and one representative from the law enforcement organization. Narratives and photographs of the award winners will be featured in *Police Chief*.

APPLICATION ([in PDF](#))

For more information contact [Nancy Kolb](#) at 1-800-THE-IACP, extension 813. Applications must be postmarked no later than May 31, 2008.

[FAQs](#) | [Contact Us](#) | [Other IACP Sites](#) | [IACP Home](#)

515 North Washington St, Alexandria, VA USA 22314 phone: 703.836.6767 or 1.800.THE IACP fax: 703.836.4543

Articles published are the opinion of the author and not necessarily that of ASIS International or Law Enforcement Liaison Council.

From: ASIS International **Subject: Certification for Integrated Physical Security Systems**

ASIS International is considering the development of a new certification focusing on integrating physical security systems (access control, CCTV, intercom, etc.) to form an enterprise wide security solution.

The proposed certification is based on passing a required examination in the areas described above. Initial eligibility and experience requirements will be established. Educational programs and materials will be available to potential applicants to allow them to gain and reinforce knowledge in the areas to be examined.

To help us in determining the potential value of the certification, we ask you to sign up to complete a brief (10 minute) questionnaire.

The link below will take you to the site where you can sign up to take the survey. Please do so immediately, as the deadline for participation is Tuesday, April 8.

<http://www.1105direct.com/t.do?id=1037396:2898088>

Please participate. The survey will help ASIS better understand the professional needs of security professionals and will lead to more targeted certification offerings.

Thank you for your cooperation.

Darryl R. Branham, CPP
Vice President
ASIS Professional Certification Board

Call for research participation. You are receiving this message because ASIS International believes that you will benefit from this information.



1625 Prince Street
Alexandria, VA 22314-2818
USA
703-518-1447
Fax: 703-518-1517
Email: councils@asisonline.org