



SPRING 2009

President's Message

Greetings Fellow Members:

We're about three weeks from our Annual Conference and we're on track for record attendance. In 2004, we had 50 attendees and we are already at 49 and counting this year. For those of you who have not yet registered, I'll reiterate the Top 10 reasons to attend this year's conference:

10. It's the 25th anniversary of the IAPSC.
9. David Zahn, author of a CSCSM book, will teach us how to succeed when the economy recedes.
8. We'll be talking about the Tuesday night banquet entertainment for years to come.
7. Ed Taylor will show us how to boost our Google ranking and get more business.
6. The weather in Palm Springs is better than _____ [insert your city].
5. Allan Hildage and Colin Braziel will identify new income streams for our businesses.
4. With the economy down, there is no better time to network with your peers and develop partnerships to get more business.
3. Some of our fellow members will share some strategies to get more business via publishing and marketing and improve our service offerings through forensic consulting and emergency planning.
2. The independence discussion during the IAPSC General Membership Meeting will be _____ [insert adjective of your choice].
1. Free beer on Monday night at the Desert Discovery Park!

On other fronts, the Certified Security Consultant (CSCSM) examination is currently being revised. If you're planning on taking the exam, now might be a good time to get it off your to do list. The references will also be changing with the test revision. Keep in mind, many of the references are free and the IAPSC has a library available to all members.

If you're on Linked In, please join the IAPSC Group:

<http://www.linkedin.com/groups?gid=726057>. A couple of members, including myself, have been fortunate to garner some business opportunities from Linked In. Similarly, blogging provides a great marketing opportunity. I am amazed at how effective this is on your search engine rankings. If you want some ideas, check out the IAPSC's blog: (<http://securityconsultants.wordpress.com/>) and also Ed Taylor's presentation at the conference. A number of our members also have blogs on their websites which provide a wealth of information for their readers (and no doubt business leads for themselves).

At our Annual General Membership meeting, we will be voting for officers and directors. These volunteer leaders willingly and selflessly give a significant amount of their time to serve the IAPSC and us. I'd like to thank them in advance for their efforts in the coming years.

Finally, since this is my last letter as President, I'd like to thank you again for allowing me to serve you. I look forward to continuing to help advance the mission of the IAPSC in other capacities.

See you in Palm Springs!

Karim Vellani

Karim H. Vellani, CPP, CSC
IAPSC President

Annual Conference

IAPSC 2009 - 25th Anniversary • April 26 - 29, 2009 • Palm Springs, CA

The program for our 25th Anniversary Annual Conference is in place and it is an exciting agenda. The theme of this year's Conference is about providing you with the tools and ideas to thrive in a tough economy. If you apply just some of what you learn at the Conference, the benefits will dwarf the cost of attending it!!!

Some Highlights Include:

Marketing

David Zahn, author of *How to Succeed As An Independent Consultant* and nationally recognized authority on consulting, will share the latest techniques in developing leads, making a winning impression, marketing yourself in a tough economy and many other priceless tips to improve your existing business

Website Rankings

Ed Taylor, nationally recognized guru in maximizing your effectiveness on the internet will show you how to obtain and maintain top Google ratings for your website, as well as drive traffic to your website.

Converting Website Visitors in Clients

So you've spent untold amounts of money on your website, but is it making money for you in return? In his Part 2 Session, Ed will let you in on the tactics you can use to "convert" a higher percentage of your website visitors into actual leads and clients., sales, opt-ins, etc. In addition, you will learn how to use new Internet technologies to modernize your website with videos, webinars, networks and more!

The Emerging World of International Security Standards

The security profession is rapidly moving towards meeting international security standards. ASIS has announced its support for the adoption of security standardization by the International Organization for Standardization. Colin Braziel and Allan Hildage of the UK have extensive knowledge and experience in utilizing these standards and will share their experience in implementing them in your consulting business.

Publications

Publications can be an excellent means to increase your income and enhance your image and credibility as a security professional. Come listen to a panel of experts discuss the direct and indirect monetary benefits of publishing, the process involved, motivation for and expectations of being published and the actual results versus what can be expected.

PLUS!!!

1. A roundtable discussion by panelists with over 75 years of consulting experience head this session, *How to Make Money When Others Aren't*. Learn tried and true techniques to be effective in your security consulting business in an economy where others are struggling!
2. Learn about the latest IAPSC Forensic Methodology which will likely become the standard for forensic experts to use in their engagements. Plus, an interactive and lively discussion on ways to jumpstart your business.
3. How many of us address emergency planning in our threat assessments? Become aware of the laws, regulations and standards regarding EP and how to integrate it into your consulting assignments. When you expand your security assessment to include emergency preparedness, you capture new revenue and build a broader client base. Here's how!!

If you have any questions regarding the Program, feel free to contact me. I hope those who have not yet registered will finally realize the financial benefit they will gain by attending. See you there!!

Jack Case
Program Chairman

New Members

Nikhil Krishen

Nityrti Associates
D-139, Saket
New Delhi, Delhi 110017
Phone: (+91) 011-2686 3168
Email: Nikhil@nityrti.com

Scot M. Lins

SML & Associates
6711 Mimms Drive
Dallas, TX 75252
Phone: 214-794-1552
Email: scot@smlassociates.net

Anastasios P. Papanicolau

Avid Planning
1 Laskaratou Str
Athens, Greece 11141
Phone: +30 (210) 228-3411
Email: papanicolaou@avidplanning.gr

James T. Patrick

The Mackall Group
732 W. Main St.
Lake Geneva, WI 53147
Phone: 910-964-6277
Email: jpatrick@themackallgroup.com

Russ Phillips

MMTS Group
Suite A102/115-1075 Bay St.
Toronto, ONT, Canada M5S 2B2
Phone: 647-408-4182
Email: russ@mmtsgroup.com

Frank Santamora

Security Experts, Consulting & Design LLC
15 Hilee Road
Rhinebeck, NY 12572
Phone: 845-876-1155
Email: frank@security-experts.us

Alan W. Zajic

AWZ Consulting
PO Box 219
Wadsworth, NV 89442
Phone: 775-835-0500
Email: alanwzajic@aol.com

Attention Authors, Free Publicity!

Curtis Baillie is, once again, offering IAPSC members the opportunity to showcase their published books and materials. On the "IAPSC Authors" page you will receive a listing that includes your picture, link to your website and a link to your IAPSC profile page. You will also receive your own web page that includes your picture, book jacket photo, a writeup about your book or material and consulting business. Go to the IAPSC Authors Page: http://www.securityconsultingstrategies.com/IAPSC_Authors.html to take a look. Click on the name of one of the authors to view their individual web page. This is a free service and free is good. Contact me if you would like to be included.

IAPSC Website

During the month of March, 2009 my website was viewed over 100 times as a direct result of the viewer clicking on my web link placed on my IAPSC profile page. I've had many prospective clients tell me they found me through my IAPSC profile. I also reported when I became a member, that on the second day my IAPSC profile was up and running, a client contacted me stating that he had found me on the IAPSC website.

Recently, I had discussions with a new member who had yet to update his member profile. This was hard to believe. What better advertising could you want? If you haven't yet contacted Kathy to have your services, environments served and other important information updated - now's the time to do so. It's all part of your IAPSC membership.

Curtis Baillie

Member Happenings

Dave Aggleton had a new article published in Security Technology Executive (used to be Security Technology & Design) in February. You can read this article in the "Articles" section of this newsletter.

IAPSC member **Curtis Baillie** recently wrote a "Web Exclusive" article for SecurityInfoWatch.com titled, Black Friday - At what cost? The article was written in response to the November 26th "Black Friday" sales events where numerous people were injured, including the death of a Wal-Mart worker in New York. The article spoke to numerous tips and guidelines for retailers to take during these types of sales events. You can read the article by clicking this link : <http://www.securityinfowatch.com/Retail/1302933>.

Frank Carpency was an instructor for the ASIS PSP review course in Dallas on April 3rd and 4th.

The Association of Security Consultants (ASC) meeting in London was attended by founding member, **Jack Case**, of IAPSC. For more information go to: <http://www.info4security.com/story.asp?sectioncode=16&storycode=4121542>

Rich Grassie's company, Techmark, was acquired by Good Harbor Consulting. For more details go to: http://www.iapsc.org/uploaded_documents/GHC-TM%20Release.pdf

08-09 IAPSC Committees

By-laws:

Chair: Brian Gouin

Members: Ken Braunstein, Bob Schultheiss

Ethics:

Chair: Curt Baillie

Web Site:

Chair: Jack Case

Consultant Certification:

Chair: Brian Gouin

Members: Karim Vellani, Linda Watson, Ralph Witherspoon

2009 Conference :

Chair: Jack Case

Technical Standards:

Chair: Frank Pisciotta

Best Practices:

Chair: Norm Bates

Members: Karim Vellani, Jim Clark, Rob Shellow, Bruce Ramm, Ralph Witherspoon, Bill Hawthorne, Jack Case, Lance Foster, Ira Somerson

Regional Meeting Taskforce:

Co-Chairs: Dave Aggleton, Jack Case, Karim Vellani

Membership Processing:

Chair: Linda Watson; *Members:* Ken Braunstein, Elliot Boxerbaum

Member Benefits:

Chair: Ken Wheatley

Member Independence Criteria Review Task Force:

Co-Chairs: Frank Pisciotta, Dave Aggleton

Members: Elliot Boxerbaum, Brian Gouin

Successful Security Consulting:

Co-Chairs: Rich Grassie, Frank Pisciotta

Strategic Planning:

Members: Curt Baillie, Norm Bates, Mark Bennett, Elliot Boxerbaum, Jack Case, Jim Clark, Brian Gouin, Kevin Murray, Frank Pisciotta, Chuck Sennewald, Linda Watson, Ken Wheatley, Karim Vellani, Ralph Witherspoon, Dave Aggleton

Member Happenings, Cont.

Business Protection Specialists, Inc. (BPS) has opened a second office in Raleigh, North Carolina. The headquarters remains in snowy Rochester, New York. This office was opened to expand BPS' vertical market and geographic diversity for their clients.

Frank Pisciotta, CSC is leading this office's operations.

Paul Timm, PSP provided school security presentations at the American Association of School Administrators (AASA) annual conference in San Francisco, the National Association of Independent Schools (NAIS) annual conference in Chicago, SchoolDude University 2009 in Myrtle Beach, and the New Mexico School Boards Association (NMSBA) conference in Santa Fe.

Ken Trump, President of National School Safety and Security Services, presented a special pre-conference workshop on school security and emergency preparedness at the National School Boards Association annual convention in San Diego. Ken also presented a regular workshop session on managing parent and media communications on school security and crisis issues, and met with superintendents and school board members nationally to discuss their school safety concerns.

Ken authored a cover story article for District Administration magazine on the lessons learned and remaining gaps for the 10th anniversary of the Columbine High School attack. He also authored an article on communicating with parents and the media for the American School Board Journal's March 2009 issue.

Ken was interviewed for a number of top-tier national news stories on the Columbine 10th anniversary.

Ken is now on Twitter at <http://twitter.com/safeschools> and has created a new blog at: www.schoolsecurity.org/blog

Member Articles

Federal Reserve Bank of St. Louis studies correlation between crime and economic swings

An interesting and timely study by an economist at the Federal Reserve Bank of St. Louis finds limited correlation between crime and economic cycles. According to the report, short-run changes in economic conditions, as measured by changes in unemployment and wages, are found to have little effect on city crime across many cities, but property crimes were more likely to be influenced by changes in economic conditions than were more violent crimes.

For more information go to:
<http://www.threatanalysis.com/blog/?p=27>



Member Articles, Cont.

A Shred of Dignity

I was recently featured in an article published in the January/February 2009 Issue of Security Shredding and Storage News. Written by reporter Mollie Day and published by Rick Downing, the article "A Shred of Dignity" voices concerns that security professionals have regarding the marketing of non-security 'certifications' that provide an illusion of best practices in secure document destruction.

The prime issue being that NAID, the National Association for Information Destruction- the self proclaimed trade organization representing mobile paper shredding companies- promotes a certification and business campaign that does not necessarily reflect the security standards and needs for many businesses who use document destruction contractors. The secure (unreadable) particle size of shredded documents, the hiring and employment standards for personnel handling business sensitive or confidential material, and the false inference of transferred liability are some of the highlighted issues addressed in this article.

I can provide a copy of the article for anyone interested. A very explicit caveat, that in my professional opinion there are many good NAID certified document destruction vendors and that the consumer, the facility manager, or the corporate security director must properly determine through due diligence where the latent credibility of the vendor exceeds the patent stamp of a purchased certification.

Thank you for your time and consideration. Please contact me if you have any questions.

Brian D. Baker, CPP
Security Consultant
Brian D. Baker Security Group
717-994-4810
814-321-3102
www.bakersecuritygroup.com

New Data-Driven Security Study is available

A new 40-page study on Data-Driven Security Programs is now available:

<http://www.threatanalysis.com/blog/?p=28>

Texas Supreme Court Rules on Shopping Center's Liability in Negligent Security Case

In previous cases, the Texas Supreme Court has "avoided imposing a universal duty on landowners to protect persons or their property from third-party criminal acts. However, [they] have also recognized that, in some circumstances, the risk of a crime may be sufficiently unreasonable and foreseeable to justify imposing a duty on landowners to protect invitees while they are on the landowner's property." In *Trammell Crow v. Gutierrez* (January 17, 2008), the court considered the five factors established in *Timberwalk Apartments, Partners, Inc. v. Cain* to determine if the crime at the Trammell Crow property (Quarry Market) was foreseeable. Those factors are: proximity, publicity, recency, frequency, and similarity.

08-09 Officers & Board Members

Karim Vellani, President
Norman Bates, Secretary
Brian Gouin, Treasurer
Elliot Boxerbaum, Past President
Dave Aggleton
Curt Baillie
Jack Case
Lou DeStefano
Frank Pisciotta
Robert Schultheiss
Ken Wheatley
Ralph Witherspoon
Howard Wood
Chuck Sennewald, Advisor

In *Trammell Crow*, three of the factors were at issue, that is, recency, frequency, and similarity. The crime in question was a shooting and alleged robbery. The victim died from his injuries, but the plaintiff's and defendants disputed whether the crime was a targeted murder (retaliation) or a robbery that resulted in a murder.

In the 22 months prior to the shooting of Gutierrez, there were 10 violent crimes on the property. All 10 were robberies, some of which resulted in minor injuries and some which resulted in no injuries. The Supreme Court, in its majority opinion, considered all 10 of them to be dissimilar to the Gutierrez shooting and found that the crime in question was not foreseeable, thus ruling in favor of Trammell Crow. The concurring opinion, on the other hand, stated, "There were ten violent crimes at the Quarry Market within the two years preceding Gutierrez's death; all were robberies, some involved deadly weapons. Given this evidence, it was foreseeable that a robbery and murder could occur."

For more information go to:
<http://www.threatanalysis.com/blog/?p=32>

The data on CCTV effectiveness continues to pour in!!

For more information go to:
<http://www.threatanalysis.com/blog/?p=31>

The logo for IAPSC (International Association of Professional Security Consultants) is displayed in a large, stylized, white font with a blue outline and a slight shadow effect.

VERIFYING AND VALIDATING VISITORS

Security Technology Executive
February 2009

Strategies for checking and issuing credentials

David G. Aggleton, CPP, CSC

Most entry control processes are designed primarily to identify and control access to those who normally inhabit a building — trusted employees and building staff — who may have been required to undergo background screening prior to being hired. Part of the entry process includes the checking of credentials issued by the facility, using security staff or automated systems — for example, a building or access control card.

Visitors — whether business guests, contractors, delivery drivers or repair personnel — do not possess building-issued credentials and are usually unknown to building security staff.

What do we need to know in order to assure ourselves that it is acceptable to allow the visitor into our facility? The term “acceptable” is subjective and depends greatly on the security level of the facility being visited — at a regular commercial office building, anyone dressed in business attire may be considered acceptable. At a high-level military facility, nothing short of background checks and

processing through metal, x-ray and explosive detectors may be the norm.

Visitor Processing

There are four elements in the process that we should follow to ensure that the visitor should be allowed into our facility: verification of identity, validation of purpose, screening and access control.

Verification: First we need to establish and verify the person’s identity. “What is your name and do you have a government-issued credential with picture identification?” A driver’s license is a commonly accepted identification credential; most states provide a machine-readable license that facilitates extracting the holder’s data and some can verify that the document is not counterfeit. However, procedures also need to be in place to address the individual who does not, or cannot, conform to the expected norm — e.g., has no driver’s license or even no picture identification. One company’s policy might be complete denial of access; another’s might be a requirement for the visitor’s host

come to the lobby and vouch for the visitor’s identity.

Validation: Once the visitor’s identity has been verified, the second task is to validate that they have a legitimate need to be in the building. Typically, this will require contact with a known, trusted person within the facility — someone who has the authority and responsibility to admit visitors. This may be as simple as phoning the visitor’s host to verify an appointment or checking a list of pre-authorized visitors. A list is most useful where there are multiple visitors for a conference or for a training course, particularly if the host may not be locatable at a regular phone number. Nothing is more frustrating than arriving a few minutes late for a meeting and knowing that the reason security cannot reach your host is because he/she is chairing the meeting in some unknown conference room!

Screening: The third element is screening for any contraband items that might be hand-carried or on the visitor’s person. Prior to the Sept. 11 attacks, it was rare to see personnel or package

screening in a commercial environment; but many facilities have implemented some level of visitor checking — from a cursory look into hand-carried bags and briefcases to a full airport-style screening. Some facilities do not perform personnel screening under normal circumstances but keep the necessary equipment close at hand to implement tighter measures if the DHS security level is heightened.

Manual screening of the person and carried bags is more intrusive and less effective than systems but is needed to verify machine-generated alerts. The use of personnel screening technology — walk-through metal detectors, package x-ray machines and even explosive detectors — has been implemented for visitors to a number of high-rise office buildings and other more sensitive environments. Security officers should have high levels of training in systems operation, manual checking and personnel interaction if the screening process is to operate smoothly.

Should all who enter the facility be screened, or are regular building occupants to be treated as trusted persons? Part of this decision rests in the nature of the facility and the nature of contraband items for which the systems are intended to deny

access. An employee with a pocket penknife in a commercial office building is a much lower threat than the same item carried by an employee entering restricted currency or bullion processing area. If tenants/employees will not be screened, is there an automated system to check their credentials and validate them as tenants/employees?

Access Control: The three elements described above usually take place in an entry lobby (front door) or a loading dock (back door.) Once the visitor has been verified, validated and/or screened they have earned a reasonable level of trust but, perhaps, not enough to be given the freedom to roam the facility. Access control from the entry point to the remainder of the facility — and any sensitive areas within the facility — is often necessary. Should the visitor be required to wear a badge that prominently announces the person's name, their host, and the floor(s)/department(s) that they may visit? Certainly this provides an additional measure of security, but only if employees are encouraged to challenge a visitor in the wrong location or one who is not wearing a badge. However, in a large community where employees are not required to wear their badges,

visitors need only remove theirs to look like employees.

A simple and effective access control measure, particularly where higher levels of security are warranted, is to assign an escort to the visitor. It becomes the escort's responsibility to control the visitor's movements while on the site. The host signs for the visitor in the entry lobby, thereby accepting responsibility for all of the visitor's actions, and returns the visitor to the exit once the visit is complete, signing that the visitor has not been out of his/her control during the visit. However, there are a number of practical limitations: the host may be a busy person and may not have the time to collect the visitor from the entry lobby. Also, the visitor may be joining a conference already in progress that is being chaired by the host, or the visitor may need to visit a number of different departments. A form on the back of the visitor's badge can be used to reassign escort responsibility from one host to another, e.g., from an administrative assistant to the conference chair and then to another department head.

A visitor badge can also double as an access control card permitting the visitor access to allowable areas or, for higher security levels, the badge can be

used in concert with an authorized employee's card — a modified two-man rule. The benefits include the maintenance of an auditable record of visitor access and the authorizing host. For simple applications, a barcode can be printed on the visitor badge; for higher security environments, more sophisticated technology can be used, including passive infrared (PIR) and radio-frequency identification (RFID) systems that allow a visitor's tag/badge to be tracked within a building on a graphic display and can be paired with the host escort.

The Systems Approach

Most visitors, 99.99 percent, arrive for legitimate purposes and should be welcomed at the facility. Active participation of smartly presented security officers who are well-trained in both equipment operation and people skills, and who show a keen interest in ensuring that any delay or inconvenience to the visitor is minimal, are the attributes that make the visitor feel at home and are most effective in detecting off-normal conditions and denial of access to the 0.01 percent of visitors who are intent on harm.

Let's look at the process discussed above as it is implemented in an automated Visitor Management System

(VMS). Such systems are being implemented at corporate facilities, commercial office buildings (at both entry lobbies and loading docks) and gated residential communities. Modified versions are also applicable for visitors to school buildings.

Pre-Approval: The validation phase can start before the visitor arrives: The (authorized) host of the visitor accesses a VMS Web server via a standard browser (and a password) and completes a form that provides, as minimum, the visitor's name, affiliation, date, time and duration of visit, and where in the facility the visitor will be permitted and if a host is needed. An e-mail can be sent automatically to the visitor with the details of the visit and presentation of the e-mail in printed form can be used as part of the verification and validation processes. Pre-approval of visitors greatly reduces processing time and reduces the number of processing stations required.

The Visitor Arrives: The first step when the visitor arrives at the visitor processing station is to verify identity. Preferably, a standard government-issued credential, such as a driver's license, is presented and its data automatically extracted by a

reader. The alternative is keyboard entry which is slow and error-prone. The VMS software can validate the visit by checking that the individual is not on a "black list" and is expected (pre-authorized) at that date and time. If not pre-authorized, the processing staff can phone the host for validation or can require the visitor to phone the host and obtain pre-authorization. In a busy entry lobby, the latter procedure is becoming more prevalent since the responsibility for authorization is transferred from the administrative staff to the trusted host. Once the verification and validation processes are complete, the system can e-mail the host with notification of arrival and print a visitor badge.

Taking and storing a photograph of each visitor is valuable as a deterrent and can be used to identify a visitor who becomes a suspect in a security incident. Printing the photo on a disposable badge to be worn by the visitor is of less value: given the quality of the camera and typical lobby lighting conditions, the print quality is very poor and the photo of questionable use unless employees and security staff in the facility are trained to check the photo against the holder. Also, as mentioned before, visitor badging is

ineffective in large facilities unless employees are also required to wear their badges.

The Visitor's Badge: The system can automatically print the visitor's badge as soon as the identity is verified and the purpose for the visit validated. The design of the badge is open to the user, but it is useful to ensure that the following information is prominently displayed: visitor's name, affiliation, host's name, meeting location (e.g., floor/room number) and expiration date. A self-expiring sticker may be of added security and, if the badge is to be used in an automated access control system, a barcode can be printed on the badge or a prox reader sensor adhered to it.

A label can be printed that is stuck on a reusable plastic badge that can be a proximity card. Any process that requires peeling off a backing or peeling off an old label is more time-consuming and creates waste. Card stock, pre-printed with standard building information, is probably best if longevity and barcode reading are issues. Although such badges

are a little more expensive to produce and need a thermal-printed piece of paper ribbon, they are part of the "visitor experience" and enhance the image of the facility.

The period of validity of a badge may be set at a single visit, multiple visits in one day, of multiple days for, say, a visitor who is attending a week-long training course. The quality of the badge should reflect its expected duration. Another factor to plan for is disposal: a badge dropped in a garbage can outside the building should not permit entry by a dumpster diver.

Visitor management systems can interface with many off-the-shelf access control systems. As soon as the visitor badge is produced, the badge identification number (e.g., barcode or proximity code) and the expiration data can be transmitted to the field panels of the card readers that will read the badge. Thus, a turnstile access control system in the entry lobby, with appropriate readers, can accept the visitor's badge and control passage into the facility.

Kiosks

The VMS process is ideal for automation — if the visitor is preauthorized and has a machine-readable, government-issued credential. ATMs and boarding pass kiosks have trained us to interface with complex systems through simple processes. Many VMSs promote the use of kiosks: the visitor dips the credential in a reader (similar to a bank card at an ATM) and, if its data matches that on a list of pre-authorized visitors, a photo can be taken and the visitor badge is printed. The self-processing procedure is very quick and cost-payback period for a kiosk can be short; however, most complex situations — a visitor who has not been preauthorized or who has a non-uniform credential — still requires staff assistance.

David G. Aggleton, CPP, CSC, is president and principal consultant at Aggleton & Associates, Inc., a security systems design and consulting firm. Dave has been planning and designing security systems for more than 30 years and can be reached at dave.aggleton@aggleton.com

Consultant Certification

Congratulations to the following people who have taken and passed the Certified Security Consultant Test.

David Aggleton	Lynda Buel	Robert Denny	Ronald Heil	Felix Nater	Charles Sennewald	Linda Watson
Sean Ahrens	Benjamin Butchko	Edward Dublois	Donald Hutton	Thomas Norman	Robert Shellow	Jim Webster
Curtis Baillie	Chad Callaghan	David Duda	Steve Kaufer	John Parris	Ira Somerson	Ralph Witherspoon
William Batterson	Frank Carpency	Warren Ferreira	Daniel Kropp	Frank Pisciotta	John Sullivant	William Wright
Mark Bennett	James Cornell	Lance Foster	Ronald Libengood	Thomas Roemer	Karim Vellani	
James Black	George Cramer	Brian Gouin	Paul Mains	Larry Schuck	Nick Vellani	
Elliot Boxerbaum	Michael Crocker	Robert Hardy	Michael Mason	Robert Schultheiss	Michael Verden	
Ken Braunstein	James Darnell	William Hawthorne	Bo Mitchell	Richard Sem	James Wagoner	