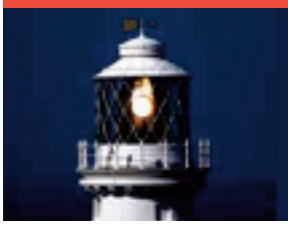


The Security Beacon

February 2017

Boston Chapter of ASIS International

In this issue...

Defining a Security Culture	1
Chairperson's Message	2
Body Cameras	3
2016 Award Winners	3
Upcoming Events	4
Twelver Shi'ism	6

Please support our generous ASIS Boston Chapter supporters

2017 ASIS Boston Chapter Leadership

Craig McQuate, Chairperson
Craig.mcquate@takeda.com

Joe Crowley, CPP, Vice Chair
jfcrowley@partners.org

Pam Perini, PSP, Secretary
Pperini1234@hotmail.com

Jim J. Healey, CPP, CFE, Treasurer
jjhealey@verizon.net

www.asis-boston.org

Editorial: Howard Communication Associates
Design: MSG Design

Developing a Culture of Security

By Lawrence J. Fennelly, CHS III, CPOI, CSSI, and Marianna A. Perry, MS, CPP

Will it be easy to develop a culture of security in your organization? The answer to this question is, "It depends." To have a culture of security in your organization depends upon whether or not you have total support from upper management. In the security industry, this is frequently called buy-in, but it is really much more than that. You have to have management participation as well as buy-in. Buy-in and participation are not the same thing. Employees of the organization need to see management actively participating and engaged in the security program. For a security program to be successful, no one is exempt from following security procedures, regardless of their title or role in the organization. Ensure that your organization does not have the "us" and "them" mentality or that management is "allowed" to disregard security procedures out of a sense of entitlement. When there is a culture of security, security belongs to everyone in the organization and everyone in the organization is an active participant.

"Measuring your program will help management justify the cost of the security awareness program."

Another critical component of developing a positive security culture is using metrics to measure the effectiveness of employee security awareness training. When effectiveness is measured, successes can be celebrated and areas that need improvement can be identified. How will you know if an employee recognized a suspicious person or incident, reduced risk or prevented a loss? Measuring your program will help management justify the cost of the security awareness program.

The Security Culture Framework is,"a community site where you can download templates, discuss best practices, share and learn about the Security Culture Framework, and about how to create lasting security culture in your organization." They define a security culture as, "The ideas, customs, and social behavior of a particular people or society that allows them to be free from danger or threats."[1]

In the article, *The Importance of a Security Culture Across the Organization*, Kevin Beaver states, "A strong security culture is both a mindset and mode of operation. One that's integrated into day-to-day thinking and decision-making can make for a near-impenetrable operation."[2]

In order to develop a culture of security in an organization, you first have to develop security awareness to ensure employees understand what security is and how important it is to the organization. CONTINUED ON PAGE 5

Chairperson's Message
Delivering value to members is Chapter focus in 2017

If you missed the January meeting, you missed a great time to connect and break bread with ASIS colleagues in the new year. You also missed Pulitzer Prize-winning speaker, Steve Kurkjian, and his fascinating talk about getting his break in investigative reporting with stories on Chappaquiddick and Woodstock.

I want to extend a big thanks to Shannon Roddy and the entire 2016 Executive Board. At the same time, I'd like to welcome to our 2017 volunteers, including Vice Chair Joe Crowley, Treasurer Jim Healey, Secretary Pam Perini, and the many selfless people who lead or serve on the various chapter committees. Please take a moment to visit the ASIS Boston website at www.asis-boston.org to see who is serving this year.

While I enjoyed the company of everyone at the January meeting, I have to admit that the turnout was disappointing. We are a chapter of over 800 members but barely 5% see the value of coming to a meeting. So the focus of the chapter leadership this year is to deliver value. We are working on booking speakers from outside the usual security arenas, and exploring methods for greater networking opportunities. On Wednesday, February 15, we will offer a repeat of our popular Speed Networking meeting, the most acclaimed and most highly-attended meeting last year. Be sure to join us for a chance to connect with your ASIS colleagues and peers.

The spring will be chock full of educational opportunities, such as the CPP Review Course in April, the Security Expo later that month and a Crime Prevention Through Environmental Design (CPTED) course in May. Attendance at the four-day course will result in an industry certification in the topic. Stay tuned for details.

While I promise the Boston Chapter leadership will work hard to deliver value to you, **we need you to do your part as well.** I am holding a Chapter office again because I have received a lot of benefit from my ASIS Boston membership and I, like many others who continue to serve, want to give back some of that benefit. I am sure every person reading this email has benefitted from his or her ASIS membership in some way. Maybe it was a professional contact made, a job lead received, an educational seminar on a much-needed topic, or a new technology explored and learned. If you have drawn a benefit from ASIS, you have a responsibility to your chapter and profession to give back. I urge you to seriously consider one year of service to ASIS Boston. You will perform a valuable service to your profession, forge new relationships with fellow Board members, shape the future of the chapter, and have some fun along the way.

If you really can't serve in a chapter office or committee, you can still do your part. Commit to bring one colleague with you to each meeting. Maybe it's a new member, an inactive old member, or a non-member, but bring someone. The Speed Networking meeting next month is a great place for new people to connect.

For those who were at the January meeting and heard many of the words I have written here, I promise I am done. Be assured your Board will work their hardest on your behalf and we hope every ASIS Boston member will commit to attending several Boston Chapter events throughout the year.

I look forward to seeing you all in February. Watch for the email and don't forget to pre-register.

Stay safe,

Craig McQuate, CPP, Chairperson
ASIS Boston Chapter

The benefits of ASIS

Not an ASIS member yet? Join NOW to take advantage of these career-boosting benefits:

- Members-only savings on CPP, PCI and PSP Board certification applications and exam fees ($450 value)
- Members-only pricing on educational webinars, classroom programs, and e-Learning ($3,500 value)
- Ability to post resumes and explore jobs in the ASIS International Career Center (invaluable)
- Volunteer leadership and executive training to advance your career (invaluable)

You'll also receive a free subscription to ASIS Boston's award-winning newsletter, *The Security Beacon*, valuable opportunities to network and connect with security professionals throughout New England, and money-saving discounts on ASIS programs and learning. Become an ASIS member to start building your future today. Go to **http://ow.ly/K3tR308qm6y** to learn more.

Body Cameras: Are they right for your business?

With ever changing technology, the use of body cameras is on the rise in both the private and public sectors. There are pros and cons to using them, with the expectation of privacy concerns and possible data breaches leading the opposing argument. Fear of Big Brother is real, especially in 2016. Cameras are everywhere and now on human bodies? The ACLU recommends police release footage and maintain a 3-year retention policy.

On the pro side, body cameras can be an invaluable tool against frivolous lawsuits. Complaints regarding excessive force also decrease. The devices provide a new training tool and can be used to weed out unsatisfactory officers. The city of Rialto, California recently did a study and found that for every dollar spent on cameras, they saved 14 in litigation. Arrests were down along with citizen complaints against the police department.

Other uses include accurate documenting of incidents, emergency drills, and individual officer training for situations including, de-escalation and pepper spray, taser and baton use. They have also been used in bomb threats, active shooter situations, and violent employee/patient/visitor events in the corporate and health care worlds.

National polls show at least 76% of US citizens approve of the use of body cameras, including 76% of males and 86% females. Responses were similarly positive across racial breakdowns, with 89% of Black respondents and 81% of White respondents in favor of the devices.

Privacy concerns

In the healthcare setting, stricter privacy issues have limited the use. HIPAA regulations make it difficult for a hospital or clinic to safeguard patient privacy with body cameras. Although a hospital is not responsible for actions taken by non-hospital employees such as local police, it is generally recommended that any body cams be turned off when on a hospital or clinic site. Today, roughly 10% of hospitals are using body cams, and 28% are using other cameras, including taser cams. These cameras turn on when the taser is turned on, leading to a two-second delay. Other concerns about these devices focus on the fact the camera does not follow the eyes of the officer since it is normally head-mounted. Furthermore, the view of the scene may be blocked by the officer's body or other people on the site. Data storage is an especial concern in healthcare settings. Since HIPAA requires safe storage, periodic security risk analyses should be performed.

In 2015, 46 states introduced legislation addressing body cameras. Four states, including California and South Carolina, enacted laws requiring certain police officers to wear them. Nine states passed laws restricting their use while Maine and Alaska leave it up to local cities and counties.

continued on page 5

Two dozen students, one organization honored at 2016 ASIS Awards Night

It was a night to remember.

Twenty-two students and one non-profit organization were recognized by ASIS Boston in November with scholarships and grants totaling $10,000. The John P. Manning Leadership Awards are given in memory of John Manning, a longtime security manager for EG&G, Honeywell and Bull, and a dedicated ASIS Boston Chapter member. Manning touched the lives of an untold number of security professionals during his career and the ASIS Boston Chapter continues his legacy by bestowing generous grants and scholarships to worthy recipients each year. Charitable organizations that do not get wide attention but do important work in improving the lives of others are eligible for recognition, as are ASIS Boston members and relatives who are enrolled in accredited institutions.

The 2016 charitable organization award winner, **Heaps of Hope, Inc.** provides financial support to women with breast cancer and offers assistance with the cost of transportation to medical appointment; payment for medication when women have no prescription coverage of very high co-pays for their medication; payment for hospital bills; assistance with the cost of integrative therapies not covered by health insurance; as well as everyday expenses such as groceries.

In addition, more than 20 children, grandchildren, nieces and nephews of ASIS members as well as ASIS members themselves received Manning Fund scholarships help with the cost of education. **See the full list of 2016 Manning Fund recipients on page 9.**

February

9

ILSSA Boston Monthly Meeting
Four Seasons Hotel
Boston, MA

15

ASIS Boston Speed Networking Event

March

6-7

CPP/PSP Review Programs
Sheraton Boston Hotel
Boston, MA

6-9

ASIS Assets Protection Course™ (APC I): Principles of Security
Sheraton Boston Hotel
Boston, MA

8

ILSSA Boston Monthly Meeting
Taj Hotel
Boston, MA

16

Joint IAHSS/ASIS Boston Dinner Meeting

April

3-5

ASIS Boston CPP Review Course
AXIS Communications, Chelmsford

20

2017 New England Security Expo
Holiday Inn, Boxborough

May

8-9

Active Shooter
Westin Las Vegas
Las Vegas, NV

Executive Protection
Westin Las Vegas
Las Vegas, NV

8-11

ASIS Assets Protection Course™: Practical Applications (APC-II)
Westin Las Vegas
Las Vegas, NV

10-11

Violence Assessment and Intervention
Westin Las Vegas
Las Vegas, NV

10-12

Physical Security: Introductory Applications and Technology Workshop
Westin Las Vegas
Las Vegas, NV

18

ASIS Boston Lunch Meeting

June

5-8

IE/ASIS Program: Effective Management for Security Professionals
Madrid, Spain

Ongoing

ACFE Webinar: Money Laundering in the Digital Currency Environment
Order online at www.acfe.com or by phoning (800) 245-3321

To register for ASIS International webinars and classroom programs, visit www.asisonline.org

Advance your career with certification from ASIS

ASIS certificate programs address the competency requirements of current security professionals and related professionals in engineering, law, and/or human resources with security management responsibilities. To receive a certificate for the course, you must take a **certificate exam.**

Programs with corresponding certificates include:

ASIS Assets Protection Course™: Principles of Security (APC I)
March 2017
Sheraton Boston Hotel

ASIS Assets Protection Course™: Practical Applications (APC II)
May 2017
The Westin Las Vegas

ASIS Assets Protection Course™: Functional Management (APC III)
July 2017
Grand Hyatt Denver

Executive Protection
May 2017
Westin Last Vegas

Risk, Threat, and Vulnerability Assessment

Executive Protection
November 2017
Hyatt French Quarter

Visit **www.asisonline.org** for costs and registration information.

Culture of security, cont'd pg 1

What is the organization securing against? A vulnerability or threat assessment will help identify the assets and the risks of the organization and then security countermeasures are put in place to help secure the identified assets and mitigate the risks. These best practices will help ensure the security program is seen as professional and following enforced procedures to comply with security policies.

Employees are a critical component of any security program. Make it personal to them. One of the largest security issues facing organizations is that employees do not understand what to report. Help them to understand what suspicious behavior is or what they should do when they observe something that doesn't seem quite right. Employees need to describe specifically what they observed, including:

- **Who** or **what** they saw;
- **When** you they it;
- **Where** it occurred; and
- **Why** it's suspicious.[3]

Think about the national campaign, "If You See Something, Say Something,"™ licensed through the Department of Homeland Security (DHS). It advises, "If you see something you know shouldn't be there — or someone's behavior that doesn't seem quite right—say something. Because only you know what's supposed to be in your everyday."[4]

Many times, it's as simple as approaching someone who is not wearing a company badge (employee, visitor, contractor or vendor) and asking if you can be of help, or, depending on the situation, contacting security and/or law enforcement and reporting the individual, using as much detail as possible. Everyone in the organization needs to understand how crime or security breaches can be prevented or they will assume that security incidents will not really impact the organization as a whole or affect them personally. Identify the risks of the organization for employees and help them understand their role in helping the organization achieve its security goals to ensure profitability and also safety.

Developing a Security Culture

Define specific incremental goals and celebrate successes when they are achieved. Each employee in the organization must act individually and directly to support the security plan in order to keep the workplace safe. Many times when a security breach is discovered, it is not the technology or the security policies or procedures that failed, but the action or inaction of people. To put it another way, it is the people operating the system or the people that are trying to circumvent the policies or procedures that are the problem. It's true that people are an organization's most valuable asset, but they are also the greatest vulnerability and/or liability. A culture of security is not for the technology within the organization. It is for the people who write the policies to enforce and follow the procedures every day.

continued on page 7

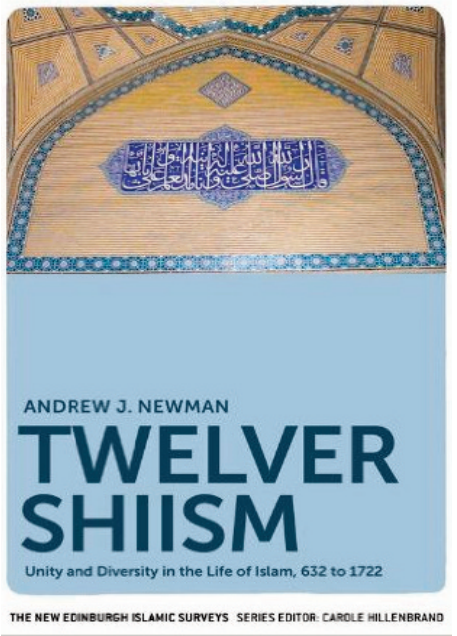
Send Us Your News!

Share your knowledge of the security industry by writing for *The Security Beacon*. Email articles and photos to **richard_zupan@identicard.com**

Body Cameras, cont'd pg 3

As such, it looks like police will be using body cams more than health care security. At the time of this writing, ten local colleges were surveyed about their use; one responded and is not using them.

Common brands are Axon Body by Taser International with a 137-degree field of view; First VU HD by Digital Ally with a 130- degree field view; and Panasonic Wearable with a 150-degree horizontal view and 140-degree vertical view. Most body cameras retail for roughly $1,000.



ASIS Book Review: Twelver Shiism: Unity and Diversity in the Life of Islam, 632 to 1722

By Andrew J. Newman
Reviewed by Mark H. Beaudry, PhD, CPP

In this book, author Andrew J. Newman provides an outstanding history of the Shia and Sunni Islam split. A reader in Islamic Studies and Persian at the University of Edinburgh, Newman probes the subject in great depth to describe the development of Islam from Mohammed's time, after his death, to the present day. The book is very factual and scholarly with a detailed description on the succession of imams within the history of the two branches of Islam. The author chronologically covers the span of history and theology, including biographies of prominent Shia figures and theologians. Newman pays close attention to details like exact transliteration, differences between Arabic and Farsi spellings and pronunciations, careful and complete footnotes, and glossary, reference lists, etc. He also makes clear and plausible how Twelver *Shi'ism* since the Safavid rule in Iran moved towards a concentration on exoteric law, with the legal experts gradually assuming several prerogatives originally held reserved to the occulted 12th Imam. In other words, it seems factually based to accept the Sunni Al-Azhar University's published opinion considering Twelver Shi'a a fifth school of orthodox Islamic jurisprudence in addition to the four still extant Sunni schools. This book is very detailed with in-depth explanations specific to the origins of certain traditions and concepts in regards to the Shia school of thought in Islam.

Newman is a gifted writer and an incredible scholar, displaying outstanding research and historical facts. Just to be clear, this is not a book for beginners who wish to start the study of *Shi'ism*. Also, the author does a very good job explaining the convoluted history of *Shi'ism* and focuses on the development of the institution of the *Imamate* from both a theological and historical perspective within three Shi'i sects: the Zaydis, the Isma'ilis, and the Twelvers. Finally, it describes how the Shiites focused on the legitimacy of Muhammad's son-in-law, Ali, as successor to the Muslim prophet, and the significance in the martyrdom of Hussein among the Twelvers and Isma'ilis.

Book reviewer Mark H. Beaudry, PhD, CPP, is a frequent contributor to The Security Beacon. He is chairman of the ASIS International Leadership Management and Practices Council and a member of the ASIS Crime Prevention and Loss Prevention Council.

Certified Protection Professional®
Board Certified in Security Management

Don't let this Early Bird offer fly away

Take your company to the next level by becoming an exhibitor at the 2017 New England Security Expo. This annual event attracts security professionals from across the region who want to learn about your business.

Go to http://ow.ly/IXnq308t7pp to take advantage of significant savings on Vendor Registration. Act NOW. This Early Bird offer ends on March 15, 2017.

Read any good books lately?

Write a review of a book you've read about security or a related subject and submit it to *The Security Beacon* for an upcoming issue. Book reviews should be 250-350 words in length. Questions? Email

Culture of security, cont'd pg 5

Some organizations have a program called **Security is Everyone's Business**. This means preventing crime and security awareness are not just the job of security officers or designated staff members. Security is Everyone's Business is a great idea, but be sure it is happening in reality and not just a concept.

A security culture is part of an overall Security Master Plan. Timothy Giles defines a Security Master Plan as "a document that delineates the organization's security philosophies, strategies, goals, programs and processes. It is used to guide the organization's development and direction in these areas in a manner that is consistent with the company's overall business plan. It also provides a detailed outline of the risks and the mitigation plans for them in a way that creates five-year business plan."[5]

A Step-by-Step Process will define how the plan will be implemented and how the organization will reach its security goals. The first step is to have a Vulnerability or Risk Assessment conducted by a trained security professional so the organization will know what assets they need to protect and what risks to retain, transfer or mitigate. When the appropriate countermeasures are put into place, the emphasis will be on layers of security along with security policies and procedures. It also may be helpful to have a safety and security committee.

The formulation of partnerships is not a new idea. They have just become more visible in recent years. Decide the goal of the partnership – is it to reduce crime and the fear of crime, for emergency response, or for a different reason? The goal of your partnership will determine the stakeholders. Regardless of the goal of the partnership, remember it is a proactive approach, not a reactive approach, and one in which members of different groups work together.

Next, identify the stakeholders in your partnership. These may be law enforcement, local government officials, fire department, emergency medical services, local emergency management personnel, community leaders, owners of commercial and residential property, area residents, area housing management, community members, local schools, neighborhood business owners, faith-based organizations, and houses of worship. The key to successful partnerships is to understand the roles, responsibilities and resources of each partner to prepare, plan and train together. The idea is a total coordination of efforts.

Plan and Train

For a partnership to be successful, planning needs to be done and the lines of communication have to stay open. Through training and practice, each partner develops a better understanding of each other's capabilities, roles, responsibilities and available resources. It's important to remember that partnerships will require ongoing maintenance to keep them engaged.

At the completion of the Vulnerability or Risk Assessment, a discussion with the security professional about recommended countermeasures will help to design a blueprint of effective security measures. The foundation for an effective physical security program that is a part of the overall security master plan is the Four D's: **Deter, Detect, Delay and Deny,** and layered security (Defense-in-Depth).[6] All countermeasures implemented should be "Best Practices" for the specific industry of the organization.

To ensure the success of your security master plan and security program, you will need to educate your community (employees) about their roles and responsibilities. Each individual should know what part they play in the overall security master plan. This is not a one-time or annual training. Instead, in order to have a security culture that is sustainable, the job of security must belong to everyone in the organization, from the lowest paid employee to the top management professional. Every person has to feel they are an important part of the security program. To develop security awareness, security has to become a part of the daily routine or a part of every job that is performed in the organization and also a part of every decision the organization makes. In order to hold employees accountable, first you must help them to learn security awareness. A security awareness program helps to create a security-conscious culture within an organization where employees are subconsciously considering risks and threats in their daily routines. As security professionals, we put security countermeasures in place to mitigate these risks and threats.[7]

Fear Reduction

Research has shown that the fear of crime or perception of crime is much higher than the actual crime rate, but fear is real and should be addressed. To reduce fear of crime, you have to identify and understand what people are afraid of and then address that specific fear.

One of the purposes of a security program is to not only implement security policies, procedures, training and countermeasures but to also direct efforts that reduce fear of crime. For example, if a source of fear in the organization is that a stranger could walk into the building at any time, organizing a company softball team is not going to fix that particular problem.

continued on page 8

Culture of security, cont'd pg 7

A company softball team may reinforce the concept of teamwork, but it is not going to help the access control problem. To address the problem, consider access control measures, such as installing a card access system at all entry locations and monitor other doors with video surveillance. Another solution may be to have security or courtesy officers in the front lobby providing customer service to each individual that enters the building. The response to employee fear has to be tailored to the specific issue. It's important that people "feel" safe at work. People are the weakest link in any security program, so a culture of security must be developed to help the people in the organization see, "where they fit in," to the big picture of security and what they can do personally to ensure the success and the security of the organization.

Many may not want to admit it, but every organization has a security culture, whether it is good or bad. It is important to understand that a negative (bad) security culture can be changed into a positive (good) security culture if the organization makes a conscious decision to change and invests in security. To promote your program, be specific about the objectives for the security program and how these objectives will be achieved. Good communication within the organization to clearly identify security responsibilities and expectations will help ensure success.

Developing a good (positive) culture of security is an ongoing process that will deliver a return on investment (ROI) for the entire organization, but an investment of time and resources must be a priority. It doesn't matter what product or service an organization makes, sells or provides, security has to be a part of it. Security should also be a part of the mission statement or vision of the organization and "just the way things are done around here."

Copyright 2016 © [Fennelly and Perry, *www.litigationconsultants.com*] *All Rights Reserved.*

Lawrence J. Fennelly, CPOI, CSSI, CHS III, is an internationally recognized authority on crime prevention, security planning and analysis and the study of how environmental factors (CPTED), contribute to criminal victimization. Marianna A. Perry, MS, CPP, has more than 30 years of progressive experience in law enforcement, physical security, safety, and loss control. Contact them at lafenn@aol.com or mariannaperry@lpsm.us.

[1] *The Security Culture Framework, Retrieved 10-24-16 from: https://securityculturefra mework.net/*

[2] *The Importance of a Security Culture. United States, 2015, Retrieved 10-24-16 from: https://securityintelligence.com/the-importance-of-a-security-culture-across-the-organization/*

[3] *"If You See Something, Say Something" campaign, Retrieved 10-24-16 from: https://www.dhs.gov/see-something-say-something/about-campaign*

[4] *Ibid.*

[5] *Giles, Timothy D. How to Develop and Implement a Security Master Plan. Florida: Auerbach Publications, 2009.*

[6] *Knoke, Michael E. (Managing Editor) Physical Security Principles. United States: ASIS International, 2015.*

[7] *Creating a Security Culture by Tom Andreas Mannerud, Retrieved 10-24-16 from: http://www.mannerud.org/2014/09/27/creating-a-security-culture/*

ASIS Boston Past Chairperson Jenn Goba, CPP, was awarded this year's Sheldon E. Goodman Award at the 2016 Awards Night in November. Goba, who is a senior investigative manager at Massachusetts General Hospital, currently serves as ASIS Region 5F Assistant Regional Vice President.

ASIS members (l-r) Steve Jussaume, Jim Foley, Don Costa and Dane Adams were among the guests at the Annual ASIS Boston Awards Night.

Convergint® TECHNOLOGIES

2016 John P. Manning Leadership Award Winners

Name	University	ASIS Member Sponsor
Christopher Moore	Boston University	Self-Nominee (ASIS Member)
Katherine Skordinski	Westfield State University	Mark Skordinski (Father)
Jordan Beaudry	Bridgewater State University	Mark H. Beaudry, PhD, CPP (Father)
Christofer Beaudry	Salem State University	Mark H. Beaudry, PhD, CPP (Father)
Erik Joseph Lundbohm	Mass Maritime Academy	Bernadette Lundbohm (Mother)
Ian Greene	Roger Williams University	James B. Greene (Father)
Alexis Brophy	Southern New Hampshire University	Phil Brophy (Father)
Mary Walsh	American Military University	Self-Nominee (ASIS Member)
Paul Murphy	Texas A&M University Maritime Academy	Harold Murphy (Grandfather)
Kathryn Murphy	Creighton University (NE)	Harold Murphy (Grandfather)
Marina Goba	Syracuse University	Jennifer Goba (Aunt)
Ross McQuate	University of MA - Amherst Commonwealth Honors College	Craig McQuate (Father)
James Mahoney	University of MA- Amherst	Tom Mahoney (Father)
Dean Westhoff	Bridgewater State University	Shannon Roddy (Aunt)
Ian Robert Carmichael	Roger Williams University	John Carmichael (Father)
Vivian Kimani	University of Massachusetts - Dartmouth	George Kimani (Father)
Nicole McIrney	Quinnipiac University	Walter McIrney (Father)
Gabrielle Joly	University of Massachusetts - Amherst	James J. Joly (Father)
Benjamin Joly	Roger Williams University	James J. Joly (Father)
Danielle Joly	Salem State University	James J. Joly (Father)
Zachary Brandt	Plymouth State University (NH)	Harvey 'Skip' Brandt (Father)
Patrick (PJ) McCurdy	Santa Clara University	Jane O'Neil (formerly McCurdy) (Mother)
2016 Charitable Award Winner	Heaps of Hope	James Healey (daughter is affiliated with the charity)

Unitex Direct
Uniform & Equipment Solutions Guaranteed
800 682-1606
www.unitexdirect.com
Celebrating over 20 years!

Physical Security Solutions for your Business
- Access Control
- Video Surveillance
- Intrusion Detection
- Intercoms & Emergency Phones
- Visitor Management & Photo ID Systems

TESLA systems Inc.
INTEGRATED SECURITY PROVIDERS
978-352-5232 teslasystemsinc.com