A STRATEGIC PLAN FOR OPEN SYSTEMS INTEGRATION AND PERFORMANCE STANDARDS (OSIPS) INITIATIVE

A COMPREHENSIVE PROGRAM DESIGNED TO CREATE GREATER FLEXIBILITY IN SECURITY SYSTEM DESIGN AND PREDICTABILITY IN APPLICATION

JANUARY 17, 2003

PREPARED BY

HUNTER KNIGHT
CHAIR
SIA STANDARDS SUBCOMMITTEE
AND

SIA STAFF

R. CHACE
D. SADDLER
M. VISBAL
K. WOODS

This Strategic Plan is confidential and the proprietary property of the Security Industry Association (SIA) and shall not be duplicated or released to others without expressed consent of SIA.

TABLE OF CONTENTS:

EXECUTIVE SUMMARY

The Security Industry Association (SIA), as the leading trade association in the world for manufacturers and service providers of security technologies and applications, proposes the OSIPS Initiative to develop integration and performance standards for security products.

The traditional security system model is undergoing an evolutionary change similar to what occurred in the IT industry. There is a rapidly increasing demand for the integration of security systems and components. Current events tell us that the demand for security integration and performance standards is so great that entities outside the security industry are taking steps to create the missing standards. Comprised of more than 500 member companies in all security technology disciplines, SIA is the natural organization to develop these standards.

If the security industry fails to take action now, it is reasonable to expect that in the not too distant future, we will pass a point of no return. The security equipment market segment could become so fragmented by the successful competitive efforts of others that it will lose the flexibility to choose a path. Once a standard has been developed and widely accepted, it is much more difficult to create a competitive alternative. Should the industry continue to neglect its role in the process of developing industry wide, defining standards, then others developing standards for the use of ***some*** security products will ultimately dictate the industry's financial future. SIA members will be without protection and will have to compete and comply with a myriad of disparate, un-harmonized standards produced from outside the security equipment sector that target specific technologies. Absent comprehensive standards, non-security industry competitors will successfully erode our market segments.

The current political environment and market forces have created a window of opportunity. By doing nothing, SIA abdicates this opportunity to others and must abide by the consequences of inaction as well as be forced into a reactive role to unknown forces. By being proactive with the OSIPS Initiative, SIA helps expand its members' future markets.

It is projected that the first 18 months of standards development will produce 10 integration and performance standards and subsequent years will average 10 standards until a critical mass of standards, estimated to be around 30, has been produced. Subsequent to this achievement, focus will shift to maintenance and upgrade of existing standards with a moderate program of new standards development.

The costs of the program will begin to be offset by contributions of work from stakeholders, investment of partner SDOs[1] in joint works, and anticipated revenues from sale of copies of the standards.

[1] SDO-Standards Developing Organizations

Program Mission

The mission of SIA Standards Program's Open Systems Integration and Performance Standards (OSIPS), Initiative is to:

1. Establish standards that will provide the most effective, flexible application of security and life safety technologies to meet the increased need for protection of people and property;
2. Assist SIA's members in the penetration of new markets;
3. Work to enhance members' existing markets;
4. Assist in establishing SIA as the preeminent representative body of manufacturers and service providers of security technologies and applications in the standards arena; and
5. Support SIA's strategic mission by collaborating and aiding the efforts of SIA's Education Department, Industry Groups, Government Relations Program, and the goal of driving product demand.

Program Goals

The OSIPS Initiative goals include:

1. Development of a family of American National Standards (ANS) that will establish broadly demanded integration and performance standards for security products;
2. Building standards in such a way that they ease the adoption of SIA member products in new markets and harmonize with existing national and international standards;
3. Ensuring that these standards facilitate innovation to meet existing and new market segment requirements;
4. Promoting the international accreditation of these standards thus creating new markets in emerging economies; and
5. Using these standards to help achieve overall SIA objectives.

The OSIPS Initiative goals do not include any effort to secure or cause the disclosure of existing proprietary performance data about any product or existing proprietary interface definitions supported by any product.

Background

Originally, the Information Technology (IT) industry provided computer systems that were closed systems, normally operating in closed environments with proprietary interfaces between components. As users demanded solutions that challenged the capacity of even the largest manufacturers, new approaches to providing solutions involving the integration of multiple suppliers' products became common. Many projects failed and many manufacturers with good ideas failed because of the complexity and one-of-a-kind nature of these approaches. Over time, a standards based industry appeared where the standards permitted innovations to be implemented in many ways, by many companies working together, in response to market forces. Competition among

manufacturers and suppliers to satisfy expanding customer demand drove the innovations that grew the market and led to product alternatives. This would not have been possible without the standards that clearly defined component capabilities and allowed components the ability to recognize and interface to each other.

The traditional security system has been and largely remains a closed system, normally operating in a closed environment with proprietary interfacing between components. The security industry, to this point, has largely followed a proprietary product strategy. However, end-users and buyers who have learned from the evolution of the IT industry are demanding the same flexibility in security systems they find in information systems technology. Today there is great demand for the ability to leverage the data gathering ability inherent in most security systems and components. Increasingly, security components and subsystems are designed to operate and be deployed across multiple sites and platforms, utilizing standardized communications. This is both a plus and minus for the security management professional, the system specifier/designer, and the system installer. The advantages of deploying a successful mission critical system may be offset by its cost or the consequences of a failed attempt. Thus the security industry is experiencing the same kind of pressures that the IT industry survived years ago.

This rapidly increasing demand for the integration of security components is not easily satisfied by closed, proprietary-only systems, which creates market opportunities for outside competitors who are not chained to an established product strategy. What the Security Industry Association's Open Systems Integration and Performance Standards (OSIPS) Initiative seeks to accomplish is the rapid evolution of the security industry learning from past success stories of the IT industry. This is a standards based tactic that serves to complement other SIA efforts.

Standards as a Tool

Standards have been, are, and will increasingly continue to be important tools in the development and evolution of markets. An essential component of the SIA Standards Program is to develop standards recognized as American National Standards, and then champion these in the international standards arena. This is envisioned as resulting in a family of nationally and internationally recognized integration and performance standards for security products that SIA members can leverage to their benefit.
SIA's program is focused on developing open system integration and performance standards that will genuinely ease the adoption of member products by other sectors and geographic markets. Standards designed to simplify adoption of compliant products by new markets are powerful market entry facilitators. Generally, this means adhering to standard rules of communications. Where reasonable, sharing common protocols and interfaces means that a user's adoption of one product paves the way for adoption of other products.

Good performance standards, which reduce the risk and cost of product adoption by others, are therefore desirable. But these standards must leave open a means for

innovators to advance products. Such innovation drives access to new market segments as existing products are enhanced to solve new problems.

Concept

Because the scope of this project is potentially vast, it is imperative that SIA Standards prioritize efforts to generate a maximum return on investment. Identification of others' efforts and partnering with them or easing their participation in SIA activities will allow SIA to efficiently use its resources in addition to broadening the support for SIA's works and establishing a leadership role for SIA in this effort. Currently, SIA participates in various standards development efforts by other SDOs, and will continue to do so in addition to maintaining an aggressive program to involve others in SIA's activities.

OSIPS will initially focus on end user demands and stakeholder involvement. With the success of these efforts, standards development will accelerate. This technical standards development effort will follow two parallel tracks:

1. Developing security product communications standards necessary to support the enhanced integration of products, and
2. Developing product performance standards.

Current Events

Current events demonstrate the need for immediate action. Other's aggressive programs of standards development are in concept or underway that will further fragment the current security market. The following are important case examples of this trend.

1. End users, including corporate, government and industrial participants at SIA Forums and other venues have routinely declared a need for performance standards and metrics that ease integration. Some have started their own efforts to establish standards and product performance metrics. SIA is now working with the Department of State/Department of Defense controlled Counter Terrorism Technical Support Office's (CTTSO) Technical Support Working Group (TSWG). The President's National Security Science and Technology Strategy led to the creation of the TSWG, its mission: "to identify needs, seek common approaches, and coordinate development of new technologies… This is accomplished through the interagency Technical Support Working Group."

2. In certain cases, the global increase in standards development has had the effect of protecting markets from U.S. products. In some cases foreign competitors have been successful at gaining global acceptance of their standard thereby isolating U.S. technology and manufacturers. A case in point occurred two years ago in the cellular telephony manufacturing industry. A struggle ensued to define an international standard for third generation products. The U.S. championed a technology known as CDMA[2], while the European Union (EU) championed

[2] CDMA-Code Division Multiple Access; http://www.cdg.org/

GSM[3] technology. The EU holds fifteen votes to the U.S.'s one vote in international standards. GSM was voted in as the technology of choice in the EU for third generation rollout, initiating a massive infrastructure upgrade to U.S. cellular providers and making U.S. technology incompatible with EU cellular networks.

3. Vertically segmented markets are developing independent standards that are radically different. Some have proceeded as far as ANS certification. These include efforts such as BACNet, M1's BioAPI Standard, and NTCIP 1205[4]. Each such standard requires SIA members to develop segment specific solutions to comply with these standards. This situation will ultimately raise costs and limit product innovation.

4. The convergence of the Information Technology (IT) sector with the Electronic Security Equipment sector can be better classified as the absorption of the Security sector by the IT sector. The IT industry has earned the reputation of being able to create and deploy system solutions that are relevant and effective. When the U. S. Government needed biometric credential reader standards developed quickly, a mandatory requirement to the adoption of this technology as a part of the defense of the homeland, they turned to IT to develop the standards. INCITS[5] created the M1 Biometrics Standards Technical Committee.

5. Various security initiatives signed into law by the U.S. Government in response to the events of 09-11 are targeted at securing the critical infrastructure and the physical borders of the U.S.A. These have served to illuminate the lack of standards in the Electronic Security Equipment sector. Examples include the USA Patriot Act[6] (Public Law 107-56) signed into law on October 26, 2001; specifically section 403 (c) TECHNOLOGY STANDARD TO CONFIRM IDENTITY; and the Aviation and Transportation Security Act[7] (Public Law 107-71) signed into law on November 19, 2001. This latter Act created the Transportation Security Agency (TSA) that will define security at all U.S. air and sea ports as well as commercial carrier terminals. These initiatives are fostering efforts to develop standards that address task specific solutions only, without a more composite "big picture" view.

6. Increased standards production from outside the industry addressing the Electronic Security Equipment sector[8] has occurred. In the security arena, the

[3] GSM- Global System for Mobile Communications; http://www.gsmworld.com/index.shtml
[4] NTCIP 1205- **N**ational **T**ransportation **C**ommunications for **I**TS (Intelligent Transportation System) **P**rotocol- Object Definitions for Closed Circuit Television (CCTV) Camera Control
[5] INCITS-InterNational Committee for Information Technology Standards; http://www.incits.org
[6] See http://thomas.loc.gov/cgi-bin/query/D?c107:1:./temp/~c107qq61QH:e232096:
[7] See http://thomas.loc.gov/cgi-bin/query/D?c107:8:./temp/~c107e0urqu::
[8] These include, but are not limited to, standards produced by and current efforts of the Telecommunications Industry, the Information Technology Industry, the Intelligent Transportation System Initiative of the U.S. Department of Transportation, the Combating Terrorism Technology Support Office of the U.S. Government, and the NFPA.

ISO/IEC, JTC1, SC 25's 18012-1 INTERNATIONAL STANDARD for HOME ELECTRONIC SYSTEMS (HES), in its final draft stage, defines system architecture and wiring standards, including electrical connectors, a security panel must use in the HES environment.

Stakeholders

The OSIPS Initiative will seek to develop a family of standards responsive to the needs of major stakeholders. Through stakeholder participation in the OSIPS Initiative, these standards will be relevant, anticipated and demanded. The basic stakeholder groups have already been identified and are listed below with the desired roles they will ultimately play in the OSIPS Initiative.

1. Government – Government is the largest and, in many ways, the most capable user of our products. Government is an end user-consumer, a specifier of required components and component capabilities, a certifier of component quality, and a regulator of acceptable products. SIA must create and maintain a strong partnership with government.

2. Critical Specifiers – Large well-established leading system specifiers must champion the results of SIA's OSIPS Initiative. For this to happen, they must be convinced that the quality of the developed standards is high and will be supported.

3. Large End Users – Large end users are critical. They will help establish the parameters of the integration and performance standards. They must be convinced that their needs have been addressed. Like the specifiers, they must be convinced that the quality of the developed standards is high and will be supported.

4. System Integrators – System Integrators are essential because they own the well of practitioner knowledge about integrating disparate products. They experience the limitations of current product strategies as increased costs and risks in projects.

5. Education & Media – These two groups have similar roles in our initiative. Both will serve to explain the goals of OSIPS, educate others about how to take advantage of OSIPS, and build demand for OSIPS products.

6. Manufacturers – Manufacturers are the cornerstones of OSIPS as they control the technical components of standards and the means to produce compliant products.

7. Related SDOs[9] – Competitors and partners in standards development, these organizations may be of great use to SIA through agreements on work areas, sharing of work products, and teaming to build harmonized standards.

IMPLEMENTATION

The OSIPS Initiative requires a stepped approach to be successful. It is imperative that the SIA Standards Committee identify not only what approaches can be undertaken with a high degree of confidence of success but also those that will generate a maximum return on investment in the immediate future as well as the long-term.

Stakeholder Enrollment

The development of a family of effective OSIPS standards is the paramount goal in this initiative. As with most "product" developments, their true effectiveness and reach depends on marketing and publicity avenues.

An aggressive campaign to encourage OSIPS standards utilization will be undertaken. Stakeholders in this process must be kept fully informed through effective communications if these standards are to have the positive impact on the marketplace for which they are being designed.

Stakeholder Communications Channels

SIA plans for a targeted approach to the various stakeholder audiences with appropriate messages. Messaging will occur in three phases with potential overlap. These are:

Phase I: Phase I will be review and approval of this initiative by the SIA Board of Directors.

Phase II: Phase II is mainly to alert audiences to the trend data regarding the demand for integration and performance standards. This Phase will also illustrate how SIA has proactively addressed this issue by developing the OSIPS Initiative and alert audiences to the market benefits to their respective disciplines.

Phase III: Phase III will be more similar to product marketing and will advertise and publicize the development and completion of standards and will promote salient reasons for their purchase and/or implementation. Since OSIPS will have both completed and developing standards simultaneously, Phases II and III will overlap.

There is general outreach that will occur within Phases II and III. Among the tools for general outreach are the following:

1) Standards Summit(s)

[9] SDO-Standards Developing Organization

a) A SIA Standards Summit will be planned for the ISC Las Vegas, (March 26-28) and potentially others later in the year, depending upon market reaction and demand.
b) This Summit will be designed as an interactive learning experience for all stakeholder segments to discover more specific details about OSIPS and to contribute their knowledge and experience.
c) The goals of the program will be to educate stakeholders and to recruit stakeholders to process, develop, and/or review documentation.

2) Overview Technical Bulletins
   a) SIA will develop a quarterly technical bulletin (with the flexibility to produce as needed special editions for timeliness and to increase in frequency to monthly when needed) that is subscription based (both free and paid).
   b) This bulletin will be a series of articles and advisories dealing with overviews of technical issues relating to the industry and on the overview of progress in specific OSIPS areas.
   c) The publications will be developed exclusively through electronic means for ease of production and delivery and publication will be launched in the first quarter of 2003.

3) General PR Outreach
   a) SIA will work with both its contracted public relations and government relations firms to develop a series of releases and stories that show the top line benefit of the OSIPS program.

4) Virtual Summits and Meetings
   a) SIA will develop a series of generic (meaning applying to all stakeholders) online or virtual "summits" to begin to educate and enroll stakeholder audiences into the OSIPS Initiative.

The following are identified as initial channels for the identified stakeholders.

1) Government
   a) Technical Support Working Group (TSWG) – SIA has made significant inroads already.
   b) New Department of Homeland Security (DHS) – SIA will work to establish significant contacts within the technical expertise of the proposed new department.
   c) The US Department of Transportation (US DOT) and Transportation Security Administration (TSA) – SIA has made good contacts in the technical areas both within the US DOT regarding PSAP communications and the TSA's envisioned TWIC[10] and related architecture and will continue to pursue theses relationships.

[10] TWIC-Transportation Worker's Identification Credential

d) NTCIP 1205[11] - This group has approached SIA in the spirit of collaboration and harmonization for a revision of this standard.
e) Government magazines and publications – SIA will develop a list of government publications and periodicals in which to promote the OSIPS Initiative.
f) Government Mailing Lists – SIA will cultivate lists of government buyers and specifiers to send promotional emails, and to enlist interest in virtual summits and live summits, etc.

2) Critical Specifiers
   a) SIA will identify specific entities and organizations representative of critical specifiers. These could include groups such as the International Association of Private Security Consultants (IAPSC), Construction Specifications Institute, the American Institute of Architects, International Facility Management Association, and others.
   b) SIA will identify publications and periodicals[12] specific to this segment in which to place promotional information about OSIPS.
   c) SIA will develop mailing lists for direct outreach about the program.

3) Large End Users
   a) SIA will identify specific entities and organizations representative of end users. These could include groups such as the International Security Management Association (ISMA), ASIS International, and related vertical trade organizations, such as the National Retail Federation, the International Healthcare Security Association, and others.
   b) SIA will identify publications and periodicals specific to this segment in which to place promotional information about OSIPS.
   c) SIA will develop mailing lists for direct outreach about the program.

4) System Integrators
   a) SIA will identify specific entities and organizations representative of systems integrators. These could include groups within related organizations such as the National Burglar & Fire Alarm Association, Central Station Alarm Association, National Systems Contractors Association, and others.
   b) SIA will identify publications and periodicals specific to this segment in which to place promotional information about OSIPS.
   c) SIA will develop mailing lists for direct outreach about the program.

5) Education & Media
   a) SIA will develop comprehensive lists of media outlets for inclusion in all general and targeted publicity efforts.
   b) SIA Standards will team with SIA Education to produce identified, key, online education programs that promote specific SIA standards and standards efforts.

[11] NTCIP 1205- **N**ational **T**ransportation **C**ommunications for **I**TS (Intelligent Transportation System) **P**rotocol- Object Definitions for Closed Circuit Television (CCTV) Camera Control
[12] Architectural Digest, ASTM International's Business Link, Compliance Magazine, Government Security, ASIS' Security Management, CSAA's Signals, etc.

6) Manufacturers
   a) SIA will utilize all of its internal communications channels and resources to consistently and concisely educate its members about the value of the OSIPS Initiative. These include: SIA News, web sites (SecurityGateway.com, SIAonline.org, SecurityLearningNetwork.com), email news service, direct email and mail lists, meetings (such as ISC), virtual events and others.

7) Related SDOs
   a) SIA will identify each organization related to and affected by our industry that is an SDO and formulate a specific outreach plan.

Messages to Stakeholders

Listed below are identified targeted message sets for the following stakeholders. (These are fluid and will be adjusted as market forces indicate.)

1. Government
2. Critical Specifiers
3. Large End Users
4. System Integrators
   a. The OSIPS standards will assist in providing greater flexibility and effectiveness in applying security technologies to meet the increasing needs of these segments.
   b. SIA and the vendor community are keenly aware of the need to evolve the technical applications of security technologies.
   c. OSIPS will allow greater flexibility in designing systems, in creating vendor relationships, and in meeting the needs of these audiences' corporate executive customers.
   d. SIA members are creating programs extremely beneficial to the customer bases. The OSIPS standards are vital to ensure levels of consistency and effectiveness in the applications of security technologies.
   e. Standards will play a role in the increasing role of safety and security in our nation.
   f. The security industry, and in particular SIA, cares greatly about how its technologies are applied.

5. Education & Media
   a. Standards are vital to the evolution and sophistication of the security marketplace.
   b. Standards, and in particular OSIPS, will establish an environment for the most effective application of security technologies.
   c. SIA is a recognized leader in the security marketplace.

6. Manufacturers
   a. Establish standards that will provide the most effective, flexible application of security and life safety technologies to meet the increased need for protection.

b. Assist SIA's members in the penetration of new markets;
c. Work to enhance members' existing markets;
d. Assist in establishing SIA as the preeminent representative body of manufacturers of security products in the standards arena; and
e. Support SIA's strategic mission by collaborating and aiding the efforts of SIA's Education Department, Industry Groups, Government Relations Program, and the goal of driving product demand.

7. Related SDOs
   a. Liaisons must be maintained and/or created where technologies intersect. It is not the intention of OSIPS to duplicate the efforts of others.

STRUCTURE OF OSIPS

Communications Standards

SIA's security product communications standards effort will be directed at establishing a family of standards based on communications standards developed by accredited ANSI SDOs such as the IEEE. International standards developed by the ISO, IEC, and others (i.e. JTC-1, CENELEC, ITU-T) will be referenced as well. Codification of "low-tech" practices will be accomplished. Generally, the approach will be to codify current practices in terms of existing national and international standards. Some extensions to ease large system integrations will be required and these, too, will be based on existing standards. Subsequent component technical standards will refer to these standards when defining interfaces. The communications standards portion of OSIPS will create standards in the following categories.

1. Electrical Interface Standards – Identify the existing national / international electrical interface standards that will be the foundation of communications between security components. Integrate them into a Security Electrical Interfaces Standard.

2. Data Encoding Standards – Identify the existing national / international data encoding standards that will be the foundation of data communications between security components. Integrate them into a Security Electrical Interfaces Standard.

3. Integrated System Routing, Session, and Presentation Standards

4. Communications Interface Devices

As noted previously, metrics for compliance will be integral to these standards.

Performance Standards

Both end users and manufacturers have identified **performance** measurement metrics at a component level as a priority. Furthermore, performance metrics for conformance to

the integration standards should be produced concurrently with these standards. Finally, a system wide metric should be developed.

Identified priorities include:

1. Security Sensor Performance Standards-The Technical Support Working Group has contracted Sandia Laboratories and Underwriters Laboratories to develop a test methodology for security system components. The first device they have identified for testing is passive, infrared (PIR) motion detectors (unit capture performance). SIA has established a liaison with all principals in this effort and will seek partnership in an effort to standardize the methodology being developed by Sandia and UL and adapt it for application to other security devices.

2. Digital Video Servers, Viewers, and Components.

3. CCTV/CCV Systems and Components-The SIA CCTV IG has identified a CCTV camera performance metric as a priority. The SIA CCTV Standards Subcommittee has looked at using UL 3044 as a basis for the development of this standard.

Management and Strategic Oversight

As with all SIA initiatives, there are three components to the OSIPS Initiative: the Board of Directors, the volunteer members and SIA staff.

Oversight of the OSIPS Initiative, the direction it takes, and the speed at which it is deployed will ultimately reside with the Board of Directors. The SIA Standards Committee's function will be equivalent to an Executive Officer's and will direct operations insuring that timelines are met.

The function of member volunteers is to provide leadership and technical expertise as well as real life, timely course modifications based on the current business environment and market factors.

The formation of Standards Subcommittees, Technical Working Groups, and Ad Hoc Committees, each with Chairs, will follow a chain of command as follows:

1. SIA Board of Directors
2. SIA Standards Committee
3. Individual Subcommittees
4. Technical Working Groups and Ad Hoc Committees

Administration (Internal SIA Staff)

1. Provide input for committee structure and meeting agendas for SIA Standards Committee, SISC, all Subcommittees, Working Groups, and Ad Hoc Committees (hereinafter referred to as Teams) and provide follow-up for each meeting.

2. Assist in setting policy for projects and standards development.
3. Ensure time lines, project deliverables, and participation is appropriate and documented. Ensure quality and conformity of standards to SIA Standards Procedures and ANSI standards development procedures.
4. Assume responsibility for coordination of all Teams' work.
5. Coordinate communications between Teams and SIA Industry Groups.
6. Conduct Team meetings with Team Chairs.
7. Ensure websites are correct and offer most current information.

Project Manager (1) and Technical Writers (3)-(Outsourced)

Each Subcommittee (or Working Group) of the OSIPS Initiative will require a Technical Writer devoted to the specific work of that Subcommittee. The role and responsibilities of this person:

1. Write initial base document in conjunction with requirements by members of the Subcommittee.
2. Write the technical specification and plain language version for each standard. The plain language version of the standard shall include an overview of the standard as it relates to the family of OSIPS standards.
3. Attend all Subcommittee meetings for input on modifications to working drafts and take meeting minutes. Type and distribute meeting minutes within time frame established by Subcommittee. Ensure approved meeting minutes are posted to website and filed appropriately.
4. Ensure all comments and questions related to standard are documented and resolved/answered in established standards procedure time frame.
5. Provide editorial input on standard project communications (press releases, web site postings, etc.) for technical and functional accuracy.

In addition to the above responsibilities, the Project Manager will oversee the work of the three Technical Writers.

Project Structure

The traditional Standards Subcommittee structure of the SIA Standards Program will need to be augmented and modified. Traditionally, the Subcommittees have been technology/component centric. This model is inadequate for the effort that SIA Standards is venturing into. OSIPS will be cutting across these traditionally segmented industry sectors.

In an effort to produce standards that are more relevant and that are anticipated by the eventual full spectrum of security industry services, including the specifier, dealer/installer and end user, SIA Standards has created the End User and Specifier Subcommittee (EUSS). This Subcommittee (SC) is envisioned as including government, industry, specifiers, dealers and installers. The purpose of this SC is:

1. To serve as a forum for these elements to input needs and desires into the SIA Standards Program

2. To serve as one of SIA's mechanisms to increase awareness of SIA's Standards efforts and telegraph SIA's intentions to the full spectrum of the security industry as well as the end users increasing acceptance of SIA's standard product and guaranteeing relevance
3. To serve as a feedback mechanism to insure that SIA's standards efforts are on track with the current prevailing market factors

The inclusion of EUSS in the SIA Standards Program is a radical departure from the traditional standards model. This SC will serve as a guide as well as a feedback mechanism.

Closer collaboration between SIA Standards Subcommittees and the Industry Groups will be achieved by a periodic meeting of the SIA Standards Committee and the Industry Group Executive Committee. The cross pollination of ideas at this level will prove beneficial to both groups and may provide the Standards Program with committed subject matter experts.

The trend in standards production worldwide is towards the utilization of web-based technologies. This is true for all facets of standards production in all arenas including ANSI's National Standards, ISO[13], IEC[14], CEN[15] and the near and far Eastern standards initiatives.

Some of the technology-based tools SIA Standards will utilize to keep interested and participating parties informed include:

1. Periodic emails at critical time junctures in the standards development process with embedded URLs pointing to draft standards available for review and comment;
2. SC members only websites; and
3. SC members' text messaging capabilities (SC member restricted access list serves and /or chat rooms).

[13] ISO-International Organization for Standardization; www.iso.ch
[14] IEC-International Electrotechnical Commission; www.iso.ch
[15] CEN- European Committee for Standardization; www.cenorm.be