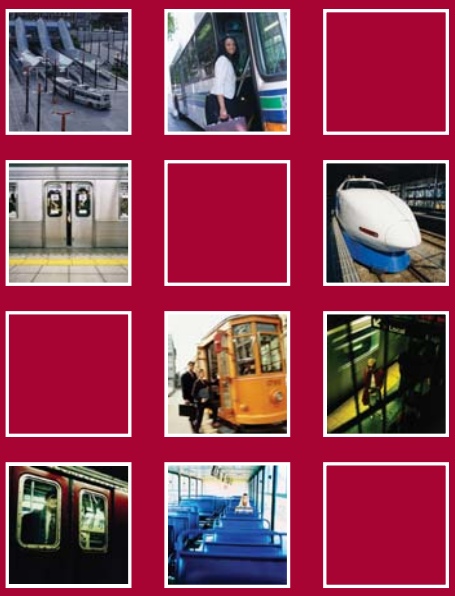

FINAL REPORT

WORKSHOP ON TRANSIT SECURITY STANDARDIZATION

Published
February 2008

Workshop Host
American National Standards Institute

World Standards Cooperation
International Electrotechnical Commission
International Organization for Standardization
International Telecommunication Union

ANSI
American National Standards Institute

Table of Contents

Background for Workshop

Every day, millions of passengers rely on commuter trains, subways, light rail (trams), and buses to take them where they need to go. Fundamental to the cities and regions they serve, public transit systems are by their very nature open, accessible, and dynamic.

In contrast, air travel uses a highly-controlled security infrastructure, requiring ticketed passengers and their luggage to undergo intensive screening at multiple checkpoints. While the airline transportation system remains a likely target, recent attacks around the world point to public transit as a target of choice for terrorists.

To assist the transit community in meeting these challenges through standards solutions, a presentation was made at the fourth meeting of the ISO/IEC/ITU-T Strategic Advisory Group on Security, 12-13 April 2007. As a result, the following resolution was passed:

> **Resolution 2 - Proposed International Workshop on Transit Security Standardization**
> *The SAG-S thanks ANSI for the offer of organizing an International Workshop on "Transit Security" and requests they move ahead with the planning as soon as possible.*

Subsequently, the leadership bodies of the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), and the International Telecommunication Union (ITU) approved this event to be convened under the World Standards Cooperation (WSC) designation.

The stated objective of the Workshop was to address the strategic role for international standards and conformity assessment programs, as well as to identify the international standards needs and gaps for public transit security, encompassing urban, suburban and regional commuter transportation by bus, rail and the land side of urban ferry operations.

To allow for a manageable and focused discussion, the Workshop focused on the transportation of people, with the following subjects considered outside its scope: air transportation/aviation security; privately owned transportation; perimeter security; transportation of freight or other goods and services.

Report Format and Acknowledgements

The following report provides the highlights of the Workshop proceedings, organized by subject matter headings. The report concludes with general observations on the state of standardization for transit security and recommendations for standards developing organizations, both nationally and internationally.

The final agenda from the Workshop is contained in Attachment 1.

Representatives from the following four stakeholder categories were present:

- End users (*e.g.*, transit personnel, first responders)
- Technologists (*e.g.*, companies and entities creating technology solutions)
- Standards Community (nationally and internationally)
- Government (various levels involved in transit security)

The list of organizations that supplied representatives to the Workshop appears in Attachment 2.

Recognition and sincere appreciation is due to the following:

- Dr. David Mussington, Deputy for Policy and Resource Management, Office of Security Strategy and Special Operations, National Railroad Passenger Corporation (Amtrak), for providing the keynote address for the Workshop.
- Dr. George Arnold, ISO Vice-President (policy) and Chairman of the ISO/IEC/ITU Strategic Advisory Group on Security; Frank Kitzantides, IEC Vice-President and Chairman of the Standardization Management Board; and Julian Minard, Delegate to ITU-T SG17 (Security) and SG13 (Next Generation Networks), for the introductory and concluding remarks that they provided on behalf of the WSC bodies.
- The moderators from each of the panels for their effective role in facilitating each of the sessions, particularly Colin Alter, Transportation Preparedness Officer, U.S DHS, Federal Emergency Management Agency, Grant Programs Directorate, Capabilities Division, Transportation Infrastructure Support Branch, for his overall leadership in helping to put together the Workshop program and securing knowledgeable speakers.
- All the speakers listed on the agenda for sharing their expertise and introducing key ideas and concepts utilized during the open dialogue sessions.
- The National Institute of Standards and Technology (NIST) for providing the meeting venue.
- The American National Standards Institute (ANSI) for serving as the meeting host and organizer, and to Matt Deane, ANSI Director of Homeland Security Standards, for the project management role that led to this final report.

Opening Roundtable – Setting the Stage

This opening session was utilized to set the context for the Workshop panel sessions. The dialogue focused on threats and vulnerabilities facing transit security stakeholders, as well as identified some approaches, solutions, and technologies that are being employed around the world to address these risks.

Challenges

- Improvised explosive devices (IEDs) are generally viewed as *the* major threat to transit agencies, so an effective way to counter them must be part of any comprehensive transit security program.
- Access control is a major issue in the transit environment. Due to it being an open system with multiple entry points, there are many potential vulnerabilities that need to be considered.
- The often high cost of addressing threats and vulnerabilities makes it a challenge for those responsible for transit security.
- The large volume of passengers in the transit environment, especially during times of overflow for special events, adds to the challenge of transit security.
- Obtaining meaningful transit participation in the development and adoption of pertinent standards can be a struggle, although at least one standards developing organization present noted that transit operators do become actively involved when a project is deemed appropriate and worthwhile for standards development.

Approaches and Solutions

- Effective access control involves the following:
  - Mass entrance and exit in minimal amount of time (quickly processing people).
  - Technology support such as closed circuit television (CCTV), although there are privacy issues to navigate with such technology.
  - Ability to deal with challenging environment for equipment (weather, heavy vibration, dust and debris).
  - Minimizing “false positive” readings.
- Risk-based approach for security, involving:
  - Risk ranked list of security sites.
  - Risk at the enterprise level (*e.g.*, 10 most important sites for the business, such as passenger carriage, revenue, etc.).
  - Use risk formula to determine vulnerabilities of these sites and risk of attack.
  - Madrid, Mumbai, London and other attacks on public transit demonstrate that attackers likes sites that have lots of people, can disrupt commerce, and are iconic.
  - Link security investment priorities to notions of threat.

Approaches and Solutions (continued)

- Effective response and business continuity measures.
- Balance between security and economic efficiency.
- An effective passenger screening system must be random (varying location and timing), quick (anything more than 10 seconds per person is too long in transit environment), and transparent (signage detailing that passenger should expect random screening).
- Interactively use technology, people (everyone who rides and is in station can provide eyes and ears), canines, to address threats.
- Think of systems based solutions set. All approaches are pieces of the puzzle. No single piece will solve the problem.
- Should focus on the first ten minutes of an attack and how to mitigate (*e.g., s*arin gas attack in Tokyo, for drivers the first 10 minute was key).
- Standards are essential to transit security because they can help "raise the bar" and bring the entire industry up to the necessary level of performance.

Physical Security

Physical security encompasses systems, equipment and facilities. Transit security is challenging because it involves an open access system that requires quick pass through of passengers.

Challenges

- Systems need to be operated and maintained in a 24/7 environment, which is frequently hostile to new generation technology.
- New devices need to be retrofitted into old environments, which typically do not have enough space, power, or are "clean enough" for high tech devices. Space issues include the lack of space for layered security (especially "stand off" space) as well as the lack of secure space within the transit system for additional equipment.
- Any maintenance within the transit system may require interruption of service.
- Size and complexity of deployment requires addition of maintenance personnel.
- Additional physical security measures often require additional operations personnel with a security background.
- Properly funding security is a constant challenge. Generally speaking, fares in public transit do not cover the cost of operations, let alone the cost of enhanced security.
- Rapidly changing state-of-the-art regarding access control, biometrics, etc.
- More technology is not always the answer. Simply having a lot of cameras is not enough, need to have sufficient monitory (*e.g.*, smart cameras or alarms automatically triggered without human monitoring).
- Successfully implementing layered physical security equipment in dense urban areas.
- There is difficulty in adding controlled entry points into a system that is essentially "open."

Approaches/Solutions

- Terrorism Mitigation Through Environmental Design (TMTED), which includes natural surveillance, territorial reinforcement, natural access control, and target hardening.
- Multi-integrated approach of personnel and techniques that are flexible/easily learned.
- Physical needs to rely on systems and equipment that are easy to use, easy to maintain, and have operating costs that are reasonable.
- Focus should be to control access to places that need the most control.

Standards Issues

- From both an operator's and a vendor's perspective, there is a lack of security and design standards.
- Standards help to simplify the product development cycle by getting the voice of the customer into the process.
- Standards should address the "how," but not the "what." Performance or effects-based standards should be the focus.
- Standards are useful for validating expenditures of money (both for government grants and by the transit agency for purchasing). Procurement goals and objectives are a strong driver for standards due to local needs, imperatives and priorities.

- Standards are needed on the following subjects:
  - Video surveillance and support tools for this surveillance.
  - Perimeter security (open facilities and closed facilities). More challenging for open facilities, which should focus on performance based approach.
  - Interoperability of systems for physical security particularly in operating environments of differing transit agency interfaces, especially access control.
  - Standard for risk management and sharing of risks within the system.
  - Explosive detection equipment including the developing threats of home-made explosives and non-nitrate based devices.
  - Vehicle borne and passenger carried IEDs.
- Conformity Assessment is the important next step in the process. Certification to accepted standards is vital, but testing must be done in the proper manner.
  - Testing helps to weed out the “snake oil” salesman selling faulty products.
  - When testing, need to look at conditions of the typical transit environment (dirty, heavy vibrations, etc.).
  - Testing also needs to consider the vastly different environmental conditions of various transit agencies (moderate vs. those with major temperature extremes) and outdoor vs. indoor installations.

Command and Control

Command and control includes subjects such as management and control, system integration and information sharing.

Challenges

- Technology in this area of transit security is not the issue, but rather the challenge resides with information sharing and collaboration.
- Effectively addressing the needs of persons with disabilities and special needs (*e.g.,* non-native language speakers).

Approaches/Solutions

- It is essential to keep employees and customers informed. This can be accomplished through passenger information and exchange systems (from the street to the platform, platform to the train, and interaction with the passenger).
- Security training for all transit employees benefits the entire system.
- To avoid language barriers, visuals and a pictorial relay of messages is a very useful way to communication. This however raises new communication problems, including training regular and infrequent riders on the meaning of these types of messages.

Standards Issues

- The proliferation of standards can be problematic. Need to condense, coordinate and make it easier for the end user to implement.
- Transit operators can often "bristle" at standards, viewing them as long to read, costly to implement, and creating new hurdles to meet. Conversely, it was noted that once transit operators become familiar with operational standards and the value they add to operations, they are anxious to expand their knowledge and incorporate them.
- Standards can help with procurement and the best way to spend money on products. There is also the comprehension gap in that standards are a baseline. There still may be the need to augment the standards to account for local requirements.
- Keys for successful standardization in this area include involving stakeholders and users early in the development process, as well as implementing research from the field.
- Gaps for standards in this area include:
    - Portal protection
    - Service interfaces between equipment and legacy systems
    - Interface between stakeholders (*e.g.*, information sharing)
    - Perimeter security
    - Support for modeling and simulation used to test systems
    - Risk assessment, threat, consequence and vulnerability (pre and post mitigation)
- Internationally relevant conformity assessment programs can assist with the challenge of standards being accepted in one place but not another. However, some local situations might result in the necessity of procurement specifications that are significantly tighter than standards.

Sensor Integration (including Access Control/Intrusion Detection)

Subjects covered by this panel included biometrics; intelligent video; explosives detection; sensors for chemical, radiological and nuclear; bio-terrorism and the transit environment.

Challenges

- The openness of the system is a challenge due to multiple entry points and the high volume of passengers in the system.
- The transit system is built for speed and mobility and passengers are sensitive to any delays. Given the volumes of passengers carried in many urban centers, the consequences of delay may have an impact upon the entire urban transportation network.
- Lessons learned from recent attacks on the transit system illustrated that:
  - Attacks are conducted through fare gates
  - Deterrence is critical
  - Aviation-style security is not possible (Mumbai lesson)
- The effects of exposure to biological agents can go undetected for hours or even days. Therefore, formulating a comprehensive response plan for an integrated system forces thinking through all the crisis management details and response management with all stakeholders (*e.g.*, public health). Explosive detection equipment remains an area where the technology is rapidly evolving as the threat environment becomes more widely understood.

Approaches/Solutions

- Automated video surveillance (sometimes called intelligent video, video analytics or "smart CCTV") increases efficiency and becomes a force multiplier. It transforms conventional security video systems into an intelligent tool that enhances the awareness of security personnel and enables more effective responses to security threats.
- Active millimeter wave systems with video tracking combines video tracking of people in frame with millimeter wave radar. Millimeter wave technology is an alternative to magnetometers or similar metal detection capability.
- Intelligent video has detection capabilities such as abandoned/stolen objects, virtual perimeter breach, motion in restricted areas, deviation from normal traffic patterns, and much more.
- Further key points regarding video surveillance include:
  - Law enforcement and legal actions in court increasingly rely on video surveillance evidence.
  - In Paris, all buses and trams (4000+ vehicles based in 25 depots) are each fitted with 4 to 8 cameras, on-board storage, GPS, a radio alarm to the control center, and fleet-wide health monitoring down to the camera level.
- Focus on the fundamentals, such as training frontline employees, public awareness, and emergency preparedness. Grant priority for those addressing fundamentals (*e.g.*, expedited funding for training).
- Informed random screening unites information and indicators in an integrated, risk-based approach to focus screening. Key areas include:

    - Behavior (attitudes, body language, reactions to police)
    - Appearance (clothing, sizes of packages carried)
    - Baggage type
    - Proximity to a target with symbolic value
    - Time and route of travel
    - Specific threat intelligence (gender, ethnicity, age)
- Focus on high risk and high consequence areas (*e.g.*, underwater, underground infrastructure).
- Incorporate visible and unpredictable deterrence tactics (*e.g.*, visible inter-modal protection response (VIPR) teams).
- To truly assist the transit community, technologies must:
    - Be portable or mobile and rapidly deployable;
    - Allow remote viewing;
    - Identify higher-risk persons to be checked by law enforcement officers, potentially useful in conjunction with behavioral observation.
- Chemical detection technology is very valuable for the transit environment. While the threat is very low, the consequences and vulnerability of public transit as a potential target remains very high. Requirements include a low false alarm rate, operating continuously in difficult environments, self calibration, low maintenance costs, possessing a reasonably useful life, and being evaluated with live-agent testing.
    - In the United States, the PROTECT system is a real-time chemical detection system that is located in a limited set of strategic passenger stations.

Standards Issues

- There is a lack of specific standards to build and integrate technologies and systems.
- Standards needed for explosives detection equipment: problems of nitrate vs. peroxide based detection technologies.
- The broadcast industry and the military community have both endorsed a digital video standard that is not proprietary (H.264/AVC), but the security world has not.
- For areas such as video analytics, in the United States there is the Authorized Equipment List (AEL) which provides a list of categories of equipment eligible for grant funding and the Responder Knowledge Base (RKB) contains actual products, including relevant standards for the products to meet. However, there are clearly a lot of gaps in equipment categories where standards are needed.
- In terms of conformity assessment, technologies need to be tested extensively in the harsh settings that duplicate the transit system environment. A useful standard in this regard (*e.g.*, testing and evaluation liquid or particle matter entering equipment) is *IEC 60529 - Degrees of protection provided by enclosures (IP Code)*.

Communications

This area includes emergency communications systems, interoperability (voice and data, surface-to-ground), sensors and how they tie into emergency communication systems (dispatch), and governance.

Challenges

- Sensors and their reliability for emergency communications is an issue.
- Communication to operations control center (OCC) staff and access to information is challenging.
- Question of how does management communicate to its own employees and to the public. There is also the related question of obtaining information from the public to management. In instances of major attack or other emergencies, call centers may be inundated with calls, thus possibly resulting in call centers missing come critical information about another simultaneous attack or incident.
- Communication between first responders is a major issue. This includes issues of cell phone interference and interoperability challenges.
- Surface to underground (and vice versa) communications is another challenge.

Approaches/Solutions

- Human factors is the underpinning of each of the communications areas and needs to be included in the planning of projects for implementing future technology solutions.
- Icons are one effective way to convey messages.
- Important to educate and covey message to passengers that encourages them to help one another during an event, especially for those needing special assistance.
- Key areas for building interoperability include governance, prototype responses for types of scenarios and related pre-incident planning. Exercises and training must accompany any acquisition of communications technology.
- An effective governance structure, including how procurement is handled, is essential.

Standards Issues

- Standards for communications solutions need to take into consideration the following elements:
    - Special environmental conditions (brake dust);
    - Interoperability (integration of systems);
    - Field sensor performance requirements (reliability);
    - Underground to surface.
- For new technology, there typically are not standards yet available. Therefore, the challenge is to develop a product without being able to hold it up to a standard.
- Once a standard is published, what is the best method to get it implemented, the carrot or the stick?

- The compliance program for Project 25 (P25) on Voluntary Common System Standards for Digital Public Safety Radio Communications has produced “robust” radios and a vital standard that includes the following important elements:
  - Supplier’s declaration of compliance backed by formal testing and published test reports.
  - Testing conducted at first, second, or third-party laboratories that are recognized for competence through on-site visits by laboratory assessment teams.
  - Lab assessment process that is patterned off of ISO/IEC 17025 but with an emphasis on measurement competence and repeatability.
- Gaps in standards for communications that were identified include:
  - Interoperability – systems integration standards;
  - Sensor performance issues (standards for chemical and explosive detectors);
  - Human factors issues;
  - Information overload;
  - Transit management to transit employee and user communications links;

Existing Transit Security Standards Initiatives

The following entities were cited at the Workshop as having either published standards, or projects in process, that support the transit security environment. This is not intended as an exhaustive list, but rather groups that were cited as key resources during the meeting.

- ISO/IEC/ITU Security Standards Portal
- ISO/TC 204/WG 8 – *Public Transport and Emergency Services*
  - Proposed candidates for new standards include *Definition and exchange of security incident transport management plans* and *Management of travel information during a security incident*.
- ISO/TC 223 - *Societal Security*
  - WG 3 on "Command and control"
- ISO/IEC JTC 1/SC 37 – *Biometrics*
  - It was noted that larger scale, mass/public transit operations are not yet wide-scale adopters of biometrics, but that biometrics have many roles to play for transit security such as credentialing, physical access control, surveillance, etc.
- JTC 1/SC 29 – *Coding of audio, picture, multimedia and hypermedia information*
  - Standard on MPEG video surveillance
- ITU-T work on Emergency Telecommunications
- American Public Transportation Association (APTA)
  - Working groups on Risk Management, Emergency Management, and Infrastructure Security, addressing the implantation of technology within the transit environment.
- European Committee for Standardization (CEN)
  - CEN WG 161 is an important sub-group addressing the subject of "Protection of the Citizen."
- ASTM International
- American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE)
- APCO International
- Institute of Electrical and Electronics Engineers, Inc. (IEEE)
- National Fire Protection Association (NFPA)
- Security Industry Association (SIA)
- Telecommunications Industry Association (TIA)
- Underwriters Laboratories (UL)

Standards Summary

During the open session following the panels, a number of general observations were made about transit security standardization:

- Standards can help take the base level of where we are in transit security and raise the bar – improve standards and opportunity to raise the entire industry up with it.
- In general, there are still too few standards supporting transit security.
- Many existing transit security standards are too specific on the "what" and not as focused on the "how."
- Effects based standards need to be developed.
- Standards can be utilized to validate expenditures of money (federal level and transit agency level).
- Procurement goals and objectives are a key driver for standards, which may recognize the system peculiarities that could require local capabilities beyond the standards (*i.e.*, temperature and weather related factors, etc.).
- Transit operators need to be involved in the standards development process for it to be truly successful. However, this can be challenging due to required time and cost, as well as the technical familiarity that key decision-makers may lack in important areas.
- Standards simplify product develop cycle by getting the voice of the customer into the process.
- Once a standard is written, strategies for implementation are essential.

Recommended Areas for Standards Development

The following areas were recommended as candidates for international standards development:

- Risk assessment (vulnerability, pre and post mitigation), risk analysis, risk management, and risk sharing for the transit environment
- Video surveillance and support tools for this surveillance
- Perimeter security (especially for open facilities). Should be effects based and perhaps require a suite of standards rather than a single standard
- Sensor performance (chemical and explosives detectors)
- Interoperability (for all areas, including surface to underground)
- Systems integration
- Explosive detection equipment
- Portal protection
- Information sharing (specifically in the area of interfaces between main actors)
- Service interfaces between equipment (especially legacy systems)

Conclusion

The results of this two-day Workshop reinforced why international standardization is important to transit security and for the safety and security of the millions of passengers each day that rely upon it.

- Standardization is increasingly significant for international cooperation.
- Standardization leads to possibilities for enhanced interoperability and shared situational awareness.
- Expanded international networks are created through standardization.
- Standardization facilitates public-private partnerships in the interest of crisis management and overall security.

This report is intended as a resource for those in the transit environment looking to standards and conformity assessment solutions to assist their security efforts.

The report also serves as a call to standards developers to review the gap areas identified in the previous section. If there are already published standards that address these needs, these should be communicated to the transit community for their usage.

Standards developing organizations that have technical committees and expertise in gaps areas are encouraged to consider the development of new standards projects to meet these needs, as well as to engage the transit security community in the process from the early stages.

Attachment 1
Final Workshop Agenda

WSC Workshop on Transit Security

Final Agenda
4-5 October 2007
Thursday: 8:30 - 17:00
Friday: 9:00 – 13:00

Hosted by the American National Standards Institute

Venue
National Institute of Standards and Technology (NIST)
100 Bureau Drive
Gaithersburg, MD 20899
USA

Workshop Objective

To address the strategic role for international standards and conformity assessment programs, as well as to identify the international standards needs and gaps for public transit security, encompassing urban, suburban and regional commuter transportation by bus, rail and the land side of urban ferry operations.

To allow for a manageable and focused discussion the following subjects were considered outside the scope of this workshop: air transportation/aviation security; privately owned transportation; perimeter security; transportation of freight or other goods and services (workshop will focus on the transportation of people).

DAY ONE	Thursday – 4 October 2007
07:30	**Registration** (coffee and tea served)
08:30 – 08:50	**Welcome / Opening Remarks** • Dr. George Arnold, International Organization for Standardization (ISO) Vice-President (policy) and Chairman of the ISO/IEC/ITU Strategic Advisory Group on Security • Frank Kitzantides, International Electrotechnical Commission (IEC) Vice-President and Chairman of the Standardization Management Board • Julian Minard, International Telecommunication Union (ITU), Delegate to ITU-T SG17 (Security) and SG13 (Next Generation Networks)

08:50 – 09:20	**Keynote Address** • Dr. David Mussington, Deputy for Policy and Resource Management, Office of Security Strategy and Special Operations, National Railroad Passenger Corporation (Amtrak)
09:20 – 09:50	**Opening Roundtable Session** Moderator: Jane Bass, Branch Chief, U.S. DHS, Transportation Security Administration, Mass Transit Security *To set the context for the Workshop panel sessions, the opening roundtable session discussed threats and vulnerabilities facing transit security stakeholders, as well as identified approaches/solutions/technologies that are being employed around the world to address the risks.* Panelists • John Martino, Deputy Chief, Patrol Operations Division Commander, Massachusetts Bay Transportation Authority (MBTA) Transit Police Department • Tony Ritchie, Executive Director, Rail and Urban Transit Security Taskforce, Transport Canada • Nick Bahr, Senior Associate, Booz Allen Hamilton • Dr. David Mussington, Deputy for Policy and Resource Management, Office of Security Strategy and Special Operations, National Railroad Passenger Corporation (Amtrak)
09:50 – 10:50	**Panel #1: Physical Security** Moderator: Colin Alter, Transportation Preparedness Officer, U.S DHS, Federal Emergency Management Agency, National Preparedness Directorate, Capabilities Division *Subjects covered by this panel included systems and equipment, and facilities.* Panelists • Colin Alter, Transportation Preparedness Officer, U.S DHS, Federal Emergency Management Agency, National Preparedness Directorate, Capabilities Division • Joseph Christen Jr., Program Manager, Infrastructure Security Program, NYC Metropolitan Transportation Authority (MTA) Capital Construction • Mark Bonatucci, Vice President, Solutions Division, ICx Technologies
10:50 – 11:05	**Break**

11:05 – 12:35	**Panel #2: Command and Control** Moderator: Jane Bass, Branch Chief, U.S. DHS, Transportation Security Administration, Mass Transit Security *Subjects covered by this panel included management and control; system integration; and information sharing.* Panelists • John Hogan, Director of Security Initiatives for Operations, Massachusetts Bay Transportation Authority (MBTA) and Chair, APTA Emergency Preparedness Standards Working Group • Dr. Leif Axelsson, Product Area Manager, Security Arena Lindholmen, Volvo Technology Corporation • Bernard von Wullerstorff, Head of Unit, Rolling Stock and Integrated Rail Systems, UNIFE – The European Railway Industry • Peter Totten, Manager of Engineering, Infrastructure Business Unit, Washington Group International
12:35 – 13:30	**Lunch** (provided)
13:30 – 15:00	**Panel #3: Sensor Integration (including Access Control/Intrusion Detection)** Moderator: Marc Caplan, Chief, Standards Program, National Institute of Justice (NIJ), U.S. Department of Justice *Subjects covered by this panel included biometrics; intelligent video; explosives detection; sensors for chemical, radiological and nuclear; bio-terrorism and the transit environment.* Panelists • Robert Pryor, Domain Manager for Surface Transportation Security Technology, U.S. DHS, Transportation Security Administration • Lance Brooks, Program Manager, U.S. DHS, Science & Technology Directorate, Chemical and Biological Research & Development Office • Dr. Hiroyasu Sato, Assistant Professor, Graduate school of Engineering, Tohoku University • Dan Heater, SPAWAR Systems Center Charleston, Law Enforcement Advanced Technology Engineering • Jean-François Sulzer, Director Advanced Marketing, Thales Security Systems
15:00 – 15:20	**Break**

15:20 – 16:50	**Panel #4: Communications** Moderator: Colin Alter, Transportation Preparedness Officer, U.S DHS, Federal Emergency Management Agency, National Preparedness Directorate, Capabilities Division *Subjects covered by this panel included emergency communications systems; interoperability (voice and data, surface-to-ground); sensors and how they tie into emergency communication systems (dispatch), governance* Panelists • Richard Spatz, Independent Consultant • Luke Klein-Berndt, U.S. DHS, Office of Interoperability and Compatibility • Fran Kernodle, President, Frances Kernodle Associates, Inc.
16:50 – 17:00 pm	**Recap**

DAY TWO	**Friday – 5 October 2007**
09:00 – 10:30	**Panel #5: Transit Security Standards Initiatives from Around the World** Moderator: Maureen Shuell, Director of Communications, Canadian Urban Transit Association (CUTA) Panelists • *Standards Activities of UNIFE - The European Railway Industry*, Bernard von Wullerstorff, Head of Unit, Rolling Stock and Integrated Rail Systems, UNIFE • *Association Francaise de Normalisation (AFNOR) Security Forum* - Francois Neumann, Technical Strategy Director, Thales Security Systems • *Swedish Standards Initiatives in Information/Flow Communications Interoperability and Leadership of ISO/TC 223* - Viktoria Hagelstedt, Technical Expert, Swedish Emergency Management Agency • *Transit Security Standardization Activities of ANSI Accredited Standards Developing Organizations (SDOs)* - Matt Deane, Director, Homeland Security Standards, ANSI • *American Public Transportation Association (APTA) Standards Program* - Harry Saporta, Safety & Security Engineering Specialist, Parsons Brinckerhoff and APTA Security Standards Working Group Chair
10:30 – 10:50	**Break**

10:50 – 11:50	**Panel #6: ISO/IEC/ITU-T Standards Initiatives** *Representatives from international technical committees with standards projects in the transit security area presented on their work.* Moderator: Dr. George Arnold, Chairman, ISO/IEC/ITU-T Strategic Advisory Group on Security Panelists • *ISO/IEC JTC 1/SC 37 – Biometrics*, Cathy Tilton, Vice-President, Standards & Emerging Technologies, Daon • *ISO/TC 204/WG 8 – Public Transport and Emergency Services* – Dave Matta, WG 8 Expert and Principle, Avail Technologies, Inc. • *Activities of the International Telecommunication Union (ITU) – Presentation posted but not delivered at meeting*
11:50 – 12:30	**Open Discussion** Moderators: Mr. Alter and Mr. Deane • *Areas that would benefit from international standardization in WSC* • *Items that participants would like captured in a summary report on this topic (issues, challenges, recommendations, etc.)*
12:30 – 13:00	**Wrap-up and Summary**

Attachment 2
Organizations Represented at Meeting

American Council of Independent Laboratories

American National Standards Institute

American Public Transportation Association

Amtrak

APCO International

ASIS International

ASME Innovative Technologies Institute

Booz Allen Hamilton

Canadian Standards Association

Canadian Urban Transit Association

ISO/IEC/ITU Strategic Advisory Group on Security

Daon Corporation

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik

Embassy of France

Ensco, Inc.

Frances Kernodle Associates, Inc.

Homeland Security Institute

ICF International

ICx Technologies

Innovative Technologies

International Electrotechnical Commission

International Telecommunication Union

ISO Central Secretariat

ISO/TC 204/WG 8, *Public Transport and Emergency Services*

KFH Group, Inc

Korean Agency for Technology and Standards

Massachusetts Bay Transportation Authority

Ministry of Economy, Trade and Industry

MTA Capital Construction

National Fire Protection Association

National Institute of Justice

National Institute of Standards and Technology

Netherlands Standardization Institute

Retlif Testing Laboratories

SECOM Co., Ltd.

Securitas Security Services USA, Inc.

Smiths Detection, Inc

Swedish Emergency Management Agency

Telecommunications Industry Association

Thales Group

The Boeing Company

The JED Group

TKstds Management

Tohoku University

Transport Canada

Transportation Research Board of The National Academies

U.S. Army - Natick Soldier RD & E Center

U.S. Department of State

U.S. Department of Homeland Security

- Science and Technology Directorate
- Federal Emergency Management Agency
- Transportation Security Administration

U.S. Navy SPAWAR Systems Center

Underwriters Laboratories

UNIFE - The European Railway Industry

Volpe National Transportation Systems Center

Volvo Technology Corporation

VRC Corporation

Washington Group International