SANDIA REPORT

SAND 2005-5841
Unlimited Release

Community Enabled Security

John Cummings, Darryl Drayer, Curtis Johnson, Judy Moore, John Whitley

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

Executive Summary

The Advanced Concepts Group of Sandia National Laboratories hosted a workshop, *FOILFest: Community Enabled Security*, on July 18-21, 2005, in Albuquerque, NM. This was a far-reaching look into the future of physical protection consisting of a series of structured brainstorming sessions focused on preventing and foiling attacks on public places and soft targets such as airports, shopping malls, hotels, and public events. These facilities are difficult to protect using traditional security devices since they could easily be pushed out of business through the addition of arduous and expensive security measures. The idea behind this Fest was to explore how the public, which is vital to the function of these institutions, can be leveraged as part of a physical protection system. The workshop considered procedures, space design, and approaches for building community through technology. The workshop explored ways to make the "good guys" in public places feel safe and be vigilant while making potential perpetrators of harm feel exposed and convinced that they will not succeed.

Participants in the Fest included operators of public places, social scientists, technology experts, representatives of government agencies including DHS and the intelligence community, writers and media experts. Many innovative ideas were explored during the fest with most of the time spent on airports, including consideration of the local airport, the Albuquerque Sunport. Some provocative ideas included:

- sniffers installed in passage areas like revolving door, escalators,
- a "jumbotron" showing current camera shots in the public space,
- transparent portal screeners allowing viewing of the screening,
- a layered open/funnel/open/funnel design where open spaces are used to encourage a sense of "communitas" and take advantage of citizen "sensing" and funnels are technological tunnels of sensors (the tunnels of truth),
- curved benches with blast proof walls or backs,
- making it easy for the public to report, even if not sure/"non-event" (e.g. "I'm uncomfortable") and processing those reports in aggregate not individually,
- transforming the resident working population into a part-time undercover security/sensor force through more innovative training and
- adding ambassadors/security that engage in unexpected conversation with the public.

The group recommended that we take actions to pursue the following ideas next:

- A concept for a mobile sensor transport (JMP)
- Conduct a follow-on workshop
- Conduct social experiments/activities to see how people would react to the concepts related to community and security
- Explore further aesthetically pleasing, blast-resistance seating areas
- The Art of Freedom (an educational, multi-media campaign).

Table of Contents

Introduction

Background

The Advanced Concepts Group (ACG) is a "technical think tank" at Sandia National Laboratories. It was formed in 1999 to investigate potential contributions that Sandia National Laboratories might make to solve long-range future problems that impact national and global security. The goal of the ACG is to harness the collective knowledge and creativity of a diverse technical group to solve real future problems of importance to the security of our nation. The Foil team within the ACG is studying the future of physical protection. It is the goal of this team to “foil” the intentions of an adversary, i.e., to make physical attacks ineffective against non-military targets. The team realizes that today’s physical protection systems are based on fixed designs while the adversary is flexible. This leads to a situation of ever-increasing security requirements and costs for facility owners. Therefore, the Foil team is looking at improving the overall security environment rather than fixating on simply adding more guns, gates and guards or other traditional security equipment.

Airports and shopping malls have been selected as case studies by the Foil team. These are facilities that are difficult to protect using traditional security devices and in fact could easily be pushed out of business through the addition of arduous and expensive security measures. Since the public is vital to the function of these institutions the Foil team is exploring how the public can be leveraged as part of a physical protection system. One element of this is determining how security can be improved through an increase in the sense of community. We are therefore exploring ways to make the good guys in public places feel safe and be vigilant while making potential perpetrators of harm feel exposed and convinced that they will not succeed. Hopefully these explorations will lead to new approaches for building community through technology and development of flexible defense strategies.

The ACG FOIL Team has decided to host several Fests to develop innovative ideas for securing public places from threats such as suicide bombings. This is a report of the first of these Fests.

Fests

A Fest is a style of workshop that the ACG has developed and uses on a routine basis. It is an organized collection of brainstorming sessions designed to bring many ideas to a topic from diverse perspectives. The process usually uses written brainstorming and small group sessions followed by large group discussions. The written brainstorms are carried out on large pieces of poster paper placed on the wall with a series of questions from the session topic displayed at each station. Participants are given approximately 45 minutes to move about the room and enter their ideas and react to the ideas of others. At the end of this time, a facilitator takes the poster papers capturing the ideas of the larger group and works with the subgroup to:

- organize the information by creating categories and grouping ideas;
- refine by editing, condensing, and clarifying;
- add new ideas, expand, and enumerate;
- synthesize by combining diverse concepts into a coherent whole; and finally
- create an outline report for the plenary session.

Each group then selects a person to present the plenary report.

The typical flow involves a few rounds of this brainstorming process to bring the entire group to a common system-level understanding of the problem and potential solutions. This is often followed by small group sessions that challenge the participants to develop ideal solutions either optimized from specific viewpoints or dealing with various artificial constraints. Often these designs are used to stimulate discussion of the barriers to and opportunities for making these solutions a reality .

The ACG has found that effective brainstorming occurs when groups of 30 to 40 participants with diverse expertise are involved, and when the problems are presented to the participants from diverse or unusual perspectives. The goal is to make each participant a little uncomfortable but not to be so uncomfortable that they disengage. This process tends to produce copious amounts of input while avoiding groupthink, marginalizes conversation hogs, and obtains input from the more deliberative, less-vocal participants. In this fest, we experimented with a few new features for these workshops – a field trip, journaling and proactive displays – which will be described in this report.

The colored artwork in this report was created by Ken Miller, the ACG resident artist, and used throughout the event to stimulate thoughts.

Session 0: Dinner discussions and Proactive Displays

The Fest began with a dinner and registration for a proactive display technology demonstration (see the next session for a description of this). The opening dinner is an important feature of our Fests, because some thought-provoking questions about the theme of the event are introduced and discussed. The goal is to encourage subconscious overnight preparation for the workshop discussions.

During dinner, the four tables discussed these topics:

Sharing Information

- What information do people make available about themselves in public (with or without intent)?
- In what circumstances are you comfortable sharing personal information with strangers?
- When do you enjoy sharing information with strangers? What information?

Figure 1 - Opening Dinner

Impediments to Community

- When do you prefer not to watch strangers or be watched by them in public?
- When do you choose not to help strangers or be helped by them?
- When do you prefer to withhold personal information in public?
- What public environments are least conducive to community and why?

Observing People

- At what public places or events do you like to watch people?
- What draws your attention to people—appearance, demeanor, activity, etc.?
- What conditions make you feel comfortable to watch people?
- What do you notice when you watch?

People Helping People

- When have you helped strangers or been helped by strangers in public places?
- What leads you to help a stranger?
- What makes you comfortable accepting help?

Registration for the Interrelativity Technology Demonstration

Figure 2 - Proactive Display in Background

Part of the goal of the Fest was to explore some technologies for encouraging conversations and the creation of a sense of "communitas" in public places, so we conducted a demonstration of ***proactive displays*** – large computer displays that can detect people nearby and show visual content relating to those people, to help people connect with each other. Participants were invited to create a biographical profile and submit an image that represented a topic they would be willing to discuss with others at the event – likely as a means of introducing who they are and indicating some hobby or area of interest. These images were then displayed on a large plasma screen at the dinner and participants used RFID tags issued for their name badges to activate their information when they neared the plasma. Unfortunately, technical issues prevented the proper operation of the RFID activation that evening, but the images and participant identifying information were displayed on a random basis throughout the dinner.

Participants were also invited to submit images that represented some their experiences or concerns related to the topics of the Fest. The questions that were posed at the registration site were:

Figure 3 - Registration at Dinner

1. People watching people
    - What places do you like to go to watch people?
    - What kinds of people do you like to watch?
    - What kinds of activities draw your attention?
    - Are there specific events where you enjoy watching people?
    - What kinds of things that people have catches your attention?

2. People helping people
    - When/where have you helped other people?
    - When/where have others helped you?
    - When/where have you seen people helping other people?

3. People sharing "information"
    - What kind of information do people reveal about themselves in public places (consciously or unconsciously)?
    - What kind of information do you sometimes like to share with people you don't know?

4. Counterexamples
    - What kinds of places do you not typically watch other people?
    - What kinds of places do people typically not help other people?
    - What kinds of places do people typically not like to share information?

Session 1: The Environment for Citizens

Our first session was designed to explore what features in public places will make people feel safe and be vigilant, in these four categories:

- Physical Environment - Layout, Architecture and Design
- Technology & Communications Infrastructure
- Processes and People's Behavior
- Role of Overt Security

In a written brainstorm, ideas were collected from all participants on large sheets of paper. Participants self-selected for small groups where the large collection of ideas were discussed and refined into a presentation for the plenary session. The following sections describe the concepts and issues discussed.

Figure 4 - A Written Brainstorm

Physical Environment – Layout, Architecture and Design

Options – Giving people options may help them feel safe. One example of this concept was that people feel safer and less vulnerable when they are driving on an open highway than when they are in a tunnel. They have a feeling that they have more options. Another example of this is the difference in feeling between elevators (containment, confinement, stress) and country roads (open, airy, calm). It was noted that structures can be built in such a way that people feel that they are contained or confined yet still have options.

Transparency - Many comments focused on transparency and the need to provide open visual access. Comments about openness, light, and ease of hearing were recurring themes throughout the brainstorm and specifically about the "back room". Transparency means no dark corners, no alleyways, nowhere to hide, and an ability to glance around in an unobstructed manner. This transparency should be augmented with a very visual presence of security such as cameras and uniformed security personnel. Walls can make you feel safe but they can also make you feel anxious since you may feel confined and unable to be aware of what is going on around you. A suggestion was made that reading "The Social Life of Public Spaces" by William Whyte may help people develop a better understanding of some of these issues.

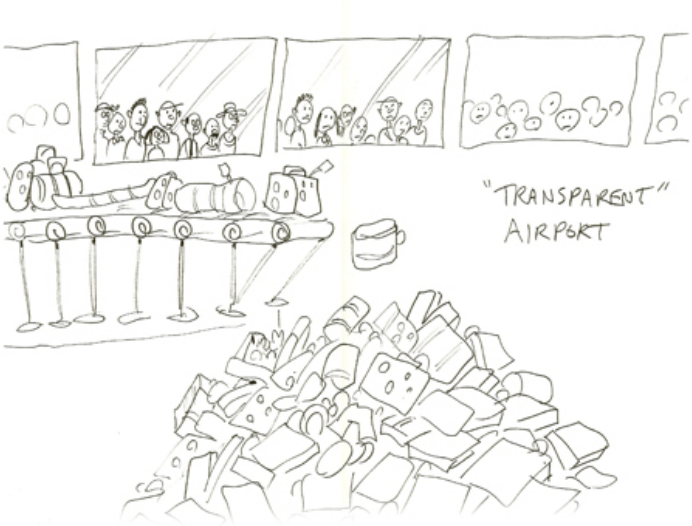

Figure 5 - The Transparent Airport Concept **Illustration by Tim Kirk**

Flexibility – Several comments were made about flexibility. Flexibility is needed to keep up with lessons learned. Also flexibility is desirable in order to reform the space as needed to respond to evolving needs for social interaction. Walls, partitions, seating groups should be easy to reconfigure to meet changing needs.

Activity Nodes – Nodes could be specifically designed for enhancing community. These nodes could foster interactions to increase connectedness between individuals. These nodes could include inward facing seating, and interactive games "in the furniture".

Overt security – One key to feeling safe is to insure that there is "explicit" security. This can take the form of cameras, bollards, and uniformed officer presence. This security must also take into account the behind-the-scenes areas such as luggage/cargo handling, mechanical areas, food delivery, and food service. Security is often minimal in these areas. Overt security can also include useful information using different kinds of media (audio announcements, visual displays) that contain a security message but are also entertaining. Security should be considered in the design of buildings, e.g., optimized for minimum number of cameras for complete coverage.

Concerns/counter arguments – There was a recurring concern about only creating an illusion of security rather than actually increasing security. Another concern was that a high feeling of safety may actually lower vigilance, i.e. if I feel safe I do not need to be as vigilant. People are naturally more vigilant when they feel unsafe, therefore if the desire to increase vigilance maybe an environment should be created that artificially creates an unsafe feeling. Providing people escape routes and places to hide during an event can also create havens for bad behavior.

The main idea from the small group discussion was the concept of two different types of awareness: communicative awareness and reactive awareness. Each type of awareness can be fostered through the built environment.

Communicative awareness is characterized by familiarity, networking, connecting and sharing. The space can be engineered to provide for consistency of behavior. In this type of space people can easily judge what is normal and pattern recognition can be used to note abnormal behaviors. In this type of area non-confrontational, phased "chat-up" security can be utilized. Areas where communicative awareness is being fostered are very open and transparent; the process is exposed.

Reactive awareness is characterized by an increased sense of vigilance and heightened use of the senses. In these spaces people should pay attention without feeling fear. One example of this type of environment is a customs area. When clearing custom, people know they are being watched and are very aware of their surroundings and their neighbors.

Technology and Communication Infrastructure

This discussion was focused on the issue of how to utilize technology and communication infrastructure to make people in public places feel safer. The first observation was that having humans watching and evaluating the situation was still a requirement. The knowledge that "you are not alone" in your security concerns was felt to be vital in creating a feeling of security. Public address announcements and signage that supply people with useful information about security procedures or a roster of creditable threats would help deal with the difficulties of getting Americans to adapt to an environment that is not 100% secure. People should have a feeling of ownership of public spaces that would make them effective "deputies" in the security scheme. Some participants believed that this question has a null answer – what makes people feel progressively "safer" has a reciprocal effect which reduces their "vigilance". The challenge is to make sure that these are linked – if I'm vigilant and everyone else is too, then I feel safer.

We are moving to a world where almost many people have a PDA. These could be used to supply helpful information and alerts, especially if used to teach people what to look for. It would be possible to connect personal (mobile) technologies with site-specific technologies and make these devices sensitive to their location, maybe even using them to make the user look up and perhaps talk to locals. Technology could be used to engage people in their physical space, as opposed to tunneling out to virtual spaces (online) [drop in, log on, and tune out]. One wants to facilitate an outward-looking community aware of its surroundings and not an inward-looking community mentally disconnected from the real world. These systems open up the ability to communicate to those closest to you (in proximity) if needed, creating an easy alert mechanism, allowing knowledge for helpers about where you are and how to get to you quickly. One could enable semi-anonymous ways for folks to interact: blue-toothing with nearby people or create boards and connections and opportunities to move relationships to real spaces.

People already scan their environments in sophisticated ways and respond to the invisible landscape and non-specific cues around them. Technology may be able to enhance the range, acuity, and speed of these scans and add rapid "reputation" information, allowing rapid evaluation of unconscious "threats". An airport back channel monitored by public and security forces could allow the public to easily share observations and concerns. This would require, among other things, a clear understanding of rules and procedures. Multi-dimensional communication opportunities seem more valuable than one-way communication, ("we make announcements to you…"). One avenue would be to create a common cell phone number to access a local security officer similar to the #77 used in some localities to report traffic problems/concerns.

Enhanced, ubiquitous video is becoming common in public places. The facility's video feeds could be supplemented by enabling airport security to receive camera phone stills and video from public. Lots of cameras can make people "feel safe" but can also raises awareness of other problems. For example, we identified the 9/11 and now the 7/7 perpetrators, but also made people realize how ineffective "security was!" "Smart" cameras are needed; cameras that do some processing onboard and transmit reduced information (establish virtual parameter within surveillance systems). The automation of "data" reduction to "information" and real-time communication could help reduce information overload and false alarms. A multi-sensor, multi-

spectral approach could provide more robust solutions (e.g. video, IR, acoustic, LIDAR, etc.). Some really want a sensor system that is able to detect motivation and intent.

The presence of kiosks in the airport that would allow the public to view video camera feeds or perhaps the presence of a Web application for public surveillance of security cameras could encourage awareness in public spaces. This would enable review over short time periods by individuals in the public place and could create a cadre of online security aficionados. The collective wisdom of crowds could be used to collect opinion of the security needed in different locations as a measure of health/security and direct security to pay attention to areas with poor health. This could even be a playful/fun activity. One problem with this idea is that people tend to "see" what they expect to see, even from sensor/cameras (tech systems). This can make them blind to the unexpected; also, humans lose vigilance of tech systems within minutes. Another idea was to have screens in public areas showing what was going on five minutes ago. This would let the public see if bags were unattended for a while. Everyone would be checking with accuracy resulting from redundancy. Participants would be motivated by a feeling of community and feedback from the professional security force. Of course this transparency also means that the bad guys also know what cameras can see and could then plan accordingly.

There is no silver bullet - a technology solution works best when it is application specific! Over-reliance on technology can even cause some to become less vigilant. People are rapid adaptors of technology if it also aids their personal life. How can multiple layers of technology be created that have to be penetrated by the adversary and are supported by the "community" of vigilance? What is the tension between public access to security info/tools (good) and terrorist reconnaissance (bad)?

People, Processes and Behavior

Safety and vigilance are often in tension. Vigilance born out of fear rarely provides a sense of safety. Safety born out of fearlessness, trust in fellow humans, and faith in security personnel and systems usually reduces vigilance. The desired state is calm, alert, and ready to act (but not overreact), while still comfortably engaged in the normal activity of the public place. Public swimming pools were cited as places where people often achieve this state. We are alert for a drowning person, but continue to enjoy ourselves and do not often become fearful or preoccupied with the danger. Driving a car was another useful example.

Many of the ideas generated involved integrating security into processes and mingling service and security roles. Employees (e.g., custodians, airline personnel, and shop and restaurant workers) at a public place could have a security role added to their jobs, if only to report unusual activity. Likewise security personnel could also provide information and expedite processes. Being checked or questioned for security feels better when it is integrated with a service—something I need.

A sense of community among the people in a public place can help create the desired state. The resident workers in a space can play a role in creating and maintaining a communal atmosphere. Activities such as games or a "Jumbotron" sweeping the crowd could be employed. Processes could be established to help people make social connections through their commonalities (e.g., hometown, hobbies, and destination). Processes, architecture or other means could be used to encourage the formation of smaller groups, where people are more likely to bond. Community activities might even be designed to make the stranger or the misfit more noticeable.

Not all community-building would have a net positive effect on security. Some activities could be distracting and reduce alertness or create a false sense of trust or security. Concepts for community building should account for those who will not participate for a variety of reasons.

Deputizing certain people for security tasks was also considered. This could be short-term (while we are on this subway car) or a more permanent status given to frequent travelers or trained volunteers. For example, people who are seated in exit rows in airplanes agree to help in emergencies in exchange for more spacious seating. Poorly executed, this could result in an "informer" or "bully" class reminiscent of fascist regimes.

To be effective in their own defense, citizens must know what to look for, know what to do when they find it, and they must be motivated to look and act. Public education must be used to dispel myths and provide actionable information without fear mongering. Citizens will only report concerns or tips when they believe the information will be used (and not misused) and when they do not fear repercussions. The "#77" cell phone highway reporting number in Maryland was cited as an effective mechanism. On-site, approachable, uniformed people with the means to respond immediately were also suggested.

One final suggestion was creating a mutual feeling of safety through mutual (and equal) vulnerability. If everyone is wearing spandex and carrying no bags, no one can hide a gun.

Role of Overt Security

Overt security provides deterrence and consequently may help prevent attacks. Roles of overt security include: deter; detect; deflect; protect; and potentially draw fire. This was critically shown after 9/11 when the National Guard at airports made many feel safer. This kind of security must be visible but unobtrusive. Security officers and systems must be seen, move around the site, and be alert. It is important that security personnel not be allowed to become complacent. Methods, processes and routes need to be altered on a regular basis – becoming dynamic and unpredictable. Overt security should be visible and interactive – providing a level of trust that people and systems are present to protect and serve. Friendly challenges should be part of that role, things such as asking for ID with credit cards, or asking "whose bag is this?" Random security checks (Q&A) can be important after check-in at a site.

Security personnel should converse with the public - not just "watching" but also interacting (speaking to people, offering help, and enabling people to get where they are trying to go). Security staff should be people that you can go to and discuss security or safety concerns (and get a prompt response). We feel safer when there is a sense that police/security operations are on our side – minimal in presence – and not engaged in arbitrary and abusive behavior or power trips. Some in the group did not agree, feeling that security staff should not talk much to customers, wanting them to be a trustworthy feature of the environment.

Security staff need to be physically fit, well trained and have a professional demeanor. Seeing first responders training would be a good thing. Public education can include explanations of why actions are taken. How security staffs are trained is very important - human error must always be considered and is a special issue when working with lethal means of response. There were

concerns about the possible immaturity of some security personnel with a gun AND authority. The group questioned whether or not a few false alarms might even be a good thing.

There must be a balance between overt security (for deterrence, detection, and response) and covert security (for diligence and for response during incidents). Covert security plays an important role, if it is known to be part of the complete security system (e.g., signs on a highway announcing unmarked patrol cars are present). Other overt security such as signage, cameras, and card readers are visible elements that imply advanced security measures. The "shooters" should perhaps be covert, but the reporting people who prompt action should be highly visible. Mistakes involving guns can have a lethal result, so their use should be restricted to professionals. Mistakes with closed circuit TV cameras (CCTV systems) are correctable, so participation and use by amateurs may be fine (in fact, a monopoly on cameras by professionals may not be best for our society). There were question raised about the role of non-lethal (or less-than-lethal) weapons for the security force, the role of dogs, or the value of having a Police station at the site.

"Helpers" can provide a secondary level of overt security. The role of customer service in security force can serve as a great "screen" to make the public feel safe without being overly surrounded by security (e.g. the Wal-Mart greeter is a key member of their security team). Site "mayors" and "ambassadors" (e.g., flower seller as "mayor of space") may be natural extensions of the overt security force. Perhaps we need "Good Samaritan"-style citizen security – people who are trained, vetted and identifiable to approach with questions and concerns (as an incentive, Samaritans could get expedited trips through security or discounts). "Channels" for the public to report their observations are needed and these channels must provide a professional and reinforcing response of some kind back to the reporters.

Issues and concerns:

- Safe and vigilant in public places seems like a contradiction. Guns and guards imply that there is a threat, and that we are not safe. Are we really trying to balance feeling safer with being safer? Are we more concerned about over- or under-reacting? Do guns in airports make you feel safe or remind you that you are not safe? But how does it make the bad guys feel? There is more than one type of bad guy: some won't be fazed by it, others will.
- Is security an "external" function done "by others" – or do "we" all become part of the "security apparatus?" Are we transferring individual responsibility to the guard?
- Police and surveillance are interpreted differently depending on who you are - teenagers and people of color are more anxious in face of overt security.
- CCTV only works if someone is really watching – "grainy" 7-11 store cameras don't make anyone feel safe or deter criminals. There is a need to evaluate and watch.
- We must remember that giving threat information to the public could alarm them, causing fear rather than increased awareness and vigilance. The group questioned the role of the media to enhance vigilance and educate the public. Should we overtly display threat condition information to support security? How much information is enough?

Session 2: The Environment for Adversaries

Our next session consisted of a written brainstorm in which we elicited from all participants what features in public places might make potential perpetrators feel exposed and convinced they will not succeed, in the same categories used in session 1. These are the ideas generated.

Physical Environment - Layout, Architecture and Design

Uncertainty – In the face of uncertainty, adversaries will not be able to have high assurance their tactics will be successful and that they will be able to obtain their desired outcome. Uncertainty could be created by changing the people flow and by having dynamic spaces. These would be spaces that could and would be rapidly reconfigured.

Denial of Anonymity – A primary means of making perpetrators feel exposed is to deny them the cover of anonymity. This could begin very simply by providing multiple languages on signs – you are spoken to and you are part of this society. This could be helpful in the long term goal of converting potential adversaries into productive members of society. If everyone entering the space could be known and addressed by name, adversaries would feel very exposed.

Layered Security – Many different layers of security are needed starting far away from the "target". Each layer should draw more attention to the potential adversary; put more of a spot light on them. Each layer should also increase the "appearance" of risk to the adversary.

Overt Security – At least a portion of the security system should be overt with very obvious cameras, physical barriers, and security personnel. This overt security should start far away from the target area, e.g., away from the terminal. A part of overt security should be "talk". The Israeli model of in-depth interviews with people would definitely make some would-be perpetrators uncomfortable.

Channeled Detection – Channeling everyone through detector/ surveillance tunnels/ portals will increase the discomfort of the adversary. A surveillance tunnel could consist of a narrow corridor where everyone passing through is being watched. Multiple sensors could be applied in these "tunnels of truth". In some locations, going from the plane to customs already has this type of feel.

Group Formation – Creation of intimate places to sit or loiter could lead to the formation of a sense of community as well as a sense of discomfort by the adversary. Spaces where it would be possible just to hang out that are comfortably anonymous would be eliminated. Intimate group places could be designed for only 6-8 people. These could be clusters of chairs facing each other throughout the airport. Long rows of chairs would be eliminated. This layout would result in random interactions between travelers. This would further lead to some level of "checking" between passengers.

Watchers – It was felt that having bright lighting, no dark corners, and spaces where people can be seen and heard from afar will help overall security. Within these areas a group of "watchers" could be present who would be vigilant about uncommon behaviors. These trained watchers could be a part of the traveling public or could be a part of the paid security apparatus.

Lower attractiveness of target – Placing religious shrines in public spaces that have meaning to would-be perpetrators may provide some level of deterrence. Similarly placing a day care center beyond thick Lexan may deter some perpetrators. In both cases, however, these actions may encourage some other types of perpetrators. Displays about how different cultures value the sanctity of life may also provide some deterrence value.

Technology and Communications Infrastructure

The first question addressed by the group was "what will make perpetrators feel safe?" The answer: they will feel safer when they know the target is understaffed, technology is not maintained, there are inadequate security resources, they will be "invisible", etc. To create an atmosphere of being exposed, one should, as with physical protection, use a layering of technologies and build in redundancy starting far away from the target. An ID with biometrics should always be required and tracked when you enter the site. Maybe one could even collect fingerprints and DNA from card-readers at check-in kiosks. The person's name could be displayed in lights – as in the Hertz rental car agency practice. Entering persons could be required to identify the flight or the person they are meeting or taking. The goal would be to protect privacy, but eliminate anonymity in public spaces. The potential perpetrator should know that the public space has a quick response to anomalous behavior. If the potential perpetrator could be identified, it might be possible to "beam" a message to them, or send them a picture of themselves at the airport. A place of a "thousand eyes" could be created so that no one could assume behaviors/actions would not be reported.

Adversaries should know (or think) that both automated surveillance and people are watching. Specially trained docents could be present to question people to help them get what they need, where they are going, and to alert security of unusual behaviors. The presence of cameras may deter adversaries who are not overly determined; realizing that in some cases the adversaries' cause may be worth the risk to them. Adversaries could also be made to feel exposed by a believable, focused, personalized intention meter that could detect intentions to commit a crime. The adversaries should think that we know and understand their game plan – what and how they plan and execute. They should feel that they are in a high tech defense area, where data is analyzed and then disappears unless it refers to them. This would assure good guys and deter bad guys.

The potential perpetrator should feel that the whole world is watching for them. Security phones should be conspicuously placed with signs encouraging people to use them. People should not be taken out-of-space, but should be making eye contact, listening, engaging in conversation. Potential perpetrators should know that everyone can and will report them! There should be a cell #77 number linked directly to central command in each area – e.g. airports/malls/… as a means of queuing security cameras and personnel. Everyone could be forced into a buddy system or random groupings, using technology to let people know things they have in common with each other. There could be TVs or radio announcements or entertainers that encourage close contact and conversation. Finally, there could be deceptive security/spoofing by changing cameras, lots of parabolic dishes, chips on boarding pass, other processes all with the goal of making someone doing surveillance become confused, concerned, and leave having too much uncertainty to feel confident to plan a successful operation.

People, Processes and Behavior

The most direct means to discourage adversaries is to present a deceptive and dynamic security front. Security-related processes, physical layouts, and personnel should change regularly and evolve over time so that any two surveillance events will provide inconsistent results and add complexity and uncertainty to adversary operational planning. Deceptive defenses—disguising actual defenses and presenting illusory defenses, such as fake or unmonitored cameras and untrained dogs—also add uncertainty, complicate operations, and increase the probability of achieving surprise over the adversary. This approach has drawbacks in its potential to confuse the public or even protective forces. Deceptions can, however, be targeted (through placement, etc.) at individuals conducting surveillance and looking for security systems and therefore be mostly invisible to the normal visitor.

Another strong deterrent is social contact. People conducting surveillance would prefer to feel invisible. Contact can range from eye contact and generic greetings to polite operational-

security-style questions, such as “can I help you get where you are going?” “Where are you from?” And “What’s your business here?” Unexpected interruptions are the most disarming. When these questions are integrated with helpful services, they feel much less invasive and threatening to the general public.

Eliminating anonymity can deter adversaries. Visitors to a site can be required to present ID, or make “reservations” in a verifiable manner. Profiling based on innumerable factors can also be used to give special attention (visible and invisible) to high-risk individuals. This can be advertised or not.

Adversaries visiting a public place should feel constantly observed by cameras, other sensors, and people. Sensors could be embedded in boarding passes and other process-related objects. Anxiety detection and other state-of-mind sensing could be employed. The general public could be encouraged to be observant by a public education campaign and also by monetary or other rewards for tips. Security personnel can be more active and engage with people more, in uniform or in plainclothes. Other staff--for example at an airport, the custodians, wait staff, clerks, pilots, flight attendants, and ticket agents--could be trained as watchers and reporters.

Finally, the social environment of a public place can be configured to make outsiders and those not present for the normal purposes of the space feel out of place and exposed. Events and entertainment designed to captivate or relax people may succeed with innocents and fail with adversaries, making them stick out. Rituals (including the regular processes of the site) can discriminate between regulars and strangers, make regulars aware of who the strangers are, and make strangers feel awkward and exposed. A strong sense of community among the people in a space can also make strangers feel unwelcome and exposed.

Role of Overt Security

Stress seems to be the natural human reaction to overt security (especially dogs). Perpetrators will feel exposed whenever they have a sense of feeling “different” and of being “watched” or “tracked” if they are on a scouting mission. Face recognition technology used when you enter the site could be valuable as well as having the same guards appear in many places. Exposure will also occur with the realization that any person they encounter has the ability to trigger security and attention to their activities. They will feel exposed if they have concern and fear of being recognized, intercepted, or separated from the rest of their group. They will be uneasy with the realization and confidence that the site and security force has sufficient resources to be functional and effective. Another deterrence is the belief that security officers will use weapons if necessary.

Layered defenses and multiple security barriers are very important. Levels of entry with different degrees of surveillance are needed and multiple points of contact for response. Security should question people – like Israeli security officers at the airports - and could act as helpful “ambassadors”. Some in the group felt that security should not be burdened by other roles such as community building. An important element should be lots of cameras and the right kind of cameras. However, somebody must be watching and we must provide actionable imaging - ‘grainy’ 7-11 store cameras don’t deter many criminals. We also need secure space to isolate potential attackers.

An exaggerated, advertised level of success for the security force to create a reputation would be desirable. Unpredictable/random security patrol routes and a clear sense of alertness by guards and dogs are needed. One way to demonstrate these attributes is by having training drills with a rapid response. Staged apprehensions and interdictions with a media component might add to the “reputation”. Drills need to look dynamic and confusing and views of these nasty environments could be shown to the public (e.g., we “case the joint” and then provide visuals, etc. that only such a person would notice or focus on).

Dogs can play an important overt security role in many venues. New technology might include an ultra sensitive "nose on a chip" as part of a robot dog. "Spiders", like in the movie Minority Report, seeking out the bad guys would be a great deterrent if known to be effective.

Issues and concerns:

- Find a way to reduce false alarm rates so that the security forces are better at detection and assessment
- Suicide terrorists do not test reality, so we must use security to attack core motivators

Session 3 The Overlap

Following the written brainstorm in session 2, the same small groups formed in session 1 discussed the ideas that seemed to meet both goals – what features in public places will make people feel safe and be vigilant and make potential perpetrators feel exposed and convinced they will not succeed. These facilitated group discussions generated reports that were given in a plenary session.

Physical Environment – Layout, Architecture and Design

Two types of security are needed; communicative security and reactive security. The physical environment could be designed so that there are areas of each type of security, and the traveler will pass through both types of areas. A healthy combination of both types of security is needed. The layering of these different types of security areas creates a sense of safety for the public and exposes the adversaries to increased scrutiny.

Communicative security could be characterized as "feel-good" security. In these areas there is openness, it is easy to see and hear. These areas will foster communication across the spectrum, e.g.,amongst travelers, between travelers and security personnel, and between travelers and airport employees. Activities in these areas are transparent. These areas create a comfortable feeling for the public.

In reactive security areas the security is overt. In these areas travelers can be looked at individually with a variety of sensors and technologies. Visible cameras, barriers, and security personnel help make the security measures obvious.

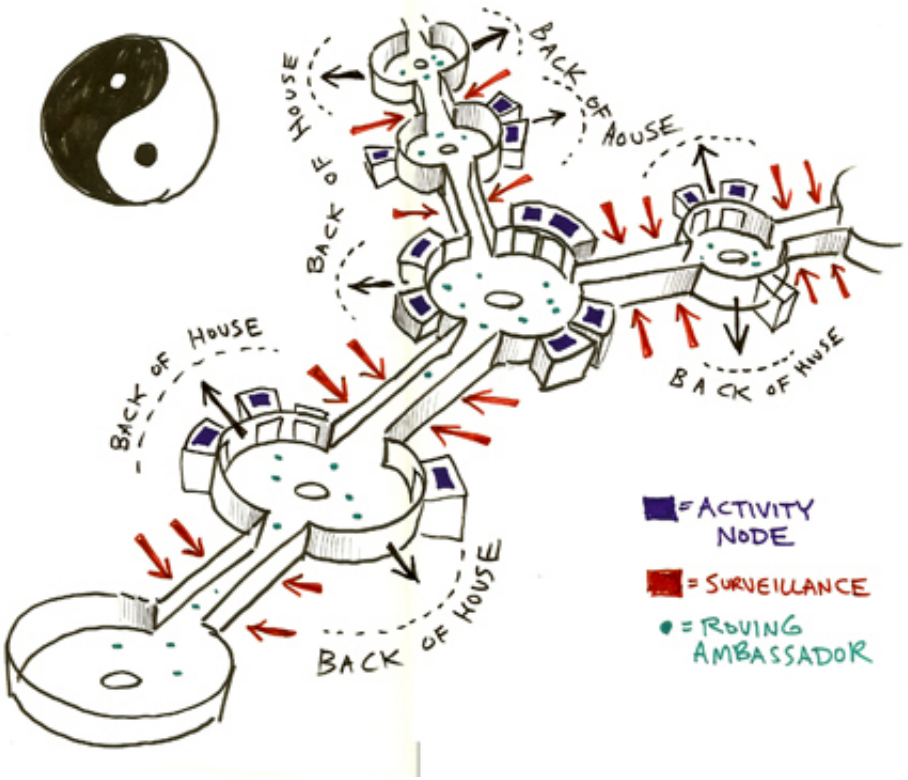

Figure 6 - Layered Reactive and Overt Security **Illustration by Tim Kirk**

This figure provides a graphical illustration of this concept. The illustration begins with open community space that is meant to be friendly. This space is filled with activities and small clusters of chairs that face each other; no one is back-to-back. Between these open spaces people are funneled through narrow spaces; surveillance corridors – “tunnels of truth”. These corridors could be equipped with deployable physical barriers so that if a problem is detected the individual or a small group of individuals could be isolated from the larger population. There is a continuing sequence of narrow and open spaces so that people are constantly “re-surveilled". This is a yin and yang concept of community. The diagram does not need to be taken as a physical design rather it illustrates the concepts of variability, randomness, and re-surveillance.

The surveillance corridors could be distributed or even mobile. For example surveillance and screening could be done while riding from the parking area to the terminal. This is the Judy Mobile Portal (JMP) concept (named after Judy Moore). In the JMP your luggage and you could be sniffed for explosives or scanned using a variety of technologies.

Throughout there is transparency so that people are able to see the back-of-house activities. Ambassadors posted in random places and wandering the facility impart a sense of security, help the public, and also act as detectors.

The idea of privatized distributed security was also discussed. In this model travelers could pay a fee and be cleared through security using private contractors. These contractors would be certified and screen to the same criteria as the TSA. This could provide the convenience of more rapid screening to those travelers willing to pay for the service. By distributing the screening functions, crowds at the airport screening locations could be reduced, thus reducing the vulnerability of large groups of people. Ultimately this may be of benefit to the general traveling public by reducing wait times at TSA screening locations.

Technology & Communications Infrastructure

There are several critical issues around the technology and communications infrastructure in public places. A major underlying concern is that both the media and the government benefit, sometimes quite directly, from fear and disproportionate concerns. The ability of the government or local security forces to provide reassurance and the quick dismissal of red herrings is an important factor in creating a trusted environment. The tendency to play into prejudices or group think and to allow for significant privacy tradeoffs must be avoided to maintain credibility and effectiveness. This will probably require the application of safeguards and constraints. The final major issue is to be continually aware that the adversary also has access to public data and utilities.

Several valuable ideas were generated from this exercise. The identification and application of best practices is a simple and effective way to improve security. Process or structural changes that can remove softer targets (such as the line at security) can have major impact on the attractiveness of a facility as a target. An onsite disposable communications infrastructure (such as 811 vs. 911) could empower the public to alert the security professionals to unusual or suspicious activities. There could even be more highly trained reserves, say among frequent users and employees of a facility. This could be applied along a sliding scale with more training giving more responsibility (and perhaps perks). The Internet could be used to form large, amateur sensor networks or even “smart posses”, reserves, or security aficionados who could watch public spaces and perhaps initiate action.

There are numerous options and approaches to implementing these ideas. A critical issue is to define the roles of both the professional security staff and/or the non-professional “public”. There could also be a redistribution of activities that occur onsite versus those that are moved offsite. The goal is to improve local awareness (outward – looking) and external communication (inward looking) and to utilize the power of human intuition, judgment and/or pattern analysis, to supplement the available detectors and sensors system. One could even apply reputation measure with real-time feedback tagged to individuals, but this would be monitored to avoid abuse. Futuristic ideas included an “intention meter” where patterns, actions, interactions, and body metrics (in response to a query or situation) would be used to determine the intention to do harm. Another idea was a system to do a collective “health” measurement and real time risk appraisal by collecting real time information from the local group in a public setting using some individual devices (such as a ring). To reduce the occurrence of abuse with these systems, the idea of reciprocal power was introduced, where both the “watched” and the “watcher” have access to the information. This open access allows the evaluation of the use of the information, but also makes it easier for the adversary to plan an operation. In these cases, a citizen review group consisting of trusted public members might play the role of watching the watchers.

People, Processes and Behavior

There was more overlap between the ideal environments for vigilance and for dissuading and exposing adversaries than expected. Face-to-face security, integrated with services, is the theme that best exemplifies the perfect marriage of these environments, e.g., personnel who greet, inquire, and direct the public. The public will both feel more secure and be reminded to be vigilant by a friendly and subtle yet overt security presence. A potential adversary doing surveillance will not relish the questions and attention.

This same philosophy holds beyond the initial greeting. The environment would integrate security with the purpose and processes of a site; people would be encouraged to interact with each other and with the resident employees of the site in dual-purpose ways (security and process, security and entertainment, etc.). Those who choose not to participate would likely be subject to more scrutiny, though this would not necessarily involve constant interruption of their peace and

privacy. Instead, it might be a more thorough vetting at the outset or being in a "risk group" that could invite more surveillance, depending upon behavior and other factors. Strangers in an environment would also be subject to more scrutiny, and this scrutiny should feel friendly and helpful to the innocent stranger.

The public should have multiple convenient means to alert the site about concerns (e.g., courtesy phones, a cell phone number, an instant messaging address, and uniformed personnel in sight). This communication system should serve multiple purposes (safety, security, information, etc.) All personnel employed at the site should have a security role—as sensors, as people to receive tips, etc. At least one channel that anyone can use should be anonymous. There should also be at least one channel in which tipsters feel that they understand who is receiving their information and what will and will not be done with it.

The overt elements of security that a casual observer would notice should be designed to avoid creating alarm or excessive privacy concerns. Once again, dual use would be a key principle. A parking garage could be instrumented to protect against theft and assault, to sense a person who needs medical attention, to help a person locate their car, and to prevent terrorism. The overt elements of security that would likely only be noticed by a professional doing surveillance would be more intimidating. Defenses would be dynamic, deceptive, and likely compartmentalized—all designed to reduce the probability of an attack by increasing the adversary's assessment of defenses, making defenses much harder to assess and anticipate, and reducing the value of any insiders. Education of the general public would be required to explain the necessity and value of this approach.

Role of Overt Security

There should be both overt and covert elements to security at the site: overt provides help to the public and imparts a feeling of safety and comfort. Overt helps detect adversaries by interaction and casual questioning. Covert provides response, and covert surveillance, perhaps alerted by overt operatives. Layers of security and public safety support should be considered:

- Overt – primary function is deterrence and response during incidents. Can provide help for customers as well as conducting surveillance. Can also be available as part of the "report to" process.
- Secondary overt support – employees who serve as ambassadors and helpers. They are trained to be vigilant and to respond (positively) to reports of "concern" from the public. They can also assist in some levels (unarmed) of support during incidents.
- Covert – primary functions are surveillance and response during some kinds of incidents.

An "ambassador" role for security personnel was discussed. Should they function as helpers to the public (like English Bobbies) or should they be completely focused on security (like German paramilitaries in airports)?

There are at least three types of perpetrators. Professionals are experienced and are hard to detect because they blend in with the "noise". (These are less likely to be suicide bombers.) Surveillance and planning operatives are more likely involved in a leave-behind bomb attack. Finally the loner, who might be mentally unstable, is more likely involved in suicide bombers. These might show physiological indicators that could be detected before an attack.

It is a natural human reaction that if you feel safe in a situation, your vigilance is diminished. When would you continue to be vigilant and when would you delegate that function to someone else? If it is your life and family at risk you might still be inclined to be vigilant. How do we encourage people to be vigilant by allowing them to act for both the public good and their own self-interest?

How much information flow can the security-side handle? How much information can your system handle and react in a timely manner? False alarms can be tolerated in an environment where heightened vigilance increases general security but does not overwhelm the security apparatus. How much will the public tolerate as far as intrusions into their privacy for security? There will be more acceptance of invasion of privacy during times of crisis. How do you maintain the level of awareness after a crisis or heightened alert has passed?

Educating the public is important. Effective use of the media for good risk and response communication is essential. Repeated visible exercises can be very helpful. The public must know they can bring concerns to overt security personnel, and their concerns will be acted upon. In addition, leverage a citizen corps can be leveraged, as well as a medical reserve. This may not be optimized in the current DHS plans and structure. Right after 9/11, the public in New York wanted to get involved. However, it is not clear if any of the public participation ever came to anything. In New York the perception is that public behavior has gone back to pre-9/11 attitudes because the public's desire to get involved in their own security was not acted upon by the government.

Session 4: Synthesis through Journaling

Participants were asked to reflect upon and synthesize the ideas developed so far for soft target environments by addressing the following questions in their journals:

1. What images, stories/events, and places are stimulating your creativity about soft target environments?
2. List the most intriguing ideas for soft target environments you heard this morning and last night.
3. Imagine you are the leader of a new team tasked with redesigning a soft target environment. At the first meeting, you want to give a short talk to give the team the benefit of your thinking so far. What would you say? What would you point to as the key:
   a. Goals or criteria?
   b. Elements?
   c. Issues/Constraints/Risks?
4. (Extra Credit) Synthesize a couple of ideas that intrigue you into an imagined environment (circle these in #2 above) and then tell a story about the experience of an individual (yourself, an innocent, and an adversary) in that environment.

The available time limited the discussion of journal entries. To give the reader a sense of the exercise, the journal entry of one participant is included.

What images, stories/events, and places are stimulating your creativity about soft target environments?

- Kitty Genevese murder (1964)
- Theological student experiment re: Parable of the Good Samaritan
- 9/11
- Israeli experience with suicide bombers
- London bombings

List the most intriguing ideas for soft target environments you heard this morning and last night.

1. Supportive (or helpful) interruptions -- belief is that when people determined to commit heinous acts are unexpectedly and persistently approached and engaged in discussion (Can I help you? etc.), they are more likely to be exposed or deterred.

2. Create an environment where such interruptions are both natural and expected (e.g., former WalMart greeters or Hare Krishna solicitors). It was pointed out that no one loiters at a car dealership.

3. Separate people from their possessions before lucrative target sets present themselves. Best environment would isolate person and possessions simultaneously so that an alert traps and confines perpetrator (Lexan booth/tunnel of truth/etc.). Big challenge is to make the isolation/testing very fast so that it does not impede the flow of people (tolerance only goes so far).

4. Empower people to act on their suspicions ("811" or "blue light" phones) and ensure that actions taken as a result of such information does not discourage people from reporting in the future (e.g., reporting abandoned bag resulting in evacuation of terminal, delayed flights, missed connections, etc.)

5. "Back of House" views of behind the scenes processes. Being able to watch baggage handling, for example, is equivalent to being able to see the kitchen in an upscale restaurant. It offers reassurance without interfering with the process.

Imagine you are leader of a new team tasked with redesigning a soft target environment. At the first meeting, you want to give a short talk to provide the team with the benefit or your thinking. What would you say? What would you point to as the key?

Goals or criteria:

- Protect people
- Identify potential troublemaker
- Do not impede the primary business model of the site (that is, keep people moving)
- When possible sample/screen when people are engaged in other necessary actions or being entertained
- Empower stakeholders

Elements:

- Avoid bottlenecks (lines)
- Separate people from property for inspect
- Utilize multi-spectral sensors (layered defenses)
- Plan ions for surveillance, analysis, action, mitigation

Issues/Constraints/Risks:

- Keep people moving
- Respect privacy (avoid overly invasive techniques)
- Cost (must be reasonable, all measures pose a terrorist tax)
- Flexibility (criminals will adapt methods to thwart static procedures).
- Anticipate actions.
- Mitigation -- nothing is foolproof
- Layered defenses -- against people, against substances, against kinetic energy
- Plan using multiple perspectives: System (e.g., transportation); Location (e.g., airport); and individual

Synthesize a couple of ideas that intrigue you into an imagined environment and then tell a story about the experience of an individual in that environment.

Ahmed had lived most of his 25 years in the Bronx, having been brought to America by his parents at the age of 5. For most of those years he had been grateful that his parents had moved from Yemen. He graduated from public schools and NYU, and had been employed for several years with an insurance company. His initial reaction to 9/11 was shock and revulsion. However, administration policies began to anger him and, as a devote Muslim; he came to believe that the

administration had declared a covert war against Islam, despite public protestations to the contrary. A trip to Yemen to visit relatives cemented and heightened his feelings about American policies. He came home burning with a sense of outrage and helplessness. However, he did not share his feelings with anyone, including close family. He started studying suicide bombings and came to believe that martyrdom would both prove his devotion and empower him. He concluded that he would detonate a device in a public place as his last act. He settled on the Mall of America in Minnesota.

His trip to Yemen had placed Ahmed on a watch list that alerted when he purchased his ticket to Minnesota on line. It also triggered an agent that would review and track recent and subsequent charges on his credit cards. He decided to purchase most of his material on site so that he would not trip any alarms en route. At the airport, an airline credit call shill (also trained as an observer) engaged Ahmed in conversation. He found nothing suspicious but reported his contact to authorities. When Ahmed checked into a hotel in Minnesota, local authorities were notified but were told the risk level was low. Ahmed cased the mall for several days. Each time he entered the mall through revolving doors, he was automatically screened for explosives and other substances. On the selected day, he was noted buying a backpack and then discretely buying quantities of nail polish remover and hydrogen peroxide from several mall stores. He was also noted buying electronic parts from Radio Shack and an electronics boutique. Authorities notified store security, but extensive camera surveillance failed to locate him. Ahmed knew that the only place he could assemble his device without being seen was in the rest room. Fortunately, an alert patron noticed the strong smell of acetone and alerted security. They intercepted Ahmed coming out of the rest room and prevented him from detonating his device. The patron was given a substantial reward, declared a hero, and received great local press.

Session 5: The Field Trip: The Albuquerque Sunport

Following our theoretical discussions, we took a field trip to the local airport, the Albuquerque Sunport, to observe some spaces in preparation for our next day design sessions. The Sunport was gracious to allow us this opportunity. We divided again into four groups to explore public areas where potential perpetrators could do surveillance and in common use by the public. The areas were selected because of the current layout of this airport. All of these areas are located before passengers go through the security checkpoint. After the tour, the groups had dinner at Gardunos Restaurant located in the airport and began discussions of what they had learned.

Rental cars, information desk, transportation

Figure 7 - Information Desk at the Sunport

Figure 8 – Close-Up View of Information Desk

Figure 9 - Offsite Rental Car Counter

Figure 10 - Rental Car Shuttle

Figure 11 - Taxi Pick-Up Zone at Sunport

Passenger Drop-Off, Pickup and Parking

Figure 13 - Offsite Parking Shuttle

Figure 14 - Parking Garage at Sunport

Figure 12 - Passenger Drop-Off at Sunport

Ticketing, Check in, and Baggage Claim

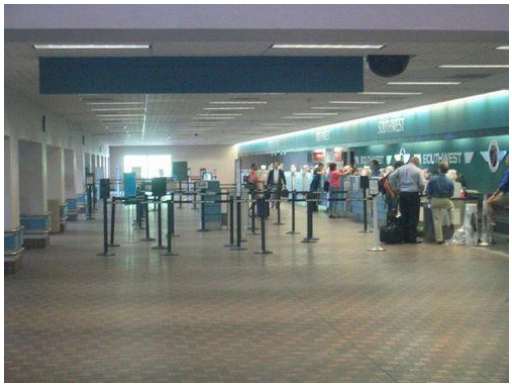

Figure 15 - Ticketing at Sunport

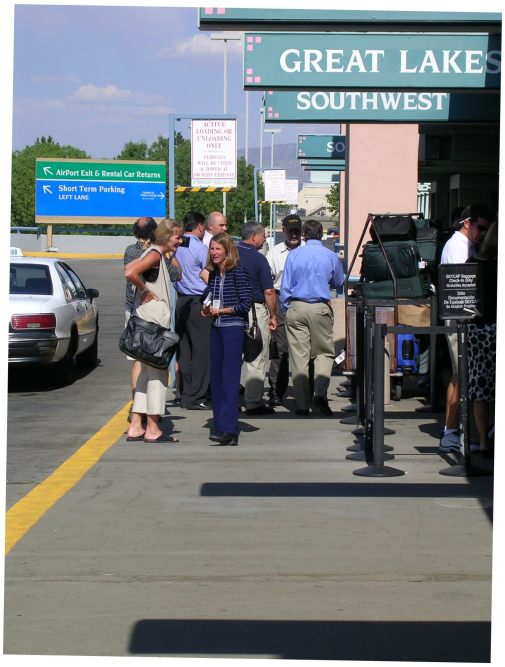

Figure 17 - Baggage Check-In at Curb

Figure 16 - Baggage Claim

Shops/Food and Meet/Greet Area

Figure 20 - Shops in Meet/Greet Area

Figure 19 - Meet/Greet Area

Figure 19 - Aircraft Display in Great Hall

Figure 18 - The Sunport Great Hall

Session 6: Developing a Vision for the Sunport

We began this day with small group discussions about what could be changed in the Albuquerque airport based on the principles of creating an environment in which the good guys feel safe and will be vigilant while the bad guys will feel exposed and deterred. Each group then reported their results to the plenary, describing possible changes to the physical layout, architecture and design, technology & communications infrastructure, processes and people's behavior, and the role of overt security.

Rental Cars, Information Desk, and Transportation

The general idea was to open the airport up, move things away from the airport and distribute them more. The physical layout could be modified so that vehicles cannot get close to the airport itself (even using support vehicles for fuel, food, trash, etc). The focus was on various attack vectors (mostly around explosives in luggage and on people). The rental car, info desk, taxi/shuttle subsystems could provide two major elements:

- Positive customer experience and assistance
- Surveillance of the customers and their luggage

The current rental car center at the Sunport is good because it is located far from the terminal. Being far away, it gets traffic and potential bombs away from the airport proper and provides the opportunity to scan people and bags on the way to the airport from the center.

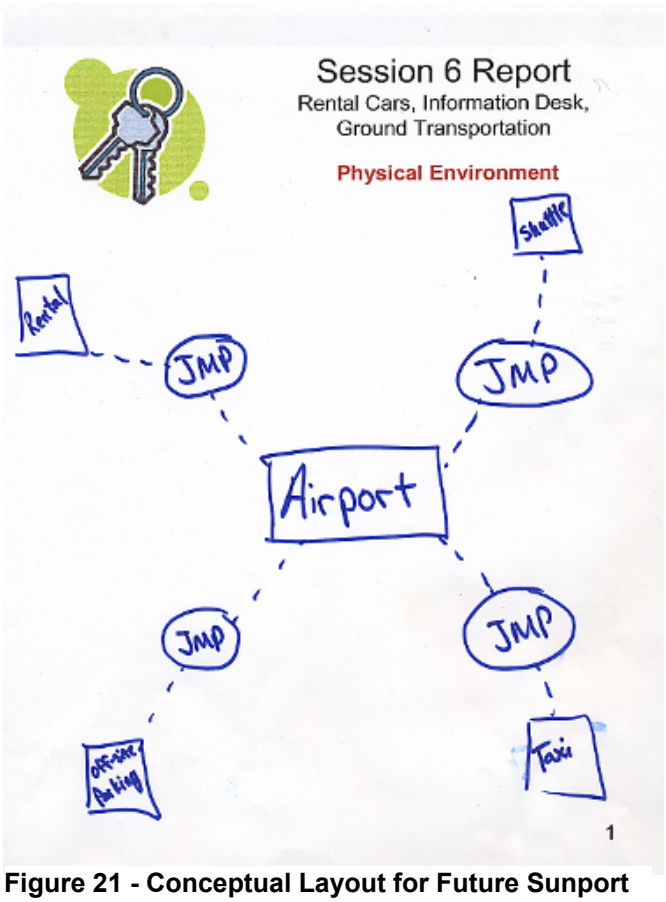

Figure 21 - Conceptual Layout for Future Sunport

Rental car shuttles, taxis, buses and shuttles will all drop off customers some distance from the airport itself (at least several hundred feet). A hub-and-spoke structure may work, with the terminal as the hub and other services the spokes. Distributed (to avoid crowds) entry points will then move the public to the airport via JMP-type systems (could be vehicles or even a conveyor belt type of "people mover"). Luggage will be moved to the airport separately (sniffed and detected along the way).

Everyone in the community at the airport must be trained to have a certain level of security awareness and the ability and encouragement to report concerns to security personnel (Taxi driver, shuttle drivers, rental car clerks, and maintenance personnel). The public must also be aware and have the ability to report concerns with

well-advertised lines of communication, and phones everywhere with signs saying they can and should be used as tip-lines. Creating a neighborhood-watch type atmosphere and community would be good and use numbers like #77 for some kind of passive non-emergency tip-line.

Physical Environment

The design goal was to move the security system away from the terminal – yet create an overall community. The concept is illustrated in Figure 22, using the concept of a JMP to move people and goods among various parts of this environment.

Technology and Communications

The suggested improvements were:

- provide enhanced sensors such as sniffers (to detect explosives, chemicals, radioactive materials, etc), CCTV (with automated surveillance),
- use JMP systems (mobile people and luggage mover platforms with embedded sensors as well as communications),
- assure multiple ways for two-way communications (e.g., “I’m on my way”, “here is your flight info”, airport directions, etc.),
- provide awareness training and describe the methods to communicate concerns (e.g., #77 or 811 from any phone), and
- assure communications are available throughout the system and that there are passive alarms.

Process & People’s Behaviors

Workers, stakeholders, and customers need to be trained to be more aware. This includes shop workers, taxi and shuttle drivers, and restaurant workers. There should be communication plans in place like neighborhood watch. “Reporting” should be more distributed and more convenient. Everyone (including customers) should feel they are part of the enhanced security system.

Overt Security

The present role is appropriate. Increased covert security with additional sensors and CCTV systems would be good. It may be best if customers do not know what is going on with luggage inspection like exactly what sensor and detection systems are being used and how they work.

Possible Downsides

People might be wary of checking luggage so far from the airport itself. There will be more opportunity for airlines and airport workers to lose the luggage. Need to be careful about encouraging the public to be part of the security team and then secretly screening/analyzing them. Care must be taken when eliminating crowds of people, so that new crowds are not created in different locations. It is labor-intensive to provide training and raise awareness level among everyone in the community: taxi drivers, rental shuttle drivers, janitors, customers, etc. The JMP system misses those people that get dropped off directly in front of the terminal if that is still allowed.

Passenger Drop-Off, Pickup and Parking

Parking, pickup, and drop-off areas are the gateway to the airport. These areas are the most vulnerable to a vehicle-borne explosive threat, which could arrive and be detonated in seconds. This is perhaps the simplest and least preventable attack available to an adversary. These areas also set the tone for the airport environment, as they are the first phase in a person’s airport experience.

Relatively simple technical measures can reduce the threat of vehicle bombs. Side and overhead barriers can limit the height and width of vehicles that can reach the pickup and drop off areas. Bollards can be added to keep vehicles from penetrating the airport building. Blast deflectors can be added to limit building damage in the event of a detonation. More cameras further out and cameras that look into approaching cars could be used to identify and stop suspicious vehicles. A more sophisticated approach could include a "weigh station" for approaching vehicles, a camera, and an algorithm comparing vehicle volume to weight to identify vehicle bombs. We are not aware of such a system, but it appears quite feasible. Especially heavy vehicles could be stopped well short of buildings and populated areas.

Parking garages are dark, unfriendly places where we harbor fears of theft and assault. Today there are a few security cameras and occasional vehicle patrols. The vision was parking garages as "aware" spaces for multiple uses. Cameras, robotic vehicles, overhead cameras on tracks, and other sensors would provide awareness. Beam breaks with audible warnings and help could increase the sense of awareness. This awareness could be used not just for preventing terrorism but also to: escort a person safely to their car, help someone find their car, get help for a person in a medical emergency, locate empty parking spaces, check if a vehicle's lights are off and windows rolled up, or find a fellow traveler who "just went to park the car." If passengers received all of these services from cameras and sensors—if awareness were for safety and service, as well as security—it would be regarded in a much better light.

Public messages to increase vigilance could be integrated with service information (e.g., flight status, delayed flights, levels with available parking, and current wait time at the security portal) so that they will be read.

The public should have ready access to means to report concerns and tips, via available phones, a number available for cellular phones, uniformed personnel, etc.

Both the real and virtual (e.g., web and public relations) spaces should be adjusted with surveillance in mind. Communications can be adjusted to create uncertainty and doubt in potential adversaries. "Honey pots" can even be put on websites for unusual search criteria that an adversary might use. More, and more overt, real and fake cameras can be added at little expense. Photos of suspicious and loitering vehicles can be mailed to vehicle owners to send the message that we are watching those who watch us.

Ticketing, Check in, and Baggage Claim

The initial impression of the Sunport ticketing area is that it was designed for efficiency, not security. There are few visible signs of security in this area which leads to a feeling of a lack of security even if covert channels exist. Overall, the check-in area feels fragmented and what seating is available is not set up to facilitate conversation as it is fixed and does not form conversation circles. The major queuing points in this area are at ticketing, with some lesser lines at the skycap curb check-in area. The team did notice that while the departure flow has some sense of "joining" a shared activity, the arrival flow is very transient with everyone anxious to get their luggage and exit. This makes security in the arrival area a particular concern. Overall, the Sunport does have a lot of open spaces and a strong Southwest theme which create a friendly, interesting, open, and inviting space with a strong local flavor.

The ticketing team felt that there were several areas where process and physical layout could be changed that would affect the overall people behavior and lead to an increased sense of security. One suggestion was for more consistencies in security with more visible cameras and uniformed security personnel. It was also observed that you could probably use interesting displays to start conversations between strangers. For example, an interactive display(s) in the ticketing line could display real-time pictures of destinations served by flights currently being ticketed. Other activities could be used as long as the focus would be to define self-organizing

activities that would lead to fun, not fear. One could also use live "performers" to entertain and even assist with traffic flow. One issue of note was the question as to whether having "fun" makes you less vigilant. If games are used to assist with security, they need to be carefully evaluated before widespread implementation.

Technology and communications could be much more effectively utilized at the Sunport. Things as simple as variable audio announcements could be used to alert travelers if they also supplied real-time useful information about the airport. There was a general feeling that there was a lack of phones, especially a place to report concerns. What paging phones exist are not well marked and not advertised as available to report concerns. One could add more of these types of house phones and then tie them into the security force system. The Sunport could also make use of interactive/static displays on queuing posts that would provide a view of different areas of the airport. This could engage travelers in watching for unusual behaviors. Interactive displays could also be used to train the public on what to watch for. An extension of this idea would be to create a subset of travelers who are the "watchers" and who would receive special training on security issues.

Finally, it was felt that overt security was not being fully utilized in the security scheme. The use of roving security interviewers could provide both a traveler service and add a layer of security. Numerous signs and billboards should be used to reinforce the message that the security force is the enforcer, but that it depends on the public to act as observers and to report unusual events. The public should be confident that their reports will be taken seriously and investigated promptly. Visible uniformed officers are essential. Some airports use police on Segway scooters to play the equivalent role of police on horseback. Being visible, approachable, and mobile are the essential characteristics. Finally, the airport should use more movable blast-resistant barriers to minimize any effects of explosive devices and make attack planning more uncertain.

Shops/Food and Meet/Greet Area

This group studied the shops and food areas at the Sunport just outside of the TSA security checkpoint. In addition, the meet-and-greet area at the exit of the secure area was analyzed.

It was noted that these areas could provide an economic advantage to the airport and be a place where people want to gather, rather than a sterile environment. This economic windfall could even be used to fund more security. Of course the problem that must be managed is the attractive target that a large number of people in one location represent. In addition, activities just outside of the security checkpoint provide an "excuse" for being in the area thus making it more difficult to discern when someone is "casing the joint". People who do not have a legitimate reason for being in the area may not stand out. Immediate and easy things to do would be to eliminate blind spots caused by some kiosks and to insure that blast-mitigating trash cans are utilized.

It was suggested that the meet-and-greet area and shops could be converted into an area with a café ambiance. The area could be designed to have an enchanting or exotic feel rather than industrial. Since wi-fi is already present, tables and seating could be provided to encourage computer usage. Seating could be arranged in semi-circular fashion in order to foster human interactions and observation. To help break up the crowd and to foil potential bombers, blast resistance could be built into the seating design. Blast-resistant clear plastic, etched with artistic designs, could be used as backing for the seating clusters. The clear plastic would allow people to see the entire area, making it feel open and bright while also mitigating the effects of a blast. Even if the blast resistant plastic is not totally effective it would have a detrimental effect on an adversary by introducing uncertainty, i.e., they can not be assured that a bomb would have the desired effect. Similarly aesthetically pleasing blast mitigating panels could be used to form the aisles of the serpentine leading to the security check point.

Figure 22 - Concept for Transparent Barriers in Queue Illustration by Tim Kirk

Another element that could be present in this space is a “Jumbotron”. As at sporting events, the Jumbotron could display pictures of people using the space. This could increase the discomfort of an adversary, making their pre-operational surveillance uncomfortable since they know that their image could potentially be shown to everyone in the airport as part of a “fun game”. These displays could also be used for informational announcements about safety and security. This would primarily be effective against surveillance missions, not against those already there to bomb the place.

Another concept would be to allow retailers to develop their own privatized security portal. For example the restaurant presently located in the area could have its own privately run security portal. Eating at the restaurant could allow you to use their portal which could have much shorter lines than the public portal. A completely privatized portal could be developed where people could pay to have shorter lines or more polite service at the screening point.

Figure 23 - Fast Pass Concept for Security Illustration by Tim Kirk

The use of security pagers, which could be run either privately or as a normal part of the TSA process, was another concept discussed. These would be pagers similar to those used when waiting for a table at a restaurant. When you check in for your flight you would be issued your security pager. Instead of going directly to the security check point you would wait for your security page. When you receive your page, it would be your signal to go to the check point for screening. This could help manage the length of lines at the check point. Another lower-cost alternative for managing lines at the checkpoint would be have a time printed on your boarding pass for your security screening appointment.

Training of the workforce in this area is also important. This includes food and beverage workers and airline employees, as well as airport employees. The entire workforce could become observers as well as ambassadors to the public. The number of interactions with the public could be greatly increased if all workers were encouraged and rewarded for being ambassadors. As the number of interactions increases the ability to detect or even deter malicious behavior increases.

Overt security in this area is also important. People need to be able to see some of the security measures. Also security measures need to start well before people reach the screening area.

Session 7: Developing a Vision for Future Airports

With the local airport experience completed, four new teams were formed to design an airport of the future applying what they had learned so far about creating an environment in which the good guys feel safe and will be vigilant while the bad guys will feel exposed and deterred. To challenge the thinking and begin the exploration of the downsides of any of these concepts, the groups were asked to emphasize a particular possible feature.

Like a Subway - Fast, No Loitering

The purpose of this design activity was to create a design optimized on limiting the amount of time spent at the airport. This “subway” type design would get a traveler from their off-airport location onto the plane following the subway model with movement the key feature. If you can keep people moving, you can minimize queues and hence improve security or at least reduce vulnerabilities. In an airport, the major bottlenecks and impediments to speed are at ticketing and at the gate. This design minimizes these queues by doing as much as possible off-site, including at home. For example, you would print your boarding pass at home or office with your photo printed on your boarding pass. If it’s an international flight, you would have passport verification integrated into the boarding pass. You could also print your baggage tags at home, attached to the boarding pass by a perforated edge. When you print the boarding pass, you would automatically alert the airline as the approximate time you expect to get to the airport. When you arrive at airport, you would show security your boarding pass and luggage tags and use biometrics as a quick way to confirm your identity (perhaps a retinal scan). Security then rips off the baggage tags from your boarding pass, attaches them to your bags, and takes the bags. You would then proceed through a metal/bomb detection system, directly onto a bus or train that stops right in front of your airplane. For frequent travelers, you would have pre-screened your electronics and other metallic items, storing their image, such that they could be automatically processed by the x-ray imaging system.

The airport in this design would have very few amenities, no restaurants, *and no restrooms* (just kidding). Its design would strongly discourage waiting around but would make your experience fast and predictable. You would not feel the need to allow for contingencies. Since airports are located outside the city, speedy mass transit lines should be available from the city to the airport. This would also allow for pre-processing of passengers during the travel time. If the plane is late, passengers would not be allowed to leave the parking area until their plane is ready. A

major requirement for this design is that people must be willing to give up a little bit of privacy to gain speed and efficiency at the airport. The benefit would be no crowds in the terminal and a highly efficient, rapid airport departure experience with greatly enhanced security.

Maximum Offsite Operations

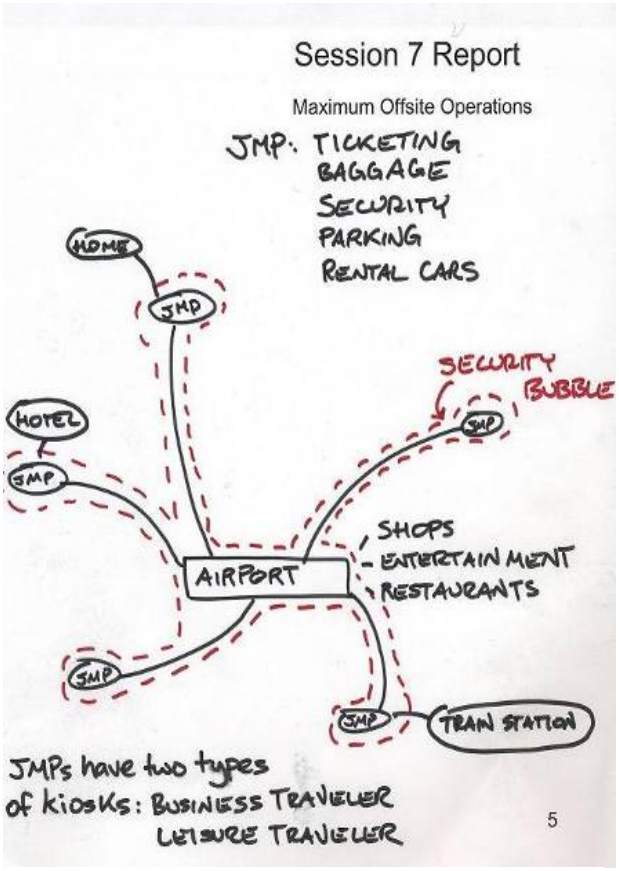

Figure 24 - New Design for Maximum Offsite Operations

The concept is to build a security bubble around the extended airport "system" (which would include the pathways to get from the offsite locations via JMP systems as well as the airport itself – see Figure 25). This creates a "sterile" airport from a security perspective. This could make the airport a possible local "destination" for dining and entertainment as well. The variety of users would need to be addressed: "just in time" travelers, family and leisure travelers, local customers (who would enter the JMP to get to the airport for shopping, dining, entertainment), employees, etc. There is also the need to address airport supplies and services (fuel, food, water, trash removal, etc) so that they do not have direct access to the airport itself (transfer to secure JMP-like systems). The major advantage of this concept is that it disperses "soft" targets (people) across many geographically dispersed locations.

Distributing the system takes the large soft target of airport crowds and parses it into many smaller groups that are less appealing to terrorists. Offsite operation elements and locations could include the customer's home for remote phone or internet check-in. It would consist of pickup hubs, JMP Points, where ticketing, baggage, security, parking and rental cars are all handled. This will require cooperation between competitors (airlines, rental car companies, vendors, etc.). Many JMP pick-up and drop-off points could be scattered throughout the city so that one is always conveniently located (e.g., at malls, office parks, hotels, park-and-ride locations, rental car area, and intermodule facilities, etc. Tailored locations for families and business travelers could be offered. Baggage could be sent ahead after offsite check in. "Ambassadors" could be involved (selective process) in making customers feel welcomed and part of the community (while providing surveillance of the customers).

Benefits include increased use of mass transit - saves gas and money (need buy-in from mass transit authorities, businesses, and government). This would add to the economy outside the airport instead of just at the airport by creating new opportunities for offsite businesses, hotels, etc. For example, a hotel could offer a JMP point and efficient easy processing as part of the incentive for passengers to stay at their hotel. The distributed JMP locations create more layers of community and security and ambassadors. The smaller groups encourage community because people from the same neighborhood who all travel often will get to know each other more by seeing each other frequently at these JMP points - "bonding" (sense of community;

perhaps built on geographic familiarity – others from your home community) begins at the offsite location with small groups traveling together to the airport itself.

This would provide a combination of speed and efficiency with increased "enjoyment" of the traveling experience. Inexperienced travelers don't hinder veterans as much with tailored entry locations. Those frequent travelers who want to participate could trade some privacy for speed/convenience as part of a "super trusted" traveler program: biometric ID systems and enhanced personal and luggage screening.

A "Theme" Airport

A theme for the airport could provide several benefits. A theme could create a sense of community through a shared "experience" in a manner similar to theme parks. The airport could become more of a destination and improve its profitability. Providing a theme could facilitate the use of non-traditional crowd-control methods that go along with the theme, and the variability of the themed environment could make an adversary uneasy. If the theme and the facility are constantly changing, it would be more difficult to do surveillance. Some people may even be more willing to participate in security if it is themed. It might be easier to encourage employees to act if they are "cast members" rather than security employees. In the post-9/11 environment the family aspect of meet-and-greet, the tearful goodbyes at the gate and the cheering family as someone walks off the plane have all been lost. A theme could potentially ease these transitions for the travelers and their families.

On the other hand themes could also have drawbacks. They could detract from the airports' main goal of transporting people. Similarly creating too much of a fun atmosphere could make people forget it is a serious place, with serious security concerns and therefore become less vigilant. Themes can also get old and stale quickly. At some point people may lose interest in the theme and simply find it annoying. If an airport becomes a symbol simply because of the theme, e.g. the Mall of America, then it may become an even more attractive terrorist target.

An alternative to a completely themed airport would be having pockets of themes. These would be places where some people could become absorbed in the theme without distracting those who don't want to participate.

The following is the list of ideas that were proposed as themes and theme conversation starters:

- Pet
- Prison
- America's most wanted
- Smart-tech
- Desert
- Native American
- Retro Tech
- Bunker
- Luxury/Casino/Luxury liner
- A club
- Tropics – Jungle South Pacific
- Surveillance
- Candy
- Willy Wonka
- Rock n roll
- Southwest
- Sports
- Seasonal – changes w/time of year or what's going on in city
- Rapid change of theme
- Historical
- Nature/ecology

The group briefly explored the elements of a specific theme. As a think exercise the group focused on giving an airport the theme of a small rural southwestern town since an airport is like a small-town that is continuously recycling because of the constant influx and departure of townspeople. It can be thought of as a one-hour small town. Some individuals became even more specific, thinking of the theme in terms of the novel "The Milagro Bean Field War".

The following are some thoughts on how various elements could be incorporated into an airport.

- The tag line for the airport could be "Milagro – No One's a Stranger Here"
- The small town sheriff would translate into the airport's explicit security. Other characters, such as the mayor and teachers could translate into other functions. In the "Milagro Beanfield War" there is "the guy with the pig", Pacheco. In the themed airport this could translate into traveler ambassadors.

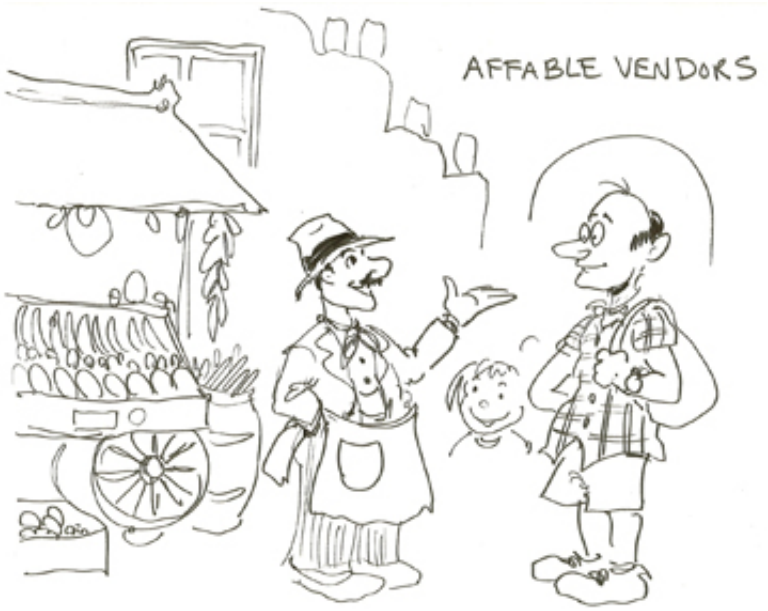

Figure 25 - Affable Vendors **Illustration by Tim Kirk**

- Shops in the airport could look like the general store and small street vendors.
- The entrance road to the airport could be made to appear like a winding rural road. This could provide opportunities for slowing down vehicles and separating out large commercial vehicles.
- At the ticket counter travelers could be enrolled into the "local community". For a brief period of time the traveler would be represented in the local census and the local newspaper. The newspaper would be continuously changing electronic dialog where the story of the airport is continuously changing and updating depending upon who is at the airport.
- Work areas could be provided that would be equivalent to the business areas of a small town. Similarly, family areas and areas for children could be made to appear like a small town park.
- A saloon theme could be used for the bars.

The "Ritz-Carlton" Airport

An airport experience in which passengers are willing to provide information about themselves in exchange for highly personalized service was explored. Ritz-Carlton pays attention to customer habits down to fine details, such as the music stations to which they tune, in order to make the customer feel special and the room feel like home. Amazon greets its customers with books they should find of interest. Lands' End maintains a virtual model of its customers and allows them to see new clothes on a body like their own. This model depends upon people's willingness to give up privacy for service or other benefits.

A travel experience on this model might include all aspects of a trip. The customer might share his or her entire itinerary, including purpose, flights, meetings, lodgings, transportation, hosts, and colleagues. The customer could be pre-screened for security, verified by biometrics. The traveler might have a profile of preferences and might also indicate preferences unique to the trip (e.g., I'd like to catch a Cubs came while I'm in town, hear some good jazz, and have a cheese steak). The traveler's luggage could make its own way to his or her room. If flight or meeting schedules change, the entire itinerary could be adjusted automatically in accordance with user-defined preferences. Travelers could order food and drinks in advance for the flight, for the layover, and for room service upon arrival. An optimal path through the airport to one's next flight could be available on PDA or cell phone, taking the traveler by the bathroom, the T-1 internet connection, the newsstand and the ice cream shop, and reminding them to check in with the office.

Docents could be available to guide people through foreign airports. Docents would be trained to observe suspicious behavior and know what to do about it.

Thus the traveler reveals preferences, tendencies, and current agenda and this history can be accumulated. A traveler's current behavior can then be compared against preferences, agenda, and history for anomaly detection. A person deviating from their agenda or their tendencies could attract more scrutiny—for both service and security reasons (e.g., are you lost or are you up to something?).

Environments that are personalized often inspire a sense of ownership in clientele. This is evident in the milieu in the frequent-traveler club lounges in contrast with the waiting areas for the general public.

This approach need not be an "elite" service, like Ritz Carlton, available only to those who can afford it. It can be a Lands' End or Amazon version. Providing a service that optimizes a traveler's layover results in increased revenue (the ice cream cone and the novel you buy) for the airport, which means that the airport vendors might be willing to pay for it. A service that juggles a traveler's entire agenda has control of the providers (transportation, food, hotel, etc.) you use and can negotiate bargain rates and/or commissions from these vendors. Travelers may be willing to open their wallets more for exactly the food, entertainment, and connectivity they request.

Concerns about classism and prejudicial treatment with this model were high during group discussions. There were also liability concerns if security elements are privatized in this model (if Acme Travel lets the terrorist through, is Acme liable for the damage?).

Session 8: Concepts for Securing Other Public Places

The final design session of the Fest was an attempt to apply what we had learned (about creating an environment in which the good guys feel safe and will be vigilant while the bad guys will feel exposed and deterred) to discuss the design of other public places.

Malls

The Malls group worked on ways to apply these ideas to shopping malls. For many reasons, malls are seen as very high on the list of potential *soft* targets for terrorists. They are highly symbolic of our consumer-oriented culture, have high concentrations of people, are visited regularly by a significant percentage of the population, and have high importance to our economy. Malls are different than mass transit in that they are privately owned, with private security (police usually only as off-site responders). Malls are also more heterogeneous in activity than airports; there are so many different activities that take place in malls that picking out something "abnormal" is much harder. While chemical or biological attacks are a possibility, explosives are the weapon of greatest concern. It would even be possible to buy ingredients and manufacture an improvised explosive device (IED) inside the mall using the restroom as a working area. Hence even a highly effective entry screen would not eliminate the threat.

There are several technological systems that could help improve mall security. People could be forced through rotating doors to get in the mall; this confined area could be a good place to put sensors to analyze for explosives and other threats. More cameras could be implemented and made overt to provide both increased surveillance and to make everyone, both potential perpetrators and the public, aware that the area is monitored. There could be more phones or means of communicating tips (such as a cell phone #77 system) to security in malls. This should be accompanied by a visible presence of uniformed security and a sense that concerns reported will be investigated. Here there is a difficult trade-off between conveying a general message to be on the lookout for suspicious behavior and being on the lookout for "terrorism". Terrorism-messages inspire fear and their effectiveness is unknown. There is also the difficult issue of how to engender vigilance and awareness without bringing up stereotypes of terrorists in people's minds? Awareness training must stress events such as the Oklahoma City bombing and the fact that it was McVeigh, a white, Christian, Gulf War hero who carried it out, not a Muslim. There was also the observation that there has been a drop-off of volunteerism in America in the past 10-20 years, raising the question of how we can expect to get volunteers for security. In summary, malls are and will always be difficult to secure. It seems that the public will be a key player in this effort. If we can increase the awareness of public safety and plan security systems that utilize the public, it will further deter terrorists and create more secure public spaces.

Sports Venues

The group was not optimistic about protecting these spaces. The simple scenario to worry about is the suicide bomber who walks in the gate, sits down, and detonates. Surveillance for such an operation would be very difficult to detect. Therefore, there doesn't seem to be much that the crowd at a game can do.

The JMP (Judy Mobile Portal) concept is highly applicable to sports venues. It could provide the service of avoiding traffic, keep crowds and vehicles apart (thus reducing vehicle-borne-bomb threats), and it could sniff and sense the crowd on their way to the game.

Food security could also be significantly improved at sporting events to prevent a food-borne bio-attack (or an accidental food-borne epidemic).

Having tickets matched with positive identification could provide a deterrent and would certainly help with forensics. Such a system could immediately identify a person out of place.

Most important in the suicide bomber scenario would be to interrupt these operations in the planning stages.

Subways

Subways are very different from airports. They are very open systems, with multiple entrances and exits, even to an individual station. New York City subways move over a million people a day. Staying on schedule is of the utmost importance for a subway. Operators want to be on time as much as passengers and they cannot subject people to long security screening times. Over the course of a month, subways can have many different groups of people riding a specific subway car at a specific time each day. There are already some subways with barrier-free stations – no ticket gates – just a conductor collecting tickets. New tunnels are very expensive and retrofitting old tunnels with new hardware is very expensive.

Overt security elements include guards (guns, gas masks, etc.), dogs, CCTV, sensors, etc. CCTV – displays could be shown to all riders (and people offsite who "log in" as "diligence volunteers") via Jumbotrons on the platforms and flat panel displays in subway cars. Trusted traveler smart cards that attach personal information to travelers and tracks their movements in the system - could be combined with CCTV image recognition. CCTV that recognizes patterns of abnormal and suspicious behavior would be very desirable. Wireless cameras could be located in the coaches. Sensors for explosives (and other items of concern) could be integrated into entrances, station platforms, and coaches. Decision making should be automated but with humans in the loop.

Methods need to be developed to "screen" without significant delay (while on stairs, escalators, passing through gates, etc.). One car could be dedicated in each train to those riders with luggage. Blast-resistant train cars and tunnels (venting concepts) need to be developed. Methods to automatically decouple train cars are needed as are diversion tunnels for train cars in case of emergency. Besides explosives other attack methods must be addressed (including chemical, biological, radiological and cyber).

Training of all employees of the system to recognize abnormalities is very important. The awareness level of employees should be increased, and then public awareness should be raised. Training must be refreshed frequently, and updated with new, current information – "awareness" is a perishable skill. First-responders are trained to stand back and evaluate before charging in (they do not want to be a "blue canary" by rushing in and dying to signal something is wrong to their colleagues). Better technology to assess critical situations and facilitate immediate decisions is highly desirable. Dogs, police with automatic weapons, and a demonstration of response power will have a deterrent effect. One goal is to achieve the perception of comprehensive security. Overt security will be needed especially following an attack to clearly demonstrate security to the public.

Communications access is needed for all travelers (not just one or two intercoms per train car) for both emergency and non-emergency calls (911 and 811). Multiple means of communication from

the public to the authorities for tips are needed: cell phones, courtesy land line phones, push-to-talk radio hubs, etc.

Public awareness programs are important. Public tips must be taken seriously when they are received. The public must know their tips are investigated or they will be discouraged from reporting more. Officials must respond rapidly and professionally if an alert occurs. It may be possible to build a transient sense of community among the riders and the employees (Familiar Stranger concept). Diligence messages can help: “Don’t just sit there with your iPOD blasting away and ignore everything around you”. We want people to notice immediately if someone leaves a bag behind and remind the person before they are gone. If they deny it is theirs or run, concern sky-rockets. By comparison, buses seem to have more sense of community than subways (a lot of the same people on same bus, at the same time of day; usually they are neighbors; one car instead of multiple cars). Homeless people are good informants on the subway system (they see everything; they can foster a good relationship cheaply with civil treatment towards them from officials).

Amusement Park Complexes

The demographics of people who visit amusement parks are very different than those of the airport. Amusement parks target very specific market segments. Families and groups of teenagers are the main users while individual adults are the exception. People also remain in amusement parks much longer than in airports, ranging from a few hours up to a few days. Because of these demographics amusement parks offer special opportunities to identify those who do not belong.

Large concentrated crowds provide special security concerns from terrorism. Visiting an amusement park is an optional activity. If there were ever to be a problem at a park, the economic consequences could be immediate and devastating since people could simply choose to stop going. There are fewer drivers for visiting an amusement park than there are for traveling. Even though there may be problems on the subway, people will probably still continue to use subways since it is a necessity.

A generic amusement park complex has the structure shown in figure 27. Typically there are very few public entrances; the public and the staff do not enter together, vehicle access is limited to only service vehicles; and there may be some special type of entrance for individuals staying at hotels associated with the park.

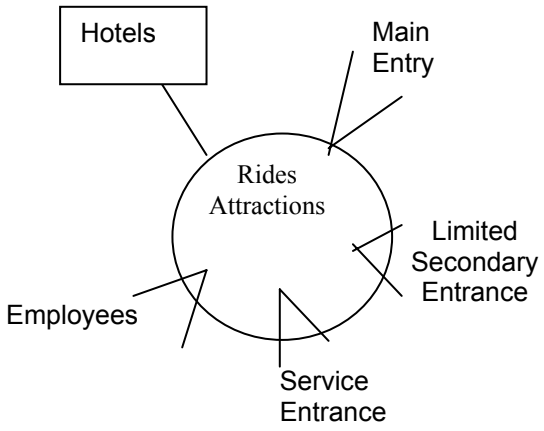

Figure 26 - Conceptual Layout for Amusement Complexes

Since individuals are at the park for entertainment, their sense of security vigilance is reduced. Parks strive to foster a high trust environment. This is interesting since often the rides at the park try to create a sense of fear but within well controlled, trusted parameters. There is a concern that once security awareness levels are raised, it would be hard to retain the high-trust environment necessary for the successful operation of the park. "Communitas", rather than a real community, is the best we can do.

Security concerns at parks are much wider than just terrorism. Theft, kidnapping, and pedophilia are all also concerns at parks.

The following are some ideas that were discussed for amusement park security:

- RFID tags on guests.
- Photos – take photos of guests throughout their visit to the park (maybe tied to an RFID tag) and then offer them a photo album of their experience at the end of the day. This will make it very obvious to an adversary that they are being watched.
- Screening at gates – limit bags, coolers, etc.
- Support for guests awareness, emergency notification.
- Customer service!
- Have explicit security.

One of the best skill-sets this country has is marketing and influencing human behavior. This skill should be utilized in increasing security, increasing awareness and building community.

The Art of Freedom Campaign

Marshall Monroe, Tim Kirk and Diane Velasco were asked to create overnight a presentation synthesizing some of what was discussed into a conceptual level idea with another level of detail. They created and pitched a concept for an educational campaign called the Art of Freedom, which could inform the public about homeland security. They argued that homeland security has a Yin and Yang feel to it with overt security as the Yin and our sense of community as the Yang. The uniting theme of this campaign is that we are all Americans and we are in this struggle together. They felt that Crime Stoppers was a good model and could be a basis for this campaign.

Figure 27 - The Pitch for the Art of Freedom

The concept pitched was a modular, collapsible "building" that contains a multimedia exhibit and could be placed in the Albuquerque Sunport initially, with a national deployment later. This would

be a campaign of information dissemination with a coordinated multi-media effort. The information would come from government agencies in consultation with professional marketers handling the message transmission. It would involve merchandise, physical exhibits, and media events and use down-to-earth subject matter experts with lots of experience to communicate a message face-to-face. The display would be aimed at children but with appeal to adults.

Concepts for of this exhibit presented and/or discussed were:

- Meet Ben Franklin who would guide you through a freedom gallery of the country, reminding us that freedom isn't free and must be bought with sacrifice. It would also remind us of E Pluribus Unum with more electronic media reflecting the diversity and dreams of the country. We discussed the need to talk about American ideals at a high enough level so that we don't get into our divisions and differences. We also need to be sensitive to foreign visitors, making sure the message is not xenophobic.
- View a video presentation from "Officer Gil", which is kept very current, on security information which should encourage everyone to be aware, not scared.
- Visit a panorama theater, with Ben Franklin narrating the start of a series of panoramic shots of the natural beauty of the country.
- Children would get a Freedom Pin at the beginning of the tour which lights up unexpectedly and begins blinking with a hidden internal LED as they exit.
- Exhibit could include activities and be distributed throughout the airport. Ideas for this included:
    - A picture or movable picture of a room for participants to pick out what's wrong (e.g. a package sitting by itself near the door).
    - Ben Franklin telling you to get your boarding pass and ID ready, to drop-off your lighters and matches in the bin, etc., before you enter the security checkpoint.
    - Show Ben Franklin going through security, with the hassles of him taking out his 18th century laptop and cell phone.
    - Show him on CCTVs in the JMP buses.
    - Have him at the baggage claim at the end of the trip reminding us of the Art of Freedom.
    - Videos on airplanes before/after the safety-belt briefing.
    - Video testimonial kiosks where people can go and give a short story to the camera that can later be included in the exhibit.
    - Hometown kiosks, where you scan your passport or boarding pass and a picture or map of, - or something about - your hometown pops up and encourages conversation with other travelers.

Ben Franklin was chosen because he was known as a great community organizer, a renaissance man, a man of science, a patriot, and an internationalist. However one could also use a few former Presidents to deliver the message, with Franklin as "host".

There will be a need to keep these exhibits fresh, with new and up-to-date information. The production role could be distributed, and contributions from students, the public and famous artists could be solicited, with the contributions reviewed by a board and the winners put in the next month's exhibits (could be done partially on a local level to give exhibits a local flavor). There will also need to be a balance so that it is informative and fun for those willing to participate but not annoying or a hassle for those who do not. It also seemed that this should be a joint venture, supported by business, government, and academia.

This should be designed so that in an emergency it could be used as a public address system.

The exhibit in the airport should really be a part of a greater campaign that could be deployed in malls, schools, and other public spaces.

Session 9: What Have We Learned?

We now began to collect from all participants what they thought we had learned in this event. This was done by a written brainstorm where participants wrote on boards around the room giving their input in fourteen categories.

1. What were the best ideas about physical environments?
2. What were the best ideas about communications?
3. What were the best technology ideas?
4. What were the best processes in public places?
5. What were the best ideas for the role of overt security?
6. What were the best ideas generated about negatively impacting the bad guys?
7. What changes in people behavior will be needed for success?
8. What will be the social and policy barriers to success?
9. What technology still needs development?
10. What will be the positive impacts on society?
11. What will be the negative impacts on society?
12. Can you identify some good opportunities for implementation?
13. How might implementation begin?
14. Any other lessons learned?

1. Best Ideas about Physical Environments

- Design buildings for security
  - More cameras and automated processing
  - Weight/size comparator for inbound vehicles
  - Barrier to stop speeding 18 wheeler
- Distributing security:
  - Fast pass for security that you can download when you check in online
  - Screening done at remote sites and/or in transit to airport hub
  - Combine “smart cards” with CCTV systems
  - J.M.P.!!!
- Create environments that promote people watching
  - Create intimate environments for loitering – no comfy place to be anonymous
  - Decentralized screens and communication bays
  - Flexible/modular installations
  - The transparent portal screeners allowing viewing of those being screened
  - Layered open/funnel/open/funnel design, curved benches with blast-proof walls or backs

2. Best Ideas about Communications

- Need for anyone to be able to quickly report concerns:
  - Lots of phones plus an easy way to report concerns; e.g. “#77”
  - Mood ring
  - Make it easy for public to report, even if not sure/”non-event” (e.g. “I’m uncomfortable”)
- Remind us to be vigilant and how to do that
  - Dynamic (digital) signage for multiple messages (security, commerce, community engagement)
  - Variability in messages to travelers
  - Maintain awareness/attention
- Use cell phone, PDA, instant messaging technologies to bring people back to here and now – instant message each other and then meet, pictures right here, or at destination, etc.
- Friendly interviewers at a kiosk

- Using modern marketing campaign to communicate back to public
    - Communications must involve/include public news media. Work cooperatively and collaboratively.
        - Art of Freedom

3. Best Technology Ideas:

- Sensing:
    - Put sensors on boarding passes
    - Sensor/info integration – cameras, tickets, sensors, mood rings
    - J.M.P.!!!
    - Determination of intent
    - Explosives detection at a distance
    - Sniffers installed in passage areas: revolving door, escalators…
    - Automated systems that compare vehicle weight to vehicle size, and alert security to vehicles that appear very heavy for their size (and could be vehicle bombs)
    - "Intelligent" CCTV systems (especially when linked to other sensor/detection systems)
- Communications:
    - The mood ring – I share my discomfort, it's aggregated with the feelings of others near by
    - Familiar strangers – people vouching for people
- Systems:
    - Computer vision technology with human oversight
    - Mixture/integration of personal/portable devices and "fixed"/embedded devices
    - Multiple threat coverage

4. Best processes in public places

- Increasing interaction of people to form temporary communities or "communitas"
- "Randomize"
- Filtering passengers (the light travelers from those with lots of luggage, etc.)
- Matching people to flights to vehicles – knowing who is coming, who is here, why
- The friendly "aware" parking garage that does security, safety, service all in one – tells you where an open space is, whether your car is still secure, etc.
- Responsive people/systems to report suspicious behavior
    - encourage people to express discomfort
    - no action unless significant numbers are uncomfortable
- Resident working population in soft target is transformed into part-time undercover security/sensor force
    - training employees to create a better sense of a close community that can protect itself
- Mixing security and service
    - Provide services to help people get where they want to go (PDA that can find a T-1 line, an ice cream cone, a taxi) that tells us your destination and intent
    - Greeters/ambassadors to engage passengers and spot abnormalities
    - Friendly trained interviewers like at the Brussels Airport
- Fast pass for security
- Need to engage Muslim community as a part of the greater national/international community against terrorism/violence
    - Think global – act local

5. Best Ideas for Overt security

- Security visibility
    - Cameras everywhere
    - Clear view of drills and training (protect/respond mode)

    - Glass allowing public to see security surveillance
    - "tip of iceberg" uncertainty with respect to overt/covert mix
    - Friendly but obvious
- Separate people and their bags
- Separate vehicles from crowds
- Dual use systems – safety, security, service
- Deceptive and dynamic defenses
    - More dogs – including "decoy dogs" (cheap implementation)
- Security forces actively engaging folks (ambassador style)
- Surveillance tunnels
- RF tag/boarding passes that can be tracked while in terminal

6. Best Ideas for making the bad guys feel exposed

- General:
    - Dynamic security: never the same → advertise this as a virtue
    - Deceptive security: fake cameras, sensors, processes
    - Keep detection systems/processes unpredictable
    - Keep things fresh – layouts, "costumes" (employees wearing different hats), content (digital or static)
- Use of Technology:
    - Lots of cameras
    - Jumbotron
    - Honey pots on public websites, websites designed with surveillance in mind
    - Send people pictures of themselves "surveilling" or loitering
- Role of clearly marked, multi-level surveillance spaces, within the context of training and alert employees and customers
- People processes:
    - Buddy system checks – I talk to you; you talk to me
    - Ambassadors that engage in unexpected conversation with the public
    - "No one is a stranger here" (we are all vigilant)
    - Kiosk interviews (Israel, Brussels…)
    - Place-based games where lots of people are looking around

7. What changes in behavior will be needed for success?

- Take an active role in detection – feel empowered to be an active part of security
    - Greater attentiveness, engagement, responsibility
    - Willingness to pick up phone or approach security officer with concerns
    - Authorities respecting/respectful of all call ins
        - Layers of response to calls
    - Accept responsibility for self
    - Willingness to relinquish some measure of our anonymity and privacy, particularly in public spaces
- Education/awareness programs that reinforce change required
    - Better understanding of vigilance vs. vigilantism
    - Accept terrorism as part of life, and adapt to deal with technology and human awareness and action
    - Public understanding of "risk" and acceptance of managing it (not eliminating it)
- More trust (means government has to engender trust)
- Public safety/dual use
    - training of employees to communicate and create sense of community for customers/passengers, having activities that will increase passenger contact and ability to react to intrusion

8. What will be the social and policy barriers to success?

- Trying to establish a new social contract finding the right balance (if there is one) between feeling safe and being vigilant
- Privacy/trust
    - Concerns about privacy – not trusting authorities with private information
    - Concern over profiling, exclusivity
    - Increased fear and racism
- Need for better articulation of relationship between freedom, privacy and anonymity
- Unions for workers may reject the role of ambassador if they perceive the worker has accountability for errors as a result of that person's work
- Social – "not my problem"
    - "leave it to the professionals"
    - Alertness fatigue
    - Efficiency/busyness/rushing though life
    - Apathy
- Misuse by people
- Policy – "what are we trying to achieve and why?"
- Lack of resources, especially money - Who pays?
- Lack of public understanding of risk, risk management

9. What technology still needs development?

- Integrated sensors
- Really intelligent CCTV systems that can detect events/behaviors/actions/people of concern
    - Disposable sensing technology (that is reliable)
    - Computer vision and AI (reasoning) technology
- Smart boarding passes
- Smart travel card – passports are passé
- Detection at a distance
    - Explosives and integrated information system
    - Bio-metrics diversity - standoff biometric needed
    - Non-cooperative, touch less biometric(s) ID
    - Nearly instantaneous sniffers so that people can be trapped in areas like revolving doors
    - Intention meter
- Transport with sensors
- False alarm and information filtering techniques to keep security pros from info overload
- Mood ring
- Human management of massive data

10. What will be the positive impacts on society?

- Greater public safety (terrorism = crime)
- Increased sense of national/international community of people against terrorism (violence) and real actions coming from the community
    - Greater social capital
    - More communications
- More confidence and peace of mind
- Sense of control
- Education with a purpose → motivation to learn
- Enhanced sense/reminder of personal responsibility
- Community enhanced/in this together
    - Sense of teamwork
- Citizenship/responsibility
- Information/education can create community

11. What will be negative impacts on society?

- Any process that slows down process flows will have negative economic impact – "terrorized" society
- Change in behaviors such that folks don't go to revenue-producing venues – major negative impact on economy
- False positives
- Always "fearful" of the worst
- Nation of "informers" is a terrible idea
- Less privacy and trust
- Loss of trust that is at the root of many of our social and economic transactions
- Increased profiling and racism
- Loss of privacy if too many cameras
- "One more thing…"
- Our best efforts are not enough
- Over-exposure to message dilutes its impact
    - Could initially create atmosphere of concern – then be ignored
- Threat awareness could increase authoritarianism and sanctions

12. Good Opportunities for Implementation

- Multi-faceted campaign – art of freedom
    - Venues, content, contributors, audience
    - Make use of TV venues to get word out to public
    - Contextualized displays
- Schools – visits by "officer Gil" and some appropriate deputies
- J.M.P. to facilitate distribution of people and strip VBIED's from crowds
- Find a willing/witting partner to help implement
- Fast security portal in Gardunos (airport restaurant)
- Any idea that can generate a revenue stream
- Services that help me get what I want when I telegraph my goals, destination (ON Star on steroids)
- Mall bathroom control
- Facilitated discussions around the country
- Physical design concepts could be implemented at little cost in all malls and airports

13. How might implementation begin?

- Develop/demonstrate some of the discussed technologies
    - With a means to evaluate impact
    - Pilot at some location
    - Determine the objective – pilot to see if objective can be met. If not, what is needed?
- New high visibility "experience" at Albuquerque Airport
- Ad campaign to announce launch of program and it's goals
- In-depth study about situations where people are routinely vigilant but feel safe (e.g., driving)
    - Evaluation requires specifying meaning of threat, vigilance, awareness
    - Computer simulation (use of models)
- Modest local funding paid for by vendors and increased revenues produced by improving public space

14. Any other lessons learned?

- No silver bullet: technology and authorities and citizens should work together
- Best security when whole community involved
- Best if security also enhances/improves safety/other operational objectives
- Look at multi-use/benefit concepts that tie terrorism vigilance/awareness to safety (accidents, health problems, crime) in public places.

- Layered defenses are always best
- The public is usually more vigilant when community is formed at least situationally
- Key idea: reduce crowds/density
- Technological solutions are seen as more productive and possible than physical design or people solutions. This approach might be short sighted. But training of people and changing a culture requires time and a consistent message.

Session 10: What Deserves More Exploration?

The final session was a large group discussion about what we need to do with the ideas generated here. In many cases people volunteered to be a part of these next steps and a few have already started. Here are the suggestions:

The JMP technology should be pursued

- This could be demonstrated at the Albuquerque Airport using common shuttle buses from the rental car facility
- Sandia National Laboratories' explosives portal developers should be engaged
- Industry has strong development in CCTV and sensors. Suggested partners were:
  - A4 Vision for vision recognition
  - Honeywell for enhanced scene awareness

Conduct a follow-on workshop that might

- Cover other public venues/places
- Involve more operators and implementers who might explore concepts and develop implementation strategies
- Try this again with new participants, give them this information, and let them use it to figure out a way to implement
- International version of this using a presentation from this group's findings to present at an International FOILFest
- Consider having a communications component including working with the media in effective ways

Sandbox for social experiments/activities to see how folks would react to these concepts

- "Neighborhood Watch" studies? – Look at the literature that is already out there!!!
- Exercise people in real places
- Ethnographic studies
- Likely university hosted – suggested University partners:
  - University of Colorado
  - Georgia Tech

Idea of aesthetically pleasing, blast-resistance seating areas

- Using Lexan
- Possible partners:
  - Architect in Battery Park area doing something similar to this
  - New Mexico Tech
  - Corps of Engineers

The Art of Freedom

- Start local
- Build to a national level

Appendix 1: List of Participants

Name	Title/Affiliation	Email	Phone
David Brin	Consultant	dbrin@sbcglobal.net	760-436-5649
Khai Truong	Interrelativity Inc.	khai.truong@gmail..com	678-458-1602
Marshall Monroe	Marshall Monroe Magic	MM@marshallmonroemagic.com	505-797-0300
Jim Hinde	Sunport/City of ABQ, Aviation Dept	Jhinde@cabq.gov	505-244-7805
Lance McKinney	Sunport Operations Manager	lmckinney@cabq.gov	505-244-7859
Lawrence Modisett	US Naval War College	modisetl@nwc.navy.mil	401-841-4057
Joseph McCarthy (Joe)	Interrelativity Inc.	joe@interrelativity.net	425-301-1802
Kathy Domenici	Domenici Littlejohn Inc.	kdomenici@comcast.net	505-246-4755
Bradd C. Hayes	US Naval War College	hayesb@nwc.navy.mil	401-841-2021
Eric Paulos	Berkeley - Intel Research	eric@paulos.net or paulos@intel-research.net	415-699-7558
Jane McGonigal	Berkeley & 42 Entertainment	janemcg@berkeley.edu or jane@4orty2wo.com	510-847-0035
Andrew Fano	Accenture Technology Labs	andrew.e.fano@accenture.com	312-693-6606
George Andler	DHS (TSA-ABQ Deputy FSD)	george.andler@dhs.gov	505-246-4104
Larry Morgan	DHS	larry.morgan@dhs.gov	202-254-5828
Robert Sauer	DHS	Robert.Sauer@dhs.gov	703-235-5716
Fred Ambrose	CIA	bigfoote@aol.com or fredaz@ucia.gov	703-874-1003
Donna Caccamise	U Colorado @ Boulder	donnac@psych.colorado.edu	303-735-3602
Robert Hertan	SFMTA	Robert.Hertan@sfmta.com	415-554-7115
Tim Kirk	Kirk Design Inc.	lindantim@charter.net	562-595-1569
Setha M. Low	CUNY	slow@gc.cuny.edu	631-329-7348
Steve Clemons	New America Foundation	clemons@newamerica.net	202-986-0342
Clark McCauley	Bryn Mawr College	cmccaule@psych.upenn.edu	610-526-5017
Mike Bazakos	Honeywell	mike.bazakos@honeywell.com	612-951-7852
Diane Velasco	Journalist?	Diane__Velasco@hotmail.com	505-890-0570
Bert Useem	UNM	useem@unm.edu	505-277-4269
Mike Maness	Abraxas Corp	mmaness@abraxascorp.com	703-821-3775
Bill McMath	FBI / JTTP Coordinator	wpmcmath@leo.gov	505-889-1568
Gerry Yonas	SNL	gyonas@sandia.gov	505-845-9820
Tommy Woodall	SNL	tdwooda@sandia.gov	505-844-7541
Jessica Turnley	Galisteo Consulting	jgturnley@aol.com	505-889-3927
John Cummings	SNL	jccummi@sandia.gov	505-845-9937
Annie Sobel	SNL	sobel@groupvelocity.com	505-844-1411
Wendell Jones	SNL	wbjones@sandia.gov	505-284-9403
Bruce Held	SNL	ebheld@sandia.gov	505-284-5404
Mark Grubelich	SNL	mcgrube@sandia.gov	505-844-9052
Nancy Hayden	SNL	nkhayde@sandia.gov	505-845-9634
Ron Stoltz	SNL	restolt@sandia.gov	505-294-2162
Judy Moore	SNL	jhmoore@sandia.gov	505-845-9415
Darryl Drayer	SNL	dddraye@sandia.gov	505-844-8479
Curtis Johnson	SNL	cjohnso@sandia.gov	505-844-8683
John Whitley	SNL	jbwhitl@sandia.gov	505-845-9763
Lindsay Dvorak	SNL	ldvorak@sandia.gov	505-284-1561
Andrew (Drew) Walter	SNL	awalter@sandia.gov	505-284-0340

Appendix 2: The Agenda

July 18-21, 2005
Sandia National Laboratories
Albuquerque, NM
Building 880/A49

Tuesday July 19

Welcome

7:30 **Bus departs from Sheraton Hotel**
8:00 **Badge Office for Badging**
8:30 **Continental Breakfast**
9:00 **Introduction of the sessions and processes for the Fest** Gameroom

Session 1: Environment for Citizens

9:30 **Written brainstorm** Big White Boards

Explore what features in public places will make people feel safe and be vigilant, in these 4 categories:

- Physical Environment - Layout, Architecture and Design
- Technology & Communications Infrastructure
- Processes and People's Behavior
- Role of Overt Security

10:15 **Small group refinements:**

- Physical Environment - Layout, Architecture and Design BMT
- Technology & Communications Infrastructure Front Gameroom
- Processes and People's Behavior Back Gameroom
- Role of Overt Security Gerry's Office

Session 2: Environment for Adversaries

11:15 **Written brainstorm** Big White Boards

Explore what features in public places will make potential perpetrators feel exposed and convinced they will not succeed, in these 4 categories:

- Physical Environment - Layout, Architecture and Design
- Technology & Communications Infrastructure
- Processes and People's Behavior
- Role of Overt Security

Session 3: Small Group Synthesis & Reports

12:00 **Small group synthesis** of the two perspectives - citizen and adversary (and lunch too!)

- Physical Environment - Layout, Architecture and Design BMT
- Technology & Communications Infrastructure Front Gameroom
- Processes and People's Behavior Back Gameroom
- Role of Overt Security Gerry's Office

1:15 **Reports** Gameroom

Reports from each group in a plenary session will bring the group to a common understanding of the features required for our environments.

Session 4: Plenary Synthesis

2:15 **Journaling Exercise** Gameroom
2:45 **Group discussion** Gameroom

Session 5: Apply Our Ideas To A Real Space

3:30 **Short briefing about the Albuquerque Sunport** Gameroom

Divide into 4 teams with these different perspectives:

- Rental cars, information desk, transportation - (shuttles, taxis .etc.)
- Parking and passenger pickup and drop-off
- Ticketing check in and baggage claim
- Shops/food and meet/greet area

4:00 **Depart for Airport**
4:30 **Observations** Sunport

Meet in the lobby area on ticketing level and then divide into teams to observe the current space that represents their team's perspective (with escort from airport).

5:30 **Dinner and team discussions** Garduno's Restaurant

Albuquerque Sunport
7:30 **Bus departs airport for hotel**

Wednesday July 20

7:30 **Bus departs from Sheraton Hotel**
8:00 **Continental Breakfast** Gameroom

Session 6 - Develop a Vision for the Sunport

8:30 **Design**
The 4 teams will generate a vision for their area of observation about what might be done to the Sunport, based on the principles of creating an environment in which the good guys feel safe and will be vigilant while the bad guys will feel exposed and deterred. They will report their results to the plenary, describing possible changes to the physical layout, architecture and design, technology & communications infrastructure, processes and people's behavior, and the role of overt security.

- Rental cars, information desk, ground transportation — Gerry's Office
- Parking and passenger pickup and drop-off — Back Gameroom
- Ticketing check in and baggage claim — Front Gameroom
- Shops/food and meet/greet area — BMT

9:30 **Reports** Gameroom

Session 7: Develop A Vision For Future Airports

10:30 **Design** (and lunch too!)

Four new teams will apply what they have learned so far about creating an environment in which the good guys feel safe and will be vigilant while the bad guys will feel exposed and deterred to design an airport of the future if they were starting from scratch. The four groups will focus on the design of an airport of the future in which:

- It's like a subway - fast, no loitering — Front Gameroom
- There are maximum offsite operations — Gerry's Office
- A "theme" airport — BMT
- "Ritz Carlton" airport ("happy traveler"; trade privacy for service) — Back Gameroom

1:00 **Reports and discussion** Gameroom

Session 8: Develop Concepts For Securing Other Public Places

2:00 **Design**

Four new teams will apply what they have learned about creating an environment in which the good guys feel safe and will be vigilant while the bad guys will feel exposed and deterred to discuss the design of other public places. The four groups will focus on:

- Malls — Front Gameroom
- Subways — Gerry's Office
- Sport venues — Back Gameroom
- Amusement park complexes — BMT

4:00 Reports Gameroom

5:00 Bus departs for hotel

Thursday July 21

Sandia Laboratories, Building 880, Room A49

7:30 **Bus and luggage van depart Sheraton Hotel**
8:00 **Continental Breakfast** Gameroom
8:30 **Presentations and discussion of advanced geospatial concepts for airport of the future**

Session 9: What Have We Learned?

9:30 Written brainstorm Gameroom

1. What were the best ideas about physical environments?
2. What were the best ideas about communications?
3. What were the best technology ideas?
4. What were the best processes in public places?
5. What were the best ideas for the role of overt security?
6. What were the best ideas generated about negatively impacting the bad guys?
7. What changes in people behavior will be needed for success?
8. What will be the social and policy barriers to success?
9. What technology still needs development?
10. What will be the positive impacts on society?
11. What will be the negative impacts on society?
12. Can you identify some good opportunities for implementation?
13. How might implementation begin?
14. Any other lessons learned?

10:00 Discussion **Gameroom**

Session 10: What Deserves More Exploration?

11:00 Discussion of suggested next steps **(and lunch too!)** Gameroom

12:00 Bus departs for airport and hotel