Using common sense to effectively integrate security technologies within a school’s security strategy

Mary W. Green
Sandia National Laboratories, MS 0762, P.O. Box 5800
Albuquerque, New Mexico 87185

ABSTRACT
Security technologies are not the answer to all school security problems. However, they can be an excellent tool for school administrators and security personnel when incorporated into a total security strategy involving personnel, procedures, and facility layout. Unfortunately, very few of the tougher security problems in schools have solutions that are affordable, effective, and acceptable. Like any other type of facility, a school’s security staff must understand the strengths and limitations of the security measures they are considering. It is imperative that the design for new schools incorporate good security practices, which will rarely increase new building costs if included in the initial planning.

1. INTRODUCTION
Because of the 1997 and 1998 tragedies involving the shooting deaths of students by other students, U.S. schools and school programs are working hard to reach out to students, to teach them to be good citizens, and to identify potentially lethal personalities. There are many excellent programs around the country that have been developed for precisely that, including programs that address the issues of bullying, anger, hate, drugs, alcohol, abuse, gangs, lack of role model, vandalism, etc. It is of great importance to the U.S. that these programs be pursued most expeditiously. Unfortunately, these programs cannot be successful overnight (indeed, many must be initiated early in a child’s life in order to be most effective) and do not yet exist in all schools. Meanwhile, security incidents are occurring in schools that must be dealt with now – perpetrators must be caught and consequences must be administered. Best case, a school would like to discourage security infractions by means of any deterrence available to them. One such approach being sought more often today is security technologies.

Security technologies are NOT the answer to all school security problems. However, many security products (e.g., cameras, metal detectors, drug-testing kits, sensors, etc.) can be an excellent tool when applied appropriately. They can provide school administrators or security officials with information that would not be otherwise available, free-up manpower for more appropriate work, or be used to perform mundane tasks. Sometimes they can save a school money when compared to the long-term cost of personnel or the cost impact of not preventing a particular incident. Too often in schools, though, these technologies are either not applied appropriately, are expected to do more than they are capable of, or are not well-maintained after initial installation. When this is the case, technologies are way over-priced.

2. WHY MANY SCHOOLS DO NOT USE SECURITY TECHNOLOGIES
Anyone working in the security field is aware that there are literally thousands of products on the market, some of them excellent, but each claiming to be “the very best of its kind”. And, unfortunately, there are a significant number of customers in the country who have been less than pleased with the ultimate cost, maintenance requirements, and effectiveness of security technologies they have purchased. Schools have been no exception to this, and also have a few inherent problems of their own:

- Schools do not usually have the funding for aggressive and complete security programs;
- Schools generally have to select the “lowest-bid” for procuring products and services;
- Many school security programs must rely on staff who earn minimum wage, which makes it difficult to hold onto well-trained people;
- School administrators rarely have training or experience in security technologies;
- Schools have no infrastructures in place for maintaining or upgrading security devices -- when something breaks, it is often difficult to have it repaired or replaced;
- Issues of privacy and civil rights lawsuits have created an obstacle course for school administrators attempting to keep their student body as safe as possible.
DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.
DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.
The issues come down to applying security technologies in schools where effective, affordable, and politically acceptable, but still within these difficult constraints.

3. EFFECTIVENESS VS. AFFORDABILITY VS. ACCEPTABILITY

A particular school security problem would cease to be a concern rather quickly if there existed a solution that was completely effective, affordable by the school environment, and politically acceptable among the community. However, this is generally not the case (i.e., “if it were cheap and easy, somebody would have already done it”).

Occasionally, a seemingly ineffective solution to a security problem is chosen, because of lack of funding or political pressures, but the deterrence of just doing something keeps the effort from being entirely wasted. People are not dumb, though, and deterrence with no detection or consequences will quickly deteriorate.

Many effective security measures are too expensive for schools, due to manpower and/or hardware costs. Often, though, cost is not the ultimate driver. Politics can and do kill many physical security initiatives in schools. Some common arguments against physical security initiatives are:

- “we’ve never done it that way before”
- “this is a knee-jerk reaction”
- “our school will look like a prison”
- “students’ rights may be infringed upon”
- “people will think we have a bad school”, and
- “we may be sued.”

A more proactive approach would be better served by counter-arguments such as:

- “we need to evolve our security strategies to keep up with the changing times”,
- “this solution will take care of the immediate threat while longer-term social programs are put into place”,
- “our school will look like it is well under control”,
- “students will live long enough to enjoy their rights”,
- “we will gain the reputation for controlling our problems”, and
- “we may be sued if we don’t take this act on”.

This is not to say that a good argument should be made for applying every physical security approach in every school. Appropriate is by far the greater “art” in security system design, and is comprised of an evolving plan, beginning with defining a particular school’s risks.

4. IDENTIFYING EACH SCHOOL’S RISKS

In the past, schools have rarely had the time or resources to consider their security plan from a system’s perspective -- looking at the big picture of what they are trying to achieve in order to arrive at the optimal security strategy. Like any other type of facility, a school’s security staff must understand WHAT it is they are trying to protect (its people or high-value assets), WHO they are trying to protect against (the threats), and the general environment that they must work within -- the CHARACTERIZATION of the facility. Only then can a facility design its optimal security strategy that operates within its financial, logistical, and political constraints. This strategy will likely include some combination of technologies, personnel, and procedures, and also do the best possible job of solving its problems within its financial, logistical, and political constraints.

No two schools are alike, and therefore, there is no single approach to security that will work the best for all schools. Even from year to year, a school’s security strategy will need revision, because the world around it and the people inside it will always be changing.

Why is this careful identification of risk important? Because few facilities in this world, and especially schools, can possibly afford a security program that protects against all likely or unlikely incidents.

Characterizing a school’s environment: Any security strategy must incorporate the constraints of the facility, so that strengths, weaknesses, and idiosyncrasies are all realized and provided for. Is the school new or old? Are the windows
particularly vulnerable? Does everyone who ever worked at the school still have keys? How many entry points are there into the buildings? Are gangs present in the area? Are the school grounds open and accessible to anyone or do fences or buildings restrict access? Is there easy access to the school roof? Where are hiding places within the building or on the premises? What is the nighttime lighting like? Is the school small enough so that most of the staff know most of the students and parents? What is the crime rate in the neighborhood? Does the interior intrusion sensor system work well or do the local police ignore the alarms due to a high false-alarm rate? Is the school administration well-liked by the students? Are teachers allowed access to the school at night? Are students allowed off campus at lunch time? How much spending money do your students generally have? Are popular hang-outs for young people close by, and does their management collaborate with the school? Are expelled or suspended students sent home or to an alternative school? How many incidents of violence have occurred at the school over the last four years? What is the general reputation of the school and how does it appear to an outsider? Are visitoIs forced to go through the front office before accessing the rest of the school? What is the “in” dress? How much does the athletic program influence the rest of the student body? Are your most vocal parents pro-security or pro-privacy?

Defining a school’s assets: For this school year, what is most at risk? The protection of the students and staff is always at the top of this list, but the measures taken to protect them will usually be driven by the defined threats. Are the instruments in the band hall a very attractive target for theft or vandalism? Is the new computer lab full of the best and most easily resold PCs? While desirable, a school cannot possibly afford to protect everything to the same level of confidence.

Defining a school’s threats: For this school year, who or what is your school threatened by? Gang rivalries? Fights behind the gym? Drugs hidden in lockers? Guns brought to school? Outsiders on campus? Drinking at lunch time? Vehicle break-ins? Graffiti in the bathrooms? Accidents in the parking lot? How sophisticated (knowledgeable of their task of malevolence) or motivated (willing to risk being caught or risk being injured) do the perpetrators seem to be? Measures taken to protect against these threats are driven by the characterization of the facility and its surroundings as mentioned earlier.

Identifying security needs and then having the funding to pay for them are usually uncorrelated at most schools. Schools have to have a “Plan B”, which may be the perfect “Plan A” spread out over several years of implementation. If the resulting desirable strategies (e.g., fencing, sensors, locker searches, speed bumps) are too costly or are unpalatable to the community, a school may then need to modify the facility constraints (e.g., back entrances locked from the outside, no open campus for students, no teacher access after 10:00 p.m., all computer equipment bolted down, no lockers for students, etc.). Most school districts or school boards will be more supportive of security measures and requested funding if they are well-educated as to the most-likely risks faced each year vs. the options available. A security staff should not have the wide-open charter of “keep everything and everybody safe”. A school board should be briefed often as to what the current security goals are and what strategies are recommended, realizing that these will and must continue to evolve. If a school board member is clearly aware of a school’s most important concerns and what is required to achieve them, then he or she is less likely to be swayed by an irate parent into making a decision that will handicap reasonable security efforts.

5. DESIGNING THE SCHOOL SECURITY SYSTEM

After identifying the risks or concerns at non-educational facilities, a methodical approach to the security plan would then examine possible solutions to each vulnerability from the perspective of

\[
\text{Detection} \quad \longrightarrow \quad \text{Delay} \quad \longrightarrow \quad \text{Response}
\]

For any problem, it is necessary first to detect that an incident or problem is occurring. For example, when someone is breaking into a building, it is necessary that this act be detected and that information be supplied to the authorities as soon as possible. Next, this adversary must be delayed as long as possible so that the response force may arrive. A simple example of delay would be firmly attaching computer components onto large, heavy desks, such as with bolts, so that a thief is forced to waste time in removing the bolts. Lastly, someone must respond to the incident, such as the police force.

For a school environment, it is probably more appropriate to expand this model:

\[
\text{Deterrence} \quad \longrightarrow \quad \text{Detection} \quad \longrightarrow \quad \text{Delay} \quad \longrightarrow \quad \text{Response/Investigation} \quad \longrightarrow \quad \text{Consequences}
\]
The most appealing step in any school security system should be to convince the perpetrator that he shouldn’t do whatever it is he is considering, whether the action is perceived as too difficult, not worth his while, or the chances of being caught are quite high. Clearly, most security measures employed in most facilities are intended for the precise purpose of deterrence, whether it be to discourage a thief, a drug dealer, or an errant employee. Often, however, deterrence comes “free” with other security measures and it would be difficult to attribute any lack of security problems directly to any particular deterrence.

Unlike other facilities, where a perpetrator would be handed over to the authorities to deal with and the consequences are determined by law, a school often has the authority and/or opportunity to establish the consequences for some incidents that occur on their campus. Indeed, these consequences can oftentimes be the deterrence needed to prevent incidents. If a school enforced the policy that any student caught with alcohol on campus will ALWAYS have to pull weeds on the athletic field for the next two days immediately after school, students may be deterred from this particular act in the future.

To illustrate the application of this model, consider the concern over vehicle break-ins in the student parking lot. A model for the security strategy to address this might be:

**Deterrence**  
Close off the parking lot to vehicle traffic during the school day. (Make students with irregular schedules park in a separate area.) Post signs that video cameras are being used. Have a campus aide located at the parking lot whenever possible.

**Detection**  
Install video cameras (vandal-resistant) in the parking lot. Send the video signal to a recorder for one-week archival.

**Delay**  
Install 8’ fencing around the outer regions of the parking lot, so that a perpetrator would be forced to climb over this fence with stolen merchandise.

**Response/Investigation**  
Review tapes. Confront perpetrator with evidence (if a student). Call authorities.

**Consequences**  
Enforce maximum consequences where possible. (This becomes additional deterrence for future.)

Few schools have the opportunity for real-time detection and real-time response to incidents -- after-the-fact reaction is normally the best a school can hope for.

This model is not appropriate for all aspects of security, and in most cases, it can serve only as a methodology for consideration. However, its use can prevent some less-thought-out strategies. A couple years ago, one large high school located in a busy downtown area was planning to purchase $100,000 worth of exterior cameras to combat nighttime vandalism being inflicted on the exterior of the building. This plan halted abruptly when the school realized no one would be available to watch the monitors from the 40+ cameras (detection) and be able to respond quickly enough to these sporadic and relatively-small incidents (response). A better and cheaper alternate plan was devised that included anti-graffiti sealer on all brick surfaces, some strategically-located wrought-iron fencing that could not be easily climbed, and the replacement of a few particularly vulnerable windows with glass block.

6. A SPECTRUM OF PHYSICAL SECURITY APPROACHES

It will be assumed that consequences for undesirable actions have been put into place at a school, otherwise, there is no deterrence to be gained from physical security measures designed to detect, delay, and respond to an incident. A wide array of security measures involving people and/or technologies can be considered for most concerns, keeping in mind the “personality” of each particular school. It should also be noted that almost all schools feel that the majority of their problems are brought onto campus by outsiders or expelled/suspended students, so that measures to keep outsiders off campus will generally be of global benefit. The following is a partial list of possible security measures for various security issues, and includes procedural and personnel approaches as well as technologies.

**Outsiders on campus**  
Enclosing campus (fencing), guard at main entry gate to campus, adult greeters in strategic locations on campus, students ID’s or badges, vehicle parking stickers, uniforms or specific dress codes, exterior doors locked from the outside
during the school day, a challenge procedure for anyone found out of class, cameras in remote locations, school laid out so all visitors must pass through front office, temporary “fading” badges issued to all visitors

**Fights on campus**
Cameras, duress alarms, whistles

**Vandalism**
Graffiti-resistant sealers, glass-break sensors, esthetically-pleasing wall murals, law enforcement officers living in trailers on campus, 8-foot fencing

**Drugs**
Drug “swipes”, hair-analysis kits (for parents), drug dogs, no lockers, drug-detection kits, random “pat-downs”

**Alcohol**
No open campus, breathalyzer test kits, no access to vehicles, no lockers, clear or open mesh back packs

**Weapons**
Portal meal detectors, hand-held metal detectors, vapor detection of gun powder, “hot-line” for info with rewards, gunpowder “swipes”, random “pat-downs”, random locker and vehicle searches, x-ray inspection of book bags and purses

**Teacher safety**
Duress alarms, roving patrols, classroom doors left open, cameras in black boxes in classrooms, controlled access to classroom area

**Theft**
Interior intrusion detection sensors, property marking to deter theft (including microdots), bars on windows, reinforced doors, cameras, doors with hinge pins on secure side, bolting computers and TVs down, locating high-value assets in interior rooms, key control, biometric entry into rooms with high-value assets, law enforcement officer living on campus

**Parking lot problems**
Cameras, parking decals, fencing, card swipe for auto entry, parking lots sectioned off, sensors in parking areas that have no access during school day, roving guards

**False fire alarms**
Sophisticated alarm systems that allow assessment of alarms before they become audible, “screamer” boxes installed over alarm pulls, purple “pixie powder” that stains hands

**Bomb threats**
Caller ID, crimestopper program with BIG rewards for informant, recording of all callers, all incoming calls routed through a district office, phone company support, no pay phones on campus, policy to extend the school year when plagued with bomb threat evacuations

**Bus problems**
Cameras in black boxes, IDs to get on school bus, security aides on buses, smaller buses, duress alarm for driver

**Terrorism**
Set-back of all school buildings from vehicle access, or reinforce structural walls that are most at risk, inaccessible air intake and water source, no line-of-sight from off campus, all adults on campus required to have a badge, vehicle barriers near main entries and gathering areas
7. USING COMMON SENSE TO EXAMINE THE APPROPRIATENESS OF A SECURITY UPGRADE

The effectiveness, and hence success, of any new security technology can be difficult to foretell before it is actually put into operation. Every school is different, every student population is different, and every community is different. A common-sense examination of the proposed security measure can help to maximize the success of the new hardware, as well as any changes to security personnel or procedures. The responsible personnel need to critically question themselves as to the desired goals, potential vulnerabilities, costs, operational constraints, and long-term requirements of the approach under consideration. The following are examples of questions that the security personnel should be able to provide satisfactory answers to before equipment is purchased or major changes are made.

◊ Do you know of other schools or facilities who have used this equipment to successfully address a similar problem? Will your implementation be of comparable size (both in amount of equipment and in area to be applied over)?
◊ Will the equipment be vulnerable to attack? For example, will cameras be accessible to someone who can get on the roof? Are your ceilings so low that a tall student could vandalize a motion sensor? Will the equipment be vulnerable to extreme weather?
◊ Will the equipment operate as desired on unusual days? For example, will the intrusion detection alarm system fail to be set on a holiday? Will teachers who use the school facility late at night set off the alarm system?
◊ Will the personnel overseeing the equipment learn its vulnerabilities and then be able to use these to their advantage?
◊ Will the amount of time and manpower required to use this equipment allow for normal school operation? For example, will you have enough metal detector portals to be able to scan each student at 5 seconds per student and still get everybody to class on time?
◊ Will the kind of information this technology provides be of reasonable benefit? For example, if a camera views a school entry with the goal of keeping outsiders off campus, is there anyone to watch the video real time and then to respond to a potential intruder?
◊ Will students/employees/outsiders be able to easily figure out the weaknesses of the security technology? For example, will anyone be aware that the cameras in the parking lot can only adequately view the first four rows of cars with enough resolution to identify an individual?
◊ If you are considering a new intrusion detection alarm system, will the sensors be appropriate for each location? Example problems could be caused by heat sensors that view a piece of equipment that may suddenly heat up, motion sensors in a hallway where posters may flap when the air conditioning comes on, etc.
◊ Is there someone to respond in a timely manner to incidents that are detected? How long will it take your security personnel or local law enforcement to show up if an alarm is generated?
◊ Do you have the support of your school principal and school board in the new change? Do school policies need to be changed in order to keep the school out of trouble?
◊ Does the use of the new technology introduce any potential liabilities to the school?
◊ Who will oversee the daily operation of the equipment and/or check that the equipment is operating properly? Who will see that the equipment gets repaired if it breaks? Can your facility then function adequately without the equipment for the amount of time it will be out? Will funding be available to repair or even to replace the equipment when needed?
◊ Who will train new operators on the equipment after the initial training by the vendor? How much time and/or experience does it take for a new operator to become proficient? Does the use of this equipment require someone fairly specialized and will that person be difficult to replace?

3. NEW SCHOOL DESIGN

Many of the existing school buildings in this country were built 15 to 45 years ago. The goals of the popular designs during this time was to achieve an inviting and open-to-the-community feeling, with multiple buildings, big windows, multiple entrances and exits, and lots of opportunities for privacy. Needless to say, these layouts are not conducive to many of today’s requirements to address security needs. To combat broken windows, the country also went through a brief period of designing schools with almost no windows some 15 or 20 years ago, however the cave-like result these designs produced was found to be objectionable to most people.

If a district has the luxury of looking forward to a new school in the future, IT IS IMPERATIVE that security personnel who are familiar with the area and the community, and who will be responsible for day-to-day security operations in the new facility, are involved in every step of the new design. This is critical to ensure that the design of the new school minimizes vulnerabilities. Some architectural firms specializing in schools are starting to incorporate good security principles, which can actually compensate in the long-term for tight security budgets, fewer security personnel, and less sophisticated security “gadgets.” The following are some suggestions to keep in mind for a new facility; the funding, location, geography, streets, and neighborhood will usually drive which ideas are possible for each new school. While this list includes only a few basic
technologies, the facility design should not preclude the straightforward installation of security technologies if required in the future.

◊ Limit the number of buildings – one building is best if it is not possible to keep all outsiders off the campus.
◊ Minimize the entrances to the school building – having one or two main entrances/exits will support efforts to keep outsiders off campus. Allow for enough room at the main entry in case a “screening area” (i.e., weapon or drug detection) needs to be incorporated later on. Alarm other exits for emergency use only.
◊ Allow for a security person to be posted at a single entrance onto campus to challenge each vehicle for identification of all occupants. Buses and school employees should have a separate and controlled entrance.
◊ Provide a drop-off/pick-up lane just for buses.
◊ Minimize the driveways or parking lots that students will have to walk across to get to the school building.
◊ Build single-stall bathrooms, to mitigate bathroom confrontations and problems.
◊ Enclose the campus. (This is more a measure to keep outsiders out rather than keep insiders in.) While an attractive wrought iron fence is ideal, a more-affordable option is an 8’ chain link fence with small 1” to 1-1/2” mesh. This height is difficult to pull up on and the smaller mesh does not allow “toeholds”. Besides defining property boundaries, a robust fence forces a perpetrator to consciously repress, rather than allowing idle wandering onto a campus that has no fencing.
◊ Make certain that the school can be closed and locked off from the gym and other facilities used during off-hours.
◊ Minimize secluded niches (i.e., hiding places) both inside and outside the building.
◊ Do not eliminate windows, but use them strategically (i.e., narrow windows that an adult cannot fit through). Consider incorporating glass block that allows in light but is less vulnerable than typical glazing.
◊ Maximize line-of-sight within the building.
◊ Minimize line-of-sight from off campus onto gathering areas, the main entry doors, playgrounds, patios, etc.
◊ Install student lockers in classrooms, so that there is no single locker area that becomes a bottleneck, and there is always the deterrence of a teacher nearby.
◊ Do not cut corners on communications, especially those required for security. Make certain that your facility has built in necessary receivers and transmitters throughout the structure to allow for dependable two-way radio use and cellular phones. (Too often, RF communications are not possible within the “bowels” of a large facility.)
◊ Where possible, have buildings and other student gathering areas set back from the street or other potential parking areas by at least 50 feet. (This is to mitigate the effects of a “car bomb”.)
◊ Have at least a basic security alarm system installed throughout all hallways, administrative offices, and in all rooms containing high-value property, such as computers, VCRs, shop equipment, laboratory supplies, and musical instruments.
◊ Allow a sworn law enforcement officer to live on campus. (Generally, the officer is allowed to move his own trailer to a strategic location on campus, and then receives free utilities in exchange for a few pre-negotiated responsibilities.) The deterrence of a police vehicle parked on campus all night and weekend can be terrific. Also, this can provide for both detection and response to situations where damage is being inflicted upon the facility, but no alarm system will normally detect it.
◊ Provide a separate parking area for work-study students or those who will be leaving during the school day. (This allows the main student parking lot to be closed off during the school day.)
◊ Make certain that exterior lighting is sufficient for safety – lights mounted to the exterior of buildings are generally inadequate for evening events.
◊ Do not underestimate the value of trees and landscaping on a school campus. An attractive, well-cared for school is generally less-attractive to thieves.

9. THE ROLE OF ORDER MAINTENANCE

One additional consideration that cannot be overlooked is the perception of chaos on a school campus. If a school is perceived as unsafe (i.e., it appears that no adult authority prevails on a campus), then “undesirables” will come in and the school will become unsafe. It is the embodiment of the “Broken Window Theory” -- one broken window left unrepaired will cause additional windows to be broken. Seemingly small incidents or issues such as litter on a school campus can combine to provide the groundwork (or even just the reputation) of a problem school. Issues of vandalism and theft can be almost as harmful to a school as actual violence -- they can create a fertile environment for loss of control.
Therefore, issues contributing to an overall order maintenance must be taken seriously. Reducing theft, deterring vandalism and graffiti, keeping outsiders off campus, keeping the facility in good repair, getting rid of trash, maintaining attractive landscaping, and improving poor lighting are all paramount to a school. Technologies such as cameras, sensors, microdots (for identifying ownership), and anti-graffiti methods can contribute significantly in many school situations (but not always!), and are possible approaches to support a school’s order maintenance.

Note: Too often school districts undervalue the ultimate importance of a reliable and conscientious maintenance, janitorial, and grounds-keeping staff. Their ultimate contribution to the order maintenance of a school can be terrific. Additionally, the janitorial staff needs to be selected with almost the same care as the teaching staff – these people have great accessibility and knowledge of a school facility. Contracting out this work without complete background checks of all workers can lead to many problems in the long run.

10. CONCLUSION

School security is not straightforward. Because of the financial, logistical, and political constraints that most schools must operate within, achieving an optimal security strategy can often be much more difficult for a school compared to a business or government facility. Careful planning in advance, whereby security personnel examine their goals and the ramification of various approaches, can help a school achieve the most effective and politically-acceptable solutions possible within their budgetary limitations.

11. ACKNOWLEDGEMENTS

This paper is a synopsis of a portion of the information that will be provided within the upcoming manual, The Appropriate and Effective Use of Security Technologies in U.S. Schools. This guide for schools and law enforcement agencies is being funded by the National Institute of Justice, Office of Science and Technology. Publication and distribution is expected in early 1999.

Sandia is a multi-program laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.