BEST PRACTICES FOR SCHOOL SAFETY AND SECURITY

December 2004
“Working toward a safer New York.”
-Governor George E. Pataki

This document was created through a collaborative effort by:

New York State
Office of Homeland Security
Director James W. McMahon

University of the State of New York
State Education Department
Commissioner Richard P. Mills

New York State Police
Superintendent Wayne E. Bennett

State Emergency Management Office
Director James W. Tuffey
FOR OFFICIAL USE ONLY

This document is for official use only. Unauthorized disclosure beyond your organization is prohibited without prior written approval from the New York State Office of Homeland Security and the New York State Board of Education.
<table>
<thead>
<tr>
<th>Page</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Letter from Lieutenant Governor Mary O. Donohue</td>
</tr>
<tr>
<td>2</td>
<td>Introduction</td>
</tr>
<tr>
<td>4</td>
<td>General Best Practices</td>
</tr>
<tr>
<td></td>
<td>S.A.V.E. Mandated Practices</td>
</tr>
<tr>
<td></td>
<td>Short-Term Practices</td>
</tr>
<tr>
<td></td>
<td>Long-Term Practices</td>
</tr>
<tr>
<td>13</td>
<td>Topic Specific Precursors and Indicators</td>
</tr>
<tr>
<td></td>
<td>Criminal Behavior</td>
</tr>
<tr>
<td></td>
<td>Recognizing a Gang Presence</td>
</tr>
<tr>
<td></td>
<td>Sexual Crimes and Child Exploitation</td>
</tr>
<tr>
<td></td>
<td>Internet Safety</td>
</tr>
<tr>
<td></td>
<td>Arson – Juvenile Fire Setting</td>
</tr>
<tr>
<td></td>
<td>Anthrax Exposure - Protocols for Mail Handling</td>
</tr>
<tr>
<td></td>
<td>Bomb Threats</td>
</tr>
<tr>
<td>32</td>
<td>Appendix</td>
</tr>
</tbody>
</table>
Mary O. Donohue  
Lieutenant Governor

To: District Superintendent of Schools  
   Superintendents of the Big 5 City School Districts  
   Superintendents of Public and Non-public Schools  
   Charter School Administrators

The Safe Schools Against Violence in Education Legislation (S.A.V.E.) was fully enacted in 2000. This comprehensive 17-point legislative action placed a number of requirements on school systems to ensure the safety of students and faculty. With the start of another school year and recent world events it is imperative that a comprehensive review of security plans and protocols be reviewed by all parties of interest.

The New York State Office of Homeland Security, the New York State Police, the New York State Education Department and the New York State Emergency Management Office have collaborated with the Federal Department of Homeland Security and several New York State School District Superintendents to provide insight, tools, guidance and direction to allow each school to enhance school safety and security plans.

This document addresses potential security concerns and provides an overview of best practice strategies and methodologies that have been implemented with successful results. The delineated strategies should not be strictly construed, as they may be modified as appropriate to suit any particular location. Additionally provided in this document are suggested courses of action that may be individually implemented as deemed prudent by each respective authority.

The course of action identifies short and long-term objectives. The short-term objectives are easily implemented at nominal cost and should be established as a building block foundation on which to add the long-term objectives to ensure a structured and sound, comprehensive program.

Review and evaluation of current safety and security protocols should be performed at the earliest opportunity with any future modifications and implementation conducted in partnership with your appropriate police department or law enforcement agency.

Sincerely,

Mary O. Donohue  
Lieutenant Governor

Office Of The Lieutenant Governor  
State Capitol  
Albany 12224
Introduction

This document has been devised to assist in developing an enhanced comprehensive safety and security program. Implementing the objectives within this program will form the foundation of a comprehensive safety and security strategy.

A number of security-related best practices, that have achieved significant and successful results, have been compiled and categorized in easily referenced fields. They are provided as potential tools and strategies for your use and by no means should be considered “end alls.” They may be utilized by themselves or with other strategies as you deem prudent. It should be understood that circumstances might require the use of additional strategies beyond those illustrated in this document.

The course of action to complete this safety and security strategy includes, but is not limited to, the following objectives:

**Short-Term**

- An awareness program for administrators, faculty, staff, students and family members through the explanation of precursors and indicators of potential terrorist and potential criminal behavior, article reviews, discussion and video highlights. The targeted or highlighted crimes include sexual crimes and child exploitation, arson, identifying a gang presence, general criminal behavior that may forecast specific crimes such as terrorism, and Internet and cyber safety for children, young adults, and school facilities.

- Regional seminars with administrators and faculty to discuss safety and security issues including, but not limited to the best practices of:
  - Physical Security and Access Control
  - Visitor ID Programs
  - After-Hour Security
  - Technological Remedies
  - Telephone Protocols
  - Mailroom Protocols
  - School Bus Identification and Tracking Methods
  - Drills.

- Vulnerability and risk assessments of every school followed with recommendations.

- Annual report and review in collaboration with primary police departments within each Counter-Terrorism Zone.
Long-Term

- Establishing additional school security assessments and reports through legislative action.

- Developing trained personnel capable of risk and vulnerability assessments and implementation of additional security strategies.

- Scheduling different types of security drills and tabletop exercises with law enforcement, fire, emergency medical services, and other emergency support services followed by critiques.

- Publishing articles on multi-hazard emergency preparedness, safety and security in school newsletters and other relevant periodicals or journals.
General Best Practices

The best practices provided in this document are a compilation of strategies that have achieved significant and successful results when used by some school districts in New York State. They are provided as potential tools for your use and by no means should be considered “end alls.” It is important as you go through the planning and updating stages in your school, to take a look at and learn from what others in your position have done so as to not re-invent the wheel, and most importantly, learn from the mistakes and good ideas of others.

The Best Practices have been split into three categories: S.A.V.E. (Safe Schools Against Violence in Education) Mandated, Short-term and Long-term Practices.

S.A.V.E. Mandated Practices are legislatively required but are worth repeating for the purposes of emphasis. Short-term Practices are strategies that can be implemented relatively quickly and with very little effort. Long-term Practices may take somewhat longer to implement because of fiscal constraints, and contractual or a host of other logistical reasons affecting necessary acquisitions. Although they may be more difficult to implement, they should not be prematurely discounted. Again, these practices may be utilized, as you deem prudent in concert or not at all with other implemented strategies.

S.A.V.E. Mandated Practices

- Individual comprehensive school safety and security plans for each building should be maintained within each school district-wide School Safety Plan.

- Each facility’s Emergency Response Plan and Safety and Security Strategy should be on file with the law enforcement and fire agencies in its region.

- Establish a clear notification process.

- Delineate clear roles of responsibility in specific emergency situations and chain of command. (Incident Command System instructional courses are available through the New York State Police and the State Emergency Management Office. (See Appendix Page 42.)

- Building schematics, blueprints, photos, and school emergency plans should be provided, if not developed with, police to allow for a tactical emergency response.
• All companies contracted by the school should provide a list of all employees to have background checks, including fingerprints conducted for any employee that will have personal contact with students or school staff ($99 cost). The school may assist in this venture through local law enforcement.

• Establish Emergency Response Teams (“E” Teams, Crisis Teams, etc.). Emergency Response Teams comprised of faculty and custodial staff should be developed. Team members should be chosen as leaders that will step up should a hazardous or emergency situation arise. As this is a voluntary role, some faculty or custodial staff often feel for a variety of reasons that they are “not the right person” to take charge in a stressful or emergency situation. As such, team member positions should be carefully chosen with scrutiny. Once individuals have been identified, teams should be structured on the capability of the individual, not necessarily their status or credentials. These groups should then be trained with specific responsibilities and teamed accordingly with backup plans. These teams can then be tasked to respond to specific emergencies contingent with their training. Additionally, either within these teams or separately, (school) “wing leaders” should be established with each wing leader provided with a master key or master access to all points within the school. This ensures easy and timely access in an emergent situation.

  **Short-Term Practices**

• Practice all aspects of your School Safety Plan. Keep in mind that natural and man-made incidents occur so be sure that you practice for, and your plan includes, a “multi-hazard approach.”

• All school districts should have some type of a lock-door policy in each school building. Only one door in the building should be unlocked and monitored at all times until school closes for the evening or weekend. Access at this supervised entrance should structurally and physically impede a visitor’s entrance into the main portion of the school.

• Your student handbook should address a comprehensive safety and security policy that is read and signed off on by both students and parents at the beginning of each school year to ensure understanding and accountability.

• Each facility should compile, analyze, and assess the most probable local areas, facilities, transportation routes, and businesses that may have a potential impact on school or district
facilities during an emergency (i.e., rivers, electric sub-stations, nuclear plants, hospitals, rail lines, communication providers, state routes, etc.).

• Implement a clear student policy for awareness against the threat of vandalism, bomb scares, or other potentially coercive circumstances. The school's position that foreknowledge of any type of these potential circumstances or threats will be thoroughly investigated with a non-participant’s behavior and lack of action assessed and potential disciplinary action considered. A written acknowledgement from student's parents, parental guardian or person in a parental relationship of this and similar safety and security policies, often presented in student handbooks, should be enacted.

• As it relates to contractors or construction crews:
  a. All contractors and construction crews on school grounds during a threat or security-related incident should be directed to leave the premises.
  b. All deliveries during a threat or incident should be terminated, discontinued and postponed for another date.
  c. All contractors while on school grounds, either during school hours or otherwise, should be escorted at all times and bare some insignia or pass designated by the school.
  d. Construction sites on school grounds should be inspected daily by school custodial staff and documented.
  e. All deliveries to school facilities should be at pre-determined times.

• All schools should implement a visible identification card and pass system having different ID badges for staff, visitors and contractors. Visitor passes should be a different color every day, have the capability to change colors or have an altered appearance after issuance of a 24-hour period. Having different lanyards or holders for identification cards for each school facility is also recommended.

• All schools should establish relationships with commercial businesses in proximity of the school that are patronized by the student body (delis, hardware stores, electronics, etc.).
• All schools should establish an ongoing relationship with the media especially, with visual mediums (television and photographers).

• Gas shut-off valves and HVAC (Heating Ventilation Air Conditioning) controls in the school should be clearly labeled or color-coded preferably at a low level or on the floor. Photos of these should be included in the building level safety plan. Knowing when to initiate emergency shut-offs for various emergency related scenarios is imperative (hazardous materials: i.e. chlorine gas, fire explosion, etc.).

• All faculty should be aware of the predetermined evacuation locations for an emergency. During an evacuation, this site should be apprised of pending staff and student arrival.

• After school has commenced, the use of backpacks in halls or classrooms should not be allowed.

• Ensure that faculty and custodial staff receive initial and refresher training to effectively respond to an emergency.

• Ensure the school website is void of any sensitive safety or security related information such as building schematics, blueprints, diagrams, drill information, bus routes etc.

• Implement mutual aid agreements with other schools.

• Establish safe areas in different sections of the school.

• Ensure an adequate public address system is on school grounds, including but not limited to cafeterias, gymnasiums and outdoor recreational areas.

• Because of the structural uniqueness of school libraries and cafeterias, safety and security plans should be specifically developed for these areas.

• Ensure faculty, students and parents report suspicious activity to the Toll Free New York State TIPS line at 1-866-SAFE-NYS or within New York City at 1-888-NYC-SAFE.

• Individual school facilities should consider sharing psychiatric and counseling services, custodial services, or staff services contingent with contractual obligations.
• Individual parent-faculty meeting locations should be located in the front of the school within easy access to the supervised and monitored entrance, and scheduled with an appointment. Any parent/visitor meetings with faculty or guidance that cannot be physically located in the front of the school area, in proximity to administrative offices or in an area that structurally impedes access to the general student population of the schools including classrooms and hallways, should be managed with the use of an escort to the meeting location.

• All visits scheduled with an appointment or otherwise, should be announced with an escort to the appropriate location.

• Visitors picking up a student should wait at the front office and should not be allowed to walk through the school unescorted.

• External locks should be placed on roof hatches to allow emergency entry only if necessary.

• Locked exit doors leading out of the building should allow emergency services access capability (i.e. a lock that can be unlocked with a handle to be pulled open from the outside).

• The school’s main office should have a direct view of the front entrance and should be clearly marked as the main office.

• Label room numbers at a lower level on doors or walls next to the door and on rescue windows as well (in case of fire).

• One phone line and or cell phone should be unlisted and used only for outgoing calls during an emergency. In an emergency, the volume of incoming calls often hampers the use of the school phone lines.

• Duress alarms can be placed under a desk in the main office or on a person to signal an emergency.

• The implementation of some type of communication device, whether cellular phones with point-to-point capability or walkie-talkie style radios, should be initiated.

• The main phone lines servicing the school should have Caller-ID capability.

• A Bomb Threat Card should be placed under each phone in the school. It is used to record important information when receiving a
telephonic threat of any kind. The Bomb Threat Card can be downloaded from: http://www.troopers.state.ny.us/Publications/crime_Prevention/bombcard.pdf.

- Implementation of a computerized student database with student and faculty photographs, emergency contact information, cell phone numbers of students and their friends’ cell phone numbers.

- Assessment of potential computerization of phone tree information.

- Installation of panic and burglar alarms.

- Parking lots, playgrounds, and fields near school building should be easily observed and closely monitored.

- Installation of numerical identification on the roofs of school buses.

- Emergency Gotta Go Bags should be kept in two separate locations in each school building and also at the off-site evacuation location. (The Gotta Go Bag contents are listed in the Appendix on page 40.)

- Emergency equipment, supplies and rations in addition to the Gotta Go Bag for the following, should be maintained in adequate amounts:
  
a. Chicken nuggets or easily stored non-perishable foods
b. Ice cream
c. Water
d. Plastic tarp (sheeting)
e. Dolls, stuffed animals, board games
f. Videos
g. Laptop computer with Internet access
h. Cameras, film, batteries and flashlights
i. Portable generators and fuel
j. First aid supplies (including special needs for medical conditions such as asthma or diabetes etc.)
k. Potassium iodide (KI) for those schools located within the 10-mile Emergency Planning Zone (EPZ) of a nuclear power plant.

- Development of an electronic mass notification system for parents and faculty (cell phones, e-mail, pagers etc.).
• Development of additional faculty training days for safety and security education, training and drills.

• Implement an alert and notification system for responding emergency teams to provide response instructions while enroute (should be incorporated into the emergency response plan).

• Definitions and procedures for the following should be included in your plan and practiced:
  a. Lockdown
  b. Lockout
  c. Early dismissals
  d. Sheltering in place
  e. Evacuation
  f. Cancellation
  g. Missing children
  h. Hazardous material and School Science Lab Safety plan (i.e., chlorine gas, propane, etc.)
  i. Criminal action including terrorist attack (i.e., chemical-biological such as anthrax, smallpox, etc.)
  j. Natural disasters (floods, etc.)

*Note:* The development of additional plans should serve as an annex and build upon the existing emergency response plan. Emergency response plans should undergo a formal review and be updated at least annually.

• Implementing and ensuring that comprehensive critiques are conducted for all drills and incidents in collaboration with emergency services partners.

*For specific definitions, refer to the document, “NYS Homeland Security for Schools,” provided by NYS Division of State Police in April 2003*

**Long-Term Practices**

• Review and re-evaluate existing laws for potential gaps that may compromise safety and security strategies, i.e. public access of annual fire inspections.

• Legislation supporting annual security assessment and report coordinated through primary police departments within each Counter-Terrorism Zone.
• Support legislation to require schools to conduct drills for different parts of the plan semi-annually.

• Structure the main entry point to physically alter and impede school access while allowing for easy monitoring through the use of reception windows, glass walls, or view rooms coupled with electronic access systems.

• The use of bollards should be expanded to offset parking distances from key areas.

• Perimeter fencing should be expanded as necessary.

• The school telephone system should be assessed for potential upgrade including but not limited to public address capability from several areas within the school, caller-ID, call forwarding, and conference call capability.

• Video cameras should be installed at key access areas including the main doors and lobby, parking lots, playgrounds, fields, and delivery receiving areas.

• Install remote lockdown systems with the capability to allow activation from several key areas.

• Install radios or some communications capability on all school buses.

• Development of a portable computerized student database with student and faculty photographs, emergency contact information, and cell phones (including students and their friends cellular numbers).

• Development of a generator backup system that allows for convenient mobility to be coupled with redundant administrative and database systems (i.e. laptop, etc.).

• The implementation of communication devices, with point-to-point capability should be expanded, to ensure all teachers and staff district-wide have immediate contact and notification capability (police department included).

• Implement an electronically controlled access system.

• Development of safety and security plans for non-school hours.
• Implement staggered shifts for several faculty members to provide late school hour patrol of halls and grounds until the last student departs.

• Emergency equipment and supplies should be routinely maintained.

• Consider utilizing contractual agreements to include stipends for in-service training on emergency medical equipment, including defibrillators, etc.

• Consider utilizing retired law enforcement or private investigators for employment background checks of contractors or security personnel that could be coordinated through the Division of Criminal Justice Services.

• Implement an electronic mass notification system for parents and faculty (cell phones, e-mail, pagers etc.).

• Implementation of additional faculty training days (education, training and drills).

• Implement and ensure that a comprehensive review of all safety and security plans is conducted annually and in collaboration with emergency responders and submitted through the Counter-Terrorism Zone to the State Oversight Committee.

• Implement security for non-business hours including weekends.
Topic Specific Precursors and Indicators

The ultimate purpose for providing precursors and indicators of any crime or potentially hazardous situation facing the school environment is prevention. Crime prevention within a school setting begins with your realization that observations may be potentially symptomatic of specific types of dysfunctional or anti-social behavior. More knowledge of these indicators will lead to a higher probability for formal intervention.

It must be strongly emphasized that no single indicator may accurately predict criminal behavior. It does, however, indicate the need for further scrutiny. The time for ignoring symptoms is long past and our awareness for certain types of potentially dangerous behavior must be further heightened with all observations keenly scrutinized and appropriately reported. When in doubt of uncharacteristic or unusual student behavior, notification should be made to appropriate authority.

Precursors and Indicators of Potential Criminal Behavior

The following are general precursors and indicators of potential criminal activities. Alone, each indicator may result from legitimate recreational or commercial activities; however, multiple indicators combined with other information can be the prelude to a criminal act including terrorism.

- Physical surveillance that may include note taking or the use of binoculars, cameras, or maps near school locations.

- Attempts to gain information of school populations, individual students, dismissal times, the school calendar, security personnel or strategies, school bus routes, or school bus information through personal contact, by telephone, mail, or e-mail.

- Attempts to penetrate or test physical security and response procedures at school locations.

- Suspicious or improper attempts to acquire official vehicles, access cards, or identification.

- The presence of individuals who do not appear to belong in the workplace, business establishment, or school locations.

- Behavior that appears to denote planning for terrorist activity, such as mapping out routes, playing out scenarios, monitoring school locations, dismissal times and protocols or school bus routes.
• Unusual inquiries regarding school hours (arrival and dismissal times), pupil attendance or population, ethnic or religious composition of the student body, the presence of security measures in place (or lack thereof), etc. Also, inappropriate queries made by individuals who do not appear to be interested in registering their children.

• Reports of videotaping, or photographing, or making observations of the school building or activities.

• Individual(s) found in areas restricted to employees only, or not open to the general public.

• Suspicious behavior by an individual(s) attempting to enter a school wearing bulky clothing that appears inappropriate. This may be compounded by the subject being alone or acting excessively nervous and/or perspiring.

• Alarming or unusual statements made by a student regarding an approaching date.

• The parking of a suspicious vehicle in the school's parking lot or in proximity to the school building, particularly for an extended period of time.

• The loss or theft of any chemicals or hazardous substances located in school laboratories or storerooms.

• The discovery of an unattended package or object inside or around school buildings or grounds.

• The discovery of new marks or noticeable force of entry onto a school bus or unusual foreign item(s) attached to the bus.

• Registration of children into school not matching their presented documentation or without the necessary documentation including, but not limited to, birth certificates, immunization records, proof of residency, or social security cards.

Only approach or question a suspicious person if you feel comfortable. If you feel uncomfortable or threatened, seek assistance. Ask the person questions such as:

• May I help you with anything?
• May I see some identification?
• Who are you visiting?
• What is the purpose of your visit?

If the person refuses to answer or respond to your questions or does not answer the question to your satisfaction, attempt to escort them to a public area and notify your supervisor or manager. Avoid detaining or getting physical with the individual. Student and faculty safety is the priority. Make sure to note the individual's original location. Then, contact your local law enforcement. Focus on their behavior and physical characteristics and keep them in your sight until law enforcement arrives.

Your impressions and assessment based upon your professional experience are extremely valuable and should help guide you in determining if a customer request, a fact pattern or set of circumstances is unusual. Please remember that the conduct itself does not have to be criminal per se for you to report it to the NY State Toll-Free Tips line. It may be contacted 24-hours a day, seven days a week by calling: 1-866-SAFE-NYS or within NYC 1-888-NYC-SAFE.

Recognizing a Potential Gang Presence

The following are general indicators of potential gang presence or activities. Alone, each indicator may result from legitimate activities and explainable behavior. Multiple indicators should prompt further scrutiny and, combined with other information, suggest a possible gang presence.

• The presence of graffiti in the school, especially in bathrooms.

• Observance of small and unique social groups on school grounds (may be ethnic in nature as well as attire oriented, i.e., clothing color).

• Affinity for certain brands of clothing, jewelry, sports apparel, and coloring.

• Refusal to wear clothing of specific colors or brands.

• Hand signs.

• Gang language or slang used.

• Common tattoo among several individuals in a group.
Faculty should pay particular attention to the following activities that would warrant further scrutiny:

- Work being created during art or technology education classes such as figurines, caricatures, illustrations or insignias, and the use of specific colors that may signify gang activities.
- Decline in study habits.
- Reduced interest in scholastic activities for unexplained reasons.
- Presence of new friends.
- Ignoring usual friends.
- Interest in gangster rap (versus rap. Gangster rap glorifies the gangster lifestyle).
- Changes in dress habits.
- Unreasonable, and unexplained stages of defiance towards parents, teachers, or security personnel.
- Unusual lack of desire to complete schoolwork, along with staying out later than normally allowed.
- Change in vocabulary.

**Sexual Crimes and Child Exploitation**

The following are general indicators that, when observed, could warrant further scrutiny. They may signify a connection with sexual crimes and possible child exploitation. Alone, each indicator may result from legitimate activities and explainable behavior. Multiple indicators should prompt further scrutiny, especially when combined with other information.

- Apparent “interest” in children possibly demonstrated by a routine or habitual appearance in or around school grounds, without a legitimate reason.
- Vague or confusing explanations when confronted, and or asked for identification in or around school grounds, without having an apparent legitimate reason.
- Parents or individuals who inappropriately immerse themselves in school activities such as sports, PTA, and or field trips in an
apparent attempt or appearance to gain the trust of faculty, parents or other children.

- Attendance at after-school programs and or school sporting events without having a child, relative, or friend participating.

- Individuals photographing or videotaping school activities or grounds including playgrounds, gymnasiums, and parking lots without an apparent legitimate reason. (Pedophile studies indicate that they love to take pictures and videos and are the single most valued possessions in the world.)

- Individuals engaging children in prolonged conversation in an apparent attempt to learn as much about the child as possible.

**Internet Safety**

Online Child Exploitation - The Problem

The anonymity of the Internet provides opportunities to exploit the trust and threaten the safety of our children. Instructing our children on cyber safety techniques and cyber predator awareness is paramount for the Internet safety of our children.

- More than 45 million children were on-line in 2002.
- Thirty-two percent of 16 to 17 year olds are online for five or more hours a day.
- Pedophiles run more than 10,000 websites.
- Internet activity is implicated in nearly 20 percent of missing children age 15 to 17.
- One in five teenagers in the U.S. who use the Internet have received an unwanted sexual solicitation.
- Almost half of the sexual solicitations of children go unreported by the child (USDOJ).
- At the time of writing of this document, the following chat rooms are open and active on the Internet:

  younggirlsex    familysex
  preteensnuffsex childslavesex
  dad&daughtersex babysex
  littleboysex    littlegirlsex
  childrapetorturesex momdaughtersex
  preteenrapesex    child_dating
Cyber Security and Awareness for Schools

Cyber Security in the education community involves multiple components. These include the privacy and security of faculty, staff, and student information that entails personally identifiable health information, administrative information such as budgets, financial systems, confidential correspondence, and grades.

The following general guidelines provide a foundation to begin the development of a comprehensive Cyber Security Program.

Your user ID is your identification and is what links you to your actions on the system.

- Protect your user ID and password and change it periodically.
- NEVER tell or share your password with ANYONE and don’t write it down.
- Create a password that’s hard to guess but easy for you to remember.
- When your computer prompts you to save your password, click on “No.”
- If you think your password has been compromised, change it immediately and notify your information security officer or manager at your organization.
- Make your password as long as possible, eight or more characters.
- Don’t use passwords and IDs of former co-workers.
- Don’t reuse your previous passwords.
- Don’t use the same password for each of your accounts.

Work Station Protection

Properly safeguarding your personal computer is one of the most important methods of protecting your information from corruption or loss.

- Log off when you are away from your terminal or PC. In many cases hitting “Control-Alt-Delete” keys then “Lock Computer” will keep others out.
- If you have a modem, make sure it does not accept incoming calls (auto-answer should be off).
- When possible, remove your data before allowing your workstation equipment to be repaired off-site or replaced by an outside vendor. Consult with your manager on how best to do this.
Protecting your Information

The best way to protect information is to copy it and store it in a secure location.

- Information should be backed up and stored securely. Do not store your information on your PC’s “C: drive.”
- If not connected to a network, save your files to CDs or floppy disks regularly.
- If connected to a network, store your files in folders set aside for you. (Check with your LAN administrator for the schedule of backups.)
- Ensure that backups reflect the most current information by copying the data on a regular basis, as well as after significant changes. The frequency of the backup cycle should be appropriate to the frequency with which you modify the information.
- Use your original installation diskettes as the backup for your PC software.

Malicious Code Protection

Malicious code can take such forms as viruses, worms, and trojans, may hide behind an infected web page or disguise itself in a downloadable game, screen saver, or e-mail attachment. If you receive an e-mail with a suspected attachment or with a known virus:

- Contact the sender and inquire if they intended to send the attachment.
- Realize it is possible that the sender may not be the legitimate source. E-mail addresses can be faked by a technique called “spoofing,” leading the recipient to wrongly assume that the sender is at fault.

Computer Viruses

Computer viruses are programs that spread or self-replicate. They usually require interaction from someone in order to activate. The virus may arrive in an e-mail message as an attachment or be activated by simply opening a message. Viruses can exhibit many different symptoms.

- Check that your anti-virus software is updated every week or set it for automatic updates.
- Before you implement new or different software, check it for viruses with a current virus scanner.
- Store diskettes as "write protected" whenever possible by setting the write protect tab on the diskette.
• Be wary of loading free or non-licensed software on your business computer.
• Consider blocking extensions such as: .bat, .cmd, .com, .exe, .pif, .scr, or .zip through content filtering software.

Worms

Worms are similar to viruses because they self-replicate. However, they also self-activate spreading quickly across networks and the Internet. They do not require any user interaction to activate. Worms spread because of vulnerabilities or “holes” in software or by tricking people into activating them.

• Install either a software or hardware firewall. A well configured firewall can stop propagation of a worm.
• Anti-virus software will often detect worms. Keep your anti-virus software up-to-date.
• Know where to find your anti-virus vendor’s “rescue” website for your home computer.
• Keep your PC and servers “patched.”

Trojans

Trojans (backdoors) are illegal code hidden in a legitimate program that, when executed, performs some unauthorized activity or function. This can range from stealing your password and credit card information to enabling someone to take control of your computer. A denial-of-service (DOS) attack prevents an organization from providing its customers any services. It also prevents web pages from being available to customers. In some instances, a group of remotely controlled, compromised desktops are combined to jointly attack a target system. To prevent installation of trojans on your machine:

• Run anti-virus software on your desktop and follow the best practices for using it.
• Be cautious when downloading games, screensavers, and other files from unreliable Internet sources.
• Be careful about file and music sharing services such as Gnutella, Morpheus, Kazaa, and Bearshare.

Spyware

Spyware and related “adware” are software sometimes downloaded from a web page, an e-mail, or installed with freeware or shareware software without the user’s knowledge. Its purpose is to track your Internet activity, redirect your browser to certain websites or monitor sites you visit. Spyware may also record your passwords and personal information to send to a malicious website.
• Read the freeware and shareware license agreement to see if adware or spyware is mentioned before installing the software.
• Choose to “close” (x) any pop up windows that contain links to web pages.
• Do not answer any dialogue boxes that appear unexpectedly; click on “close” (x). Clicking on “No” or “Cancel” sometimes installs spyware.
• Beware of visiting web pages that you are unfamiliar with.
• Install software to detect spyware and adware on your PC.

Hoaxes

Hoaxes are e-mail messages that resemble chain letters, offer free money, contain dire warnings, and other incredible stories. If you receive one, delete it. Sharing hoaxes slows down mail servers and they may be a cover for a hidden virus.

Mobile Computing Security

Computers are now accessible via a variety of means. A person may even download data from the Internet to their cell phone. Further, laptops, PDAs and cell phones because of their compact size are more easily stolen or misplaced. If your laptop is gone, your data is as well. Small computer devices carry information that must be protected. Treat your portable devices carefully like a laptop and keep an eye on it. If you use a laptop, remember the following:

• Secure it with a cable lock or store it in a locked area or locked drawer.
• Backup your data.
• Encrypt confidential information stored on it.
• Keep it with you during air and vehicle travel until it can be secured safely. Do not forget to retrieve it after passing through airport security.

Wireless Security

Wireless networks and laptops are popular for their convenience and portability. The Internet can be reached via radio waves without having to plug your machine into a network. It is with the same ease of connection that unscrupulous individuals connect to unprotected networks. Attackers conduct drive-by eavesdropping, called “war driving,” to listen in on unsecured devices in homes and businesses. Take the following steps to secure any wireless equipment:
• Change the default out-of-the-box settings to enable a secure connection on your laptop.
• Have a policy regarding use of wireless devices in your organization.

Remote Access

Remote Access allows users to access data from outside locations using dial-up equipment and public telephone lines or wireless phones on the Internet. The outside locations may include other sites as well as a place of business.

• Keep dial-up numbers confidential.
• Remote access to the office via the Internet should use encryption such as SSL or virtual private network (VPN).

Social Engineering

Social Engineering is an approach to gain access to information through misrepresentation. It is the conscious manipulation of people to obtain information without their realizing that a security breach is occurring. It may take the form of impersonation via telephone or in person and through e-mail. Some e-mails entice the recipient into opening an attachment that activates a virus. This was the case with the “MyDoom” virus.

• Before providing information to a telephone caller ascertain if the individual is authorized to receive it.
• Immediately report any suspicious calls to the appropriate individual in your organization.
• Before opening any e-mail attachment, ask yourself if there is anything suspicious about the e-mail.

Phishing

Phishing is a scam in which an e-mail message directs the e-mail recipient to click on a link that takes them to a website where they are prompted for personal information such as a pin number, social security number, bank account number or credit card number. Both the link and website closely resemble an authentic website, however, they are not legitimate. If successful, personal accounts may be subsequently accessed. If you receive one of these e-mails:

• Do not click on the link.
• Delete the e-mail message.
Patching

People are constantly finding security holes (i.e. vulnerabilities) in computer software that could be used to infect your computer with a virus, spyware or worse. When vulnerabilities are discovered, the software vendor typically issues a fix (i.e. patch) to correct the problem. This fix should be applied as soon as possible because the average time for someone to try to exploit this security hole can be as little as a few days.

- Newer software and operating systems can be set to automatically apply updates. If your software supports this, set up the automatic updates.
- For older software, the software vendor typically makes the patches available on its website. Websites should be checked at least once a month for updates and follow the instructions to apply them. If the vendor provides e-mail notification, subscribe to the notifications and follow the instructions in the e-mail to apply the patch as soon as possible.
- Many organizations may already have a process for automatically applying patches, so check with your help desk before applying patches on your work computer.

Possible Symptoms of a Compromised Computer

- Slow or non-responsive; not behaving normally.
- Experiencing unexpected behavior.
- Running programs that you weren’t expecting.
- Showing signs of high level of activity to the hard drive, modem or network interface and you have not touched the keyboard in the last 30 minutes.
- Conveying odd or strange messages on your screen.
- Running out of disk space unexpectedly.
- Unable to run a program suddenly because you don’t have enough memory and this hasn’t happened before.
- Receiving numerous pop-up screens.
- Displaying pop-up screens messages that appear to be very specific to you and or your computer.
- Receiving e-mail messages from people you don’t know complaining about something you sent, said/or never ordered.
- Displaying web pages differently.
- Growing log files that disappear or have gaps.
- Rejecting your password.

If you are experiencing these symptoms, contact your help desk immediately.
Security Breaches

Security breaches can take several forms. The best defense against security breaches are conscientious and alert users. You are the most important person for early detection and prevention. Examples of breaches include:

- Damage to equipment, facilities or utilities.
- Loss or misplacement of media (i.e. disks, tapes, paper) containing confidential/highly restricted information.
- Inappropriate use of the computing environment.
- Unauthorized access or attempted unauthorized access to information or computing resources.

If you discover a security breach, you should report the breach to your Information Security Officer or manager immediately.

Security Tips Related to Terrorism

- Implement "information security" programs. Evaluate the storage, access, and security of sensitive information.
- Create guidelines and conduct periodic assessments of school and district websites to avoid posting of security-sensitive information.
- Use school district call-in lines, websites, and other information sources that can be accessed by the school community to provide ongoing information to the school community.
- Be prepared for e-mail threats, hoax incidents (such as bomb scares), and other "spin-off" security concerns that could result from pranksters and others who may capitalize on the sensitivity of the day.
- A serious and timely response should be given to all incidents, with appropriate consequences for all inappropriate behavior. (Appropriate law enforcement personnel should be contacted to help determine the validity of such e-mail communications and that have the resources to determine the origin of the communications.)

Arson – Juvenile Fire Setting

Juveniles are arrested for the greatest share of arson than any other age group. Historically, juvenile fire setting has been viewed as a problem particular to curious kids. Fire setting is the symptom of a problem, not the problem itself.
Generally, the most common factor among all juvenile fire setters is a severely disturbed home environment with one or no biological parents present. Further, observations that may be indicative and may be important include but are not limited to:

- Higher levels of aggression
- Disruptive behavior
- Low self-esteem
- A poor school performance
- A history of truancy
- Hyperactivity
- Poor relationships and an inability to get along with peers

The majority of juvenile fire setters are males and the intensity and enormity of fires set tend to increase with age. Any single or combination of the aforementioned factors may warrant further scrutiny should circumstance indicate arson as a potential occurrence.

**Anthrax Exposure**

Anthrax infection can occur in three forms: cutaneous (skin), inhalation, and gastrointestinal. Infection with anthrax almost always involves the transmission of anthrax spores.

Cutaneous anthrax is the most common naturally occurring form of anthrax infection. Humans can become infected with anthrax by handling products containing anthrax spores. These spores are introduced into the body under the skin through a cut or abrasion. Low-level germination of the spores into vegetative bacteria then occurs at the primary site leading to swelling and tissue death at the point of entry. Skin anthrax does not usually develop into a serious infection if it is treated with antibiotics.

Inhalational anthrax is the most serious form of the disease and occurs when anthrax spores are breathed into the lungs. There the spores germinate into vegetative bacteria that continue to multiply resulting in severe breathing problems and death should treatment not be sought quickly. The anthrax attacks of 2001 demonstrated that fine mists of anthrax spores can be generated from opening letters and therefore provide an opportunity for exposure.

The following described measures provide a means of reducing exposure to those responsible for receiving and opening mail and offer guidance on developing response plans should an incident be suspected.
Protocols for Mail Handling – New York State Health Department & State Police
Bio-Terror Prevention Protocols:

General:

- Every business and organization should assess and review their protocols for handling mail. Common sense and care should be used in inspecting and opening mail or packages.
- Examine unopened envelopes for foreign bodies or powder.
- Do not open letters with your hands: use a letter opener.
- Open letters and packages with a minimum of movement to avoid spilling any contents.
- Each organization should assess whether it is a possible target for criminal acts. Based on this assessment, you may wish to take additional precautions such as wearing gloves and restricting the opening of mail to a limited number of trained individuals.

What Types of Letters May be Suspect:

- Any letter or package that has suspicious or threatening messages written on it.
- Letters with oily stains.
- Envelopes that are lopsided, rigid, bulky, discolored or have a strange odor.
- Envelopes with no return address.
- Unexpected envelopes from foreign countries.
- No postage or non-cancelled postage.
- Improper spelling of common names, places or titles.

For Suspect Envelopes:

- DO NOT open the envelope or package.
- LEAVE it and EVACUATE the room.
- KEEP others from entering.
- NOTIFY your supervisor, who should call 911 or the local law enforcement authorities.

DO NOT PANIC IF YOU FIND PACKAGES THAT ARE OPENED AND WHICH CONTAIN SUSPICIOUS MATERIAL.

- Anthrax organisms can cause skin infection, gastrointestinal infection or pulmonary infection. To do so, the organism must be rubbed into abraded skin, swallowed, or inhaled as a fine, aerosolized mist. It does not leap into one's body. All forms of the disease are generally treatable with antibiotics.
Anthrax cannot be easily aerosolized out of an envelope or package containing powder. The same facts and conditions are generally true for other bacteria likely to be considered as biological weapons.

Contain the Exposure:

- Close off the room (doors and windows), do not allow anyone other than qualified emergency personnel to enter.
- Close the package or envelope to limit additional exposure. Do not clean powder up; keep others away.
- Do not touch your eyes, nose or any other part of your body.
- If possible, wash your hands thoroughly with soap and water.
- If clothing is heavily contaminated, don't brush vigorously.
- If possible, close down the building's heating and air conditioning systems.
- Make a list of all people who had actual contact with the powder for investigating authorities.

Notify Appropriate Authorities. Immediately contact:

- 911 or your local law enforcement authorities,
- Your local FBI field office, and your local health department.
The New York State Education Department and the New York State Police developed the *New York State School Revised Bomb Threat Guideline* in February 1999 to provide school administrators with suggested activities and response measures before, during, and after the receipt of a bomb threat. The purpose of this guidance document is for school officials to make informed decisions in consultation with local law enforcement officials as it relates to preparing for, and responding to bomb threats in schools.

A bomb threat is a criminal act. No bomb threat should be treated as a hoax when it is first received. The school has an obligation and responsibility to ensure the safety and protection of the students and other occupants upon the receipt of any bomb threat. The following actions may be used when managing a bomb threat in a school building. These actions require planning, preparation, and training.

A. Evacuation of the building after searching exit routes and evacuation areas.

The decision to evacuate a building or to take shelter is dependent upon information about where the bomb is placed and how much time you have to reach a place of safety. Prudent action dictates that students and other occupants be moved from a place of danger to a place of safety. Routes of egress and evacuation or sheltering areas must be thoroughly searched for suspicious objects before ordering an evacuation. Failure to properly search evacuation routes before an evacuation takes place can expose students and staff to more danger than remaining in place until the search has taken place. Assistance is available from local police agencies and the New York State Police to train staff to check evacuation routes.

B. Sheltering students in an area that has been “sanitized and cleared.” School administrators may “sanitize and clear” an area in the school building, such as a gymnasium, to shelter students, faculty and staff while a full building search is conducted.

Assembly spaces, such as a gymnasium, must first be thoroughly searched by volunteer school personnel and law enforcement personnel for suspect objects. This includes searching areas such as bleachers, locker rooms (including lavatory facilities), equipment storage areas, etc. This option may be particularly useful when inclement weather conditions are such that a full-scale building evacuation may endanger students, faculty, and staff. Severe cold weather is an example of such a condition. It is strongly recommended that
school officials carefully coordinate this option in cooperation with local law enforcement officials.

C. Preclearance of the building and maintenance of security to ensure no suspicious objects have been brought into the building by students, visitors, or staff.

This option may only be implemented prior to the receipt of an actual bomb threat. This option is appropriate when a school reasonably anticipates the receipt of a bomb threat or if there is a particular concern over the possibility of a bomb threat. An example of this may be during the administration of Regents examinations or during other school-wide events. This option may not be reasonable during other times. If the school administrator chooses to enact prudent procedures and there is reasonable accountability for ensuring the safety of students and other building occupants, then evacuation is not required. This approach may also be particularly helpful in the event of multiple bomb threats or bomb threats directed at all schools in a county, BOCES, or school district.

School administrators who choose this option must ensure that all steps for ensuring the security of the building are followed completely. Local law enforcement officials and the New York State Police are available for consultation in preparing such a plan and for training school staff on screening techniques.
## Appendix

<table>
<thead>
<tr>
<th>Page</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>Excerpt from, “Lessons Learned from the Beslan, Russia School Tragedy” article</td>
</tr>
<tr>
<td>34</td>
<td>Article from Fox News, “Terror Fears Pose Legal, Security Issues for School”</td>
</tr>
<tr>
<td>36</td>
<td>New York State Homeland Security System for Schools</td>
</tr>
<tr>
<td>38</td>
<td>Gotta Go Bags</td>
</tr>
<tr>
<td>39</td>
<td>School Emergency Resource Page</td>
</tr>
<tr>
<td>41</td>
<td>The State Emergency Management Office</td>
</tr>
<tr>
<td>45</td>
<td>Messages from the Commissioners</td>
</tr>
</tbody>
</table>
The following is an excerpt from the “Lessons Learned from the Beslan, Russia School Tragedy” article:

**Lessons Learned from the Beslan, Russia School Tragedy**

This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid “need-to-know” without prior approval of an authorized DHS official. No portion of this report should be furnished to the media, either in written or verbal form, or posted on a publicly available website.

**Overview**

This Bulletin is being issued to advise recipients of what is currently known about the 2004 Chechen affiliated terrorist attack on the school in Beslan, North Ossetia, Russia, and to provide protective measure guidance. There is no imminent threat to U.S. schools and the group that conducted the operation has never attacked or threatened to attack U.S. interests. However, the extensive media coverage and the high casualty rate generated by the incident in Beslan warrant a summary of lessons learned from that incident and protective measure guidance for helping to prevent and respond to a similar terrorist

Title: Lessons Learned from the Beslan School Attack

Date: October 6, 2004

**Protective Measures**

Most school districts have already developed emergency and crisis management plans. The following recommendations for protective measures are provided for use during the regular review and update of those plans. Protective Measures in the short-term should emphasize procedural safeguards for school populations and facilities. These protective measures include the following:

- Review and validate all school emergency and crisis management plans for completeness and currency. Helpful guidance can be found at: www.ed.gov/emergencyplan.

- Raise awareness among law enforcement officers and school administrators by conducting tabletop exercises (TTX) for school emergency and crisis management plans.
• Raise awareness among school workers and students by conducting “all hazards” awareness training for the school environment.

• Raise community awareness of any potential threat and vulnerability.

• Prepare the school staff to act in a crisis situation and exercise this ability.

• Consider a closed-campus approach to population control that would strictly limit visitors.

• Consider a single entry-point for all attendees, staff, and visitors.

• Focus patrols by law enforcement officers around and on school grounds.

• Have a plan to maintain contact with school buses.

• Ensure that emergency communications from and to schools are present, operable, and exercised.

• Obtain “Terrorism: Preparing for the Unexpected” brochure from the local Red Cross Chapter and distribute it to parents of students in grades K-12, staff, and faculty. http://www.redcross.org/pubs/dspubs/terrormat.html

• Report suspicious activity and individuals to proper authorities.

Protective Measures in the long-term should emphasize physical safeguards that involve physical plant enhancements to present a more robust target and to provide a more survivable environment. Among the measures schools should consider are the following:

• Install secure locking mechanisms for all external and internal doors and windows, with quick-release capability from within for fire escape.

• Install robust window and external door protection means with quick-release capability from within for fire escape.

• Consider a safe area (or safe areas) within the school for assembly and refuge during crises. Consider retrofitting of robust structural enhancements and an over pressurization system in the safe area(s).
• Consider applying protective coating for windows on facilities that face traffic areas. That and other helpful information on school facilities can be found at: www.edfacilities.org.

The following activities may suggest terrorist surveillance of educational facilities. Alone, each indicator can result from legitimate recreational or commercial activities or criminal activity not related to terrorism; multiple indicators, however, could suggest a heightened terrorist threat:

• Unusual or prolonged interest in security measures or personnel, entry points, and access controls or perimeter barriers such as fences or walls.

• Interest without reason in obtaining site plans for schools, bus routes, attendance lists, and other information about a school, its employees, or students.

• Unusual behavior such as staring at or quickly looking away from personnel or vehicles entering or leaving designated facilities or parking areas.

• Observation of security reaction drills or procedures.

• Increase in anonymous telephone or e-mail threats to facilities in conjunction with suspected surveillance incidents--indicating possible surveillance of threat reaction procedures.

• Foot surveillance involving two or three individuals working together.

• Mobile surveillance using bicycles, scooters, motorcycles, cars, trucks, sport utility vehicles, limousines, boats, or small aircraft.

• Prolonged static surveillance using operatives disguised as panhandlers, shoe shiners, food or flower vendors, newsagents, or street sweepers not previously seen in the area.

• Discreet use of still cameras, video recorders, or note taking at non-tourist locations.

• Use of multiple sets of clothing and identification or the use of sketching materials (paper, pencils, etc.).

• Questioning of security or facility personnel.
• Unexplained presence of unauthorized persons in places where they should not be.

Law enforcement agencies, security personnel, and educational administrators should be aware and remain alert to indicators of surveillance activities. School officials are encouraged to review and update their evacuation plans as well as security and emergency policies. In addition to planning and the need for frequent exercises involving both the schools and the First Responder Community (Law Enforcement and Fire/EMS), planning and exercises should involve the local medical community to ensure that mass casualty contingencies are fully covered. Emergency medical treatment for children is significantly different from adults and should be factored into any plan or exercise. In conjunction with this Joint Information Bulletin, the Department of Education will disseminate this information in its own format to its constituents using Department of Education channels. Information on suspicious activities potentially related to terrorism should be forwarded immediately to local law enforcement ultimately to the local FBI JTTF and the DHS HSOC as previously indicated.

**Article from Fox News**

Terror Fears Pose Legal, Security Issues for Schools – Oct. 13, 2004
(http://www.foxnews.com/story/0,2933,135360,00.html)

This week, Russia ends its official 40-day mourning period for the victims of the Beslan (search) terror attack. While the world remains horrified by the massacre of hundreds of children by Chechen (search) rebels, the incident poses some interesting, if frightening, liability questions for school districts in the United States.

Like every custodian of children, a school district can, as a general matter, be liable for injury to students if it has notice of some potential or impending harm and fails to take reasonable steps to avoid it. The formulations vary from state to state, and the plaintiff's burden can differ depending on the type of harm suffered. In recent years, the number of circumstances in which school districts have been found liable for injury to students has increased. For example, school districts have faced liability for the intentional, criminal conduct of teachers who covertly sexually harass students. It has been widely reported that the U.S. military apprehended an individual in Iraq who possessed two CDs filled with publicly available information on eight school districts in six states. The information included evacuation plans and instructions on how to deal with a crisis. The Department of Homeland Security (search) has stated that the individual has no known ties to terrorism and has worked with schools in Iraq. At the same time, the individual who possessed the CDs apparently was someone sought by authorities in Iraq, and DHS thought the information significant enough to pass
along to the school districts mentioned on the CD. What's contained in the CDs seems equivocal, but if it poses a threat, that threat is severe. Statements by some school officials show they believe they should take preventative action, but need more precise information. "It's very frustrating because we weren't told by the authorities which school it was and the information hasn't really flowed down locally to the police or to us," said John Scavelli, superintendent of schools in Franklin.

Township, N.J. Does the law require a prudent superintendent to take a vague warning, combine it with what is known of wider security conditions, and then act? The answer is, they probably should. This is not a firm answer, but much of negligence law is not governed by statute. Should lawsuits arise from a terrorist incident at a school, the jury will be asked whether a prudent superintendent could foresee a terror attack and take effective precautions. However vague the information, these school districts have received some warning. Also consider that school superintendents already have the reference point of Beslan. At Beslan, between 17 and 25 Chechen rebels who had traveled from some distance away practically walked into a school, herded students and parents into a gymnasium, and then wired it with explosives. One would have to ignore recent news to not see signs of similar events taking place in the U.S. For example, the Department of Homeland Security is now investigating an intelligence report, reputedly provided by reliable elements of Russia's security services, that a group of 25 Chechen terrorists illegally entered the United States from Mexico in July. (The DHS has said repeatedly that it will not militarize our southern border because, they say, there is no evidence of terrorists entering from Mexico.) Not only does the size of that group approximate the number of terrorists believed to have carried out the Beslan massacre, but according to the report, they chose a point of entry in a mountainous area of Arizona that is known to be difficult for immigration authorities to patrol. This suggests that the group placed a higher value on anonymity than would-be immigrants, who are frequently apprehended, photographed, bused back across the border, and make a successful entry later the same day. Any school district trying to gauge its liability exposure in this area can take heart in the fact that many of our country's inner-city schools have succeeded in controlling their entrances through the use of locked doors, police and metal detectors. Additional security measures would likely be required to stave off a Beslan-like threat, but school officials must begin to investigate and implement such measures now. For as disturbing as these thoughts may be, for these eight school districts, a jury might one day require it.
New York State Homeland Security System for Schools

The New York State Education Department, State Department of Homeland Security, and State Police, in consultation with BOCES and the New York State Center for School Safety, developed the *New York State Homeland Security System for Schools*. The purpose of this guidance document is for school officials to make informed decisions in consultation with local law enforcement officials as it relates to the status of the National Color Code System. The following chart (next page) summarizes the recommended actions for schools at each color code level.

The full document may be accessed at the following link: http://www.emsc.nysed.gov/deputy/Documents/alerts/cover-toc.html.
The ultimate responsibility for actions taken in a district rests with district administration. These recommended actions are guidelines and should be implemented based on the judgment and discretion of authorized district officials.

* See page 7 for definitions.
** See page 13 for instructions and response actions.
*** See page 16 for instructions and response actions.
# Gotta Go Bags

Gotta Go Bags are school emergency bags that are filled with supplies that you may need to have or take with you in an emergency. A minimum of two bags should be kept in each building. The bags should be kept in different locations in the school in the event that one location is not accessible. It is also a good idea to keep a bag at an outside location such as, in an evacuation site.

There are school level gotta go bags and district level gotta go bags. The bag should be updated periodically, to make any necessary changes or replacements.

The following is a list of basic items schools and districts may need to include in the bags.

## School Level Supplies:

- Student register with parent emergency numbers
- List of students with custody limitations
- Teacher/Employee roster
- Teacher schedules
- School emergency plan
- Building floor plans - Not the blueprints, the internal layout with rooms numbered.
  (10 copies - to give to agencies responding to an incident.)
- Exterior school grounds maps - 5 copies
- Map of local area
- Cellular phones - consider battery charging/power adapters
- Emergency phone numbers
- Bell horn(s)
- Portable radios
- Master keys to building - 2 sets, minimum
- Pens and pencils
- First aid supplies
- Student tracking forms - carbonless system
  where the teacher/employee can record the students with them.
- Index cards and note pads
- Other forms or documents the school may require
- Flashlights and batteries
- Duct tape
- AM/FM radio
- Blanket
- Cups, plastic containers and a water source
- Towels
- Utility knife
- Screwdriver
- Pliers
- Plastic bags

Things you may need that won’t be stored in the gotta go bag:
- Student medications
- Teacher/Employee daily attendance record
- Student daily attendance record

## District Level Supplies:

- First aid supplies
- Blankets
- Building floor plans - multiple sets for each building
- District emergency plans
- Parent reunification forms
- Computer (desk or laptop) and printer
- Material to make signs for directing parents to the reunification center

Keep in mind that personnel from other schools may be able to assist you in evacuating the building.
School Emergency Resource Page

American Academy of Pediatrics
http://www.aap.org/advocacy/releases/disaster_preparedness.htm

American Red Cross: Masters of Disaster
http://www.redcross.org/disaster/masters/

Emergency Planning Resources for Parents & Teachers
http://www.fema.gov/kids/teacher.htm#terror

FEMA: Multihazard Emergency Planning for Schools (Independent Study)
http://training.fema.gov/EMIWeb/IS/is362.asp

National Association of School Psychologists
http://www.nasponline.org/NEAT/index.html

National Clearinghouse for Educational Facilities – Disaster Preparedness
http://www.edfacilities.org/rl/disaster.cfm

National Organization on Disability (Preparedness for Children With Disabilities)
http://www.nod.org/emergency/index.cfm

New York State Center for School Safety
http://int11.mhrcc.org/scss/

NFPA: Risk Watch
http://www.nfpa.org/riskwatch/home.html

Practical Information on Crisis Planning: A Guide for Schools and Communities;
U.S. Department of Education, Office of Safe and Drug-Free Schools,
Washington, D.C.

http://www.mhric.org/scss/ProjectSAVE.pdf

New York State Health Department, Bureau of Communicable Disease Control
518-473-1730 (day); 866-881-2809 (after hours)
In New York City, call New York City Department of Health Mental Hygiene: 212-
788-9830 (day); Poison Control Center 212-764-7667 (after hours)
http://www.health.state.ny.us/nysdoh/bt/mailprotocol.htm
New York State Police Bomb Threat Card
http://www.troopers.state.ny.us/Publications/Crime_Prevention/bombcard.pdf

New York State Police Gotta Go-Bags
http://www.troopers.state.ny.us/Schools_&_Communities/Gotta_Go_Bags/

New York State Emergency Management and State Police Incident Command System Training for Schools
http://www.nysemo.state.ny.us/TRAINING/TrainingHome.htm
The State Emergency Management Office

Its Role

The New York State Emergency Management Office (SEMO) coordinates Emergency Management Services for the State by providing leadership, mitigation measures, planning, education and resources to protect lives, property and the environment. SEMO coordinates these activities through local government officials, specifically county emergency managers.

Planning Assistance

SEMO staff can provide technical planning assistance to school officials in developing and updating Building-Level Emergency Response Plans or District-Wide School Safety Plans. Working in coordination with local emergency managers, SEMO can assist school officials in applying the latest concepts of all-hazards emergency preparedness to school planning efforts. Assistance can include identifying ways to incorporate security procedures into the overall response plan, as well as addressing key points to consider when integrating the school emergency response with local emergency responders. Contact the appropriate SEMO Regional Office for further information.

Incident Command System (ICS) Training

Schools officials can receive training in the Incident Command System (ICS) to effectively manage a response to an emergency. The ICS training offered by SEMO is part of the curriculum for training in the National Interagency Incident Management System (NIIMS) Incident Command System. The curriculum has several levels of training, starting with the very basic and progressing to the advanced level. The SEMO website is a good source to access the Introduction to ICS (I-100), designed to prepare course participants for the intermediate and advanced levels of training. The I-100 Course is an Independent Self-Study course that can be done on line by logging on to http://www.nysemo.state.ny.us/TRAINING/Training.Home. To inquire about additional ICS training, visit the website or contact the SEMO Regional Office that serves your area.

Training Using HAZNY (Hazards New York)

SEMO has recently revised the automated hazard analysis program, HAZNY (Hazards New York). HAZNY is a Microsoft-based planning tool used to identify and rank internal and external hazards that may potentially affect a school facility or school district. From the hazard ranking, school officials can quickly and easily identify and prioritize their mitigation and planning efforts. SEMO has developed a HAZNY Train the Facilitator Course designed to teach public officials on how to conduct a hazard analysis for their own usage. Contact
the appropriate SEMO Regional Office to inquire about a Train the Facilitator Course in your area.

**Professional Development Series (PDS) Courses**

SEMO offers a variety of Professional Development Series (PDS) Courses designed to enhance the participant’s knowledge of emergency management concepts, practices and methodologies. While all can be done by Independent Self-Study, SEMO routinely conducts the PDS Curriculum across the state. The courses offered are as follows:

1. Principles of Emergency Management
2. Emergency Planning
3. Exercise Design
4. Effective Communications
5. Decision Making and Problem Solving
6. Leadership and Influence
7. Developing Volunteer Resources

Additional course information, training announcements and course schedules can be found by visiting the SEMO website at: http://www.nysemo.state.ny.us/TRAINING/Training.Home.htm.

PDS announcements and on line study can also be found by visiting the Federal Emergency Management Agency (FEMA) web page at: http://www.fema.gov.

**Multi-Hazard School Safety Training**

School officials can also inquire about attending courses at the Emergency Management Institute (EMI) in Emmitsburg, Maryland. EMI has many programs in emergency management, including FEMA’s “Multi-Hazard School Safety” course. The listing for these courses is accessible through the SEMO website, or through the local county emergency manager’s office.

**Potential Community Hazards**

SEMO can provide the hazard ranking of potential external hazards that school official should consider when conducting their own hazard analysis. This list is community-based and availability is subject to which municipalities have done a Hazard Analysis. SEMO can provide Hazard Analysis reports of jurisdictions that have done the analysis to school officials.
Weather Information

SEMO coordinates with the National Weather Service (NWS) and other sources for weather-related training and information. A variety of weather-based links can be found on the SEMO home page to aid in obtaining weather facts, forecasts and hazardous weather information.

Additional Links

Additional links and information on a variety of SEMO programs can be found on the SEMO home page at http://www.nysemo.state.ny.us. Links include guidance from the SEMO Planning Section, information from the Hazard Mitigation Section and links to local emergency management officials.

Contacts

SEMO headquarters, located in Albany, utilizes five regional offices to coordinate activities in support of local government. The regions and contacts are as follows:

Region 1: Includes Nassau and Suffolk Counties, and the New York City Metropolitan area.

Regional Director
250 Veteran's Memorial Highway
Hauppauge, NY 11788-5506
Bus: (631) 952-6759
Bus Fax: (631) 952-3364
semoregion1@semo.state.ny.us

Region 2: Includes Rockland, Orange, Westchester, Putnam, Ulster, Sullivan, Dutchess, Columbia, Greene, and Delaware Counties.

Regional Director
171 Cheney Drive
Poughkeepsie, NY 12601
Bus: (845) 454-0430
Bus Fax: (845) 454-4620
E-mail: semoregion2@semo.state.ny.us

Regional Director  
5 Fox Farm Road  
Queensbury, NY  12804-1107  
Bus: (518) 793-6646  
Bus Fax: (518) 793-6647  
E-mail: semoregion3@semo.state.ny.us

**Region 4:** Includes Broome, Tioga, Chenango, Cortland, Tompkins, Schuyler, Cayuga, Seneca, Onondaga, Madison, Oneida, Oswego, Lewis, Jefferson, and St. Lawrence Counties.

Regional Director  
Hancock Field  
6900 Thompson Road, Room 113  
Syracuse, NY  13211  
Bus: (315) 438-8907  
Bus Fax: (315) 438-3550  
E-mail: semoregion4@semo.state.ny.us

**Region 5:** Includes Chemung, Steuben, Allegany, Cattaraugus, Chautauqua, Erie, Wyoming, Livingston, Yates, Ontario, Genesee, Wayne, Monroe, Orleans, and Niagara Counties.

Regional Director  
1144 East Union Street  
Newark, NY  14513-9201  
Bus: (315) 331-4880  
Bus Fax: (315) 331-3934  
E-mail: semoregion5@semo.state.ny.us
Messages from:
The Honorable Mary Donohue, Lieutenant Governor:

Our children are our most precious resource and hope for tomorrow. As a mother of two, former teacher, District Attorney and State Supreme Court justice, I know that we must do everything possible to protect them in our communities and in our schools. In 2000, Governor Pataki signed into law the Safe Schools Against Violence in Education Act, a comprehensive series of recommendations from the statewide Task Force I chaired, which was aimed at reducing violence in schools. Project S.A.V.E., brought together educators, law enforcement and emergency planners from across the state to develop plans and guidance that our schools can use to maximize our children’s safety. But we haven’t stopped there.

We continue working with our local law enforcement and school districts to review, assess and implement safety and security strategies to ensure our schools continue to be the safest in the nation. In today’s state of world affairs, this strategy couldn’t be more appropriate.

In addition to the comprehensive guide, this video illustrates best practices and security strategies found in schools throughout our great state. It emphasizes our efforts to instill security awareness and implement the best security levels in all of our schools.

The Governor and I hope that you use these examples to continue to make your school safer today for the benefit and future of our children.

James W. McMahon, Director, Office of Homeland Security:

The world we live and work in today is a far different place than it was three years ago. Security in our communities has taken on an entirely new focus and importance. As a State, New York has done everything possible to ensure the safety of its citizens - in the workplace, on our streets and in the schools. Daily we work with law enforcement agencies throughout the State doing just that. But we need YOUR help. As educators, you know the trust parents place in your hands to ensure the safety and well being of their children. Governor Pataki’s signing into law the Safe Schools legislation in 2000 was a strong step to assuring the safety of our schools by bringing educators and law enforcement officials together to work in unison developing comprehensive security strategies. I urge you to continue those cooperative efforts in your communities. Work with your local law enforcement, public officials and emergency response agencies. We all need to be aware....and be prepared. I am confident that many of the security strategies and best practices you will see in this video
will be of assistance to you. Take these tips and work with your local law enforcement to fashion a strategy that works in your community. It will take time, patience and cooperation. But we can never be too careful to protect our most precious resource, our children.

Wayne E. Bennett, Superintendent, New York State Police:

Our Educational system shapes and defines our nation. Children are our most important asset and deserve to feel safe at home, as well as in the school environment. The School Resource Officer program is a proactive effort to form partnerships between law enforcement and schools.

In our ongoing effort to keep our young people away from crime and to provide them with opportunities to succeed, school resource officers become mentors to students and liaisons to the communities they serve. Duties of the SRO's include working directly with students and teaching them conflict resolution, restorative justice, anger management, crime prevention programs and personal safety skills. They also present safety and crime prevention programs to all school employees, as well as parents and school board members, and work to improve relations between law enforcement and the community.

Each year, because of the successes of the SRO program, additional school districts from across the state request their own SRO services. Parents should not have to worry about their children's safety in the classroom. With these programs, police departments provide school districts, and all those who teach our children, the resources to ensure a safe and secure learning environment.

Richard P. Mills, Commissioner, State Education Department:

School emergency planning and response to any type of issue is of critical importance and touches all of us in the education community. Many schools throughout New York State have faced situations that required use of their emergency response plans. In these cases, school administrators, faculty and staff exercised judgment in carrying out their duties to ensure the safety of the children in their care.

But we need to do more. We need to test and update emergency plans continually with law enforcement and emergency management professionals. By doing that administrators, faculty and staff will learn and
practice the actions that would be necessary in a real emergency. I encourage you to take advantage of the resources available in this package.

James W. Tuffey, Director, State Office of Emergency Management:

Given the current state of world affairs today, we know that it pays to be prepared. And based on our experience, a key element to achieving that goal is to develop an emergency plan, which factors in all variables and all hazards. Emergency plans cannot be created in a vacuum. All of the key players who work in your community to make it a safer place must be part of the Planning Process. Make your emergency plan a living, breathing document. A plan shouldn't be sitting on a shelf gathering dust. So, I encourage you to take the time now to sit down with your local emergency manager, local law enforcement, and other emergency services officials to revisit the plan. Think outside the box. And when you are done with the review, take the next step: Test the plan by conducting drills and exercises in your school, involving local law enforcement and other response officials. We have a saying in our profession that goes like this: "Plan for the worst and hope for the best." I am sure that you will find that the plans you develop now will make your school a safer place and ready for the unexpected both today and in the future.