Homeland Schools Preparing for Bioterrorism

U.S. public schools are including plans for responding to bioterrorism incidents in their Incident Response Plans, according to the National Resource Center for Safe Schools (NRCSS, www.safetyzone.org, select: “publications”; NRCSS SafetyZone Newsletter Volume 3, Issue 4, Winter 2001; “bioterrorism”). Procedures to limit possible contamination from substances such as anthrax include teaching personnel who find suspicious packages not to bring them to the school office. Instead, experts recommend leaving the package where it was found and securing the doors and windows in the classroom or office where the package was discovered.

FBI Advisory is available at www.kysafeschools.org/pdfs&docs/safemail.pdf.
TECHNICAL ASSISTANCE

We are here to help you! DynCorp supports the DoDEA Safe Schools Program by responding to requests from DoDEA school administrators.

So, contact us...

Robert Michela, Director, Safe Schools Program, michelar@dynCorp.com, (703) 461-2207
Brian McKeon, mckeanb@dynCorp.com, (703) 461-2271.

Student School Violence Discussions

Students in school violence discussion groups sponsored by the state of California reported that they find conflict management and peer mediation more effective with students who choose to participate. Students also indicated that physical fights often result from poor communication. Results from the student discussion groups are summarized in the report, School Violence Prevention & Response (www.ocjp.ca.gov/publications/pub_schlvio.htm).

Alternative Education for Students at Unsafe Schools

The Leave No Child Behind Act requires U.S. public schools to offer alternative education to students, but only if the students can document that their school qualifies as a “persistently dangerous school”. According to the National Association of Secondary School Principals (NASSP), student victims of a violent criminal offense or students who document that their school is violent would have the opportunity to attend charter schools (www.nassp.org/news/essa_req.html).

SROs Use Non-Lethal Weapons

Ninety three percent of School Resource Officers (SROs) wear non-lethal agents such as pepper spray as part of their regular police equipment, but only 7% of SROs wear electronic tasers according to the National Association of School Resource Officers (NASRO). The report summarizes responses from SROs surveyed at the NASRO convention.

Survey highlights include:

- 24% SROs have taken guns from students
- 87% SROs have taken knives from students
- 84% SROs believe that crimes on school campuses are generally under reported to police
- 91% SROs believe that an unarmed officer puts students at greater risk of harm or injury
- 97% SROs wear guns as part of their daily police equipment

Risk Reduction Planning Similar to Military Field Survey Activities

The DoDEA Five-Phase model for Safe School Planning uses an approach similar to that of an operations security survey used by military security planners. Safe School Plans should be based on the vulnerabilities of the school community to potential or existing threats. Threats can be external, internal, or a combination of the two. Military field survey activities include data collection, identification of vulnerabilities and key indicators, assessing risk, and developing countermeasures. Both systems begin with the identification of the threat and end with a plan to overcome it.

Identifying Problems (Phase One) is similar to the data collection step in a field survey process. With the problems identified, the safe school committee can establish security objectives (Phase Two). Then the committee can evaluate existing measures and identify options (Phase Three). These phases are equivalent to the military’s procedures for determining vulnerability, assessing risk, and developing countermeasures.

The inability of existing measures to overcome a threat will define the vulnerability that must be addressed during Phase Four: Select Options. Selecting options based on an identified threat ensures that your plan is properly focused and analytically sound. Writing a plan is easy once you have completed the first four phases.

The planning tools provided in the DoDEA Safe Schools Handbook are designed to assist you in properly identifying the threat. Use Tool 1: Incident Worksheet, to analyze data from previous incidents, i.e. Serious Incident Reports. Study the completed Incident Worksheets to discern patterns of threats. Tool 2: Student Surveys and Tool 3: Staff Surveys, provide information about potential incidents or incidents that have occurred but were not reported. Anonymous crime reporting “hotlines”, student suggestion boxes, and personal communication with students are also means of obtaining information about possible threats.

Tool 6: Program and Policy Review and Tool 7: Physical Security Review indicate how well existing programs, policies and physical security measures are working. The less capable the existing security measures are of responding to the threat, the greater the risk. Tool 8: Options Worksheet assists the committee in identifying appropriate responses for reducing risk (i.e. countermeasures).

Investing Safe Schools Committee members’ time to properly define the threat at the beginning of the Safe School Planning process saves the principal time at the end of the process and facilitates the writing of the Plan.
Intervention Strategies

Teaching Parents to Sign-In at the School Office

Involving parents in implementing visitor sign-in policies can enhance school security. Schools often find this security policy tough to implement because the office is not located near the school entrance, or there are several entrances to the school. Parents familiar with the school often go directly to a parent-teacher meeting or school activity rather than visiting the school office first. However, a well-communicated policy supported by friendly but firm reminders from school staff members converts this potential vulnerability into an opportunity to strengthen parent-school connections. Some schools communicate policy to parents via student handbooks, school Internet sites, or letters to parents.

The Southeast Regional Drug-Free Schools and Communities Center (SERVE) describes how parents assist Texas High Schools with security. SERVE recommends that older schools with several entrances designate one entrance just for visitors during the school day (Reducing School Violence: Building a Framework for School Safety, p.29, available from SERVE, www.serve.org/publications/vision23bpfss.htm.) Signs at other entrances direct visitors to the appropriate entrance and school office.

DoDEA parents could assist by sitting near the appropriate entrance to welcome visitors and escort them to the school office. Personnel in the school office can encourage future compliance with the sign-in policy by reminding visitors that parents and educators on the Safe School Committee opted for visitor sign-in procedures to protect students. Parent assistance implementing sign-in policy enhances school climate because it reminds all the members of the school community of the need to take responsibility for school security. This proactive approach to enhanced security awareness increases the probability that a hostile intruder will be identified and reported in time for the school to respond.
Computer Security

Many U.S. public schools are now required to write a computer security policy according to the Texas Association of School Boards (TASB). According to TASB’s policy update on Internet Use (www.tasb.org/policy/sp/sp_netuse.shtml#4), federal law requires schools receiving ESEA funding to establish an Internet safety policy requiring the use of filtering software to prevent exposure to obscenity, child pornography, and “harmful” materials. At Blair High School in Montgomery County, Maryland, the Teacher Handbook (www.mbhs.edu/resources/teacher/Handbook.html) describes computer security guidelines regarding unauthorized access, inappropriate communication, plagiarism, computer vandalism, and illegal use of the Internet. Penalties for student violations of computer security policy include loss of computer privileges, school detentions, in-school suspensions, police referral, or student expulsions.

<table>
<thead>
<tr>
<th>Unauthorized Access</th>
<th>prohibits reading other students’ e-mail, learning others’ passwords, or attempting to access other computer networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inappropriate Communication</td>
<td>prohibits students using or obtaining obscene, vulgar or inappropriate language, pictures or other material from the Internet</td>
</tr>
<tr>
<td>Plagiarism</td>
<td>prohibits students using others’ work; students should provide proper academic citations for documents found through Internet searches</td>
</tr>
<tr>
<td>Computer Vandalism</td>
<td>prohibits the introduction of computer viruses into the computer network or damaging the physical computer equipment</td>
</tr>
<tr>
<td>Illegal Use of Internet</td>
<td>prohibits using the school computer network for activities such as obtaining and installing software from the Internet</td>
</tr>
</tbody>
</table>