United States
Environmental Protection
Agency New England

# Colleges and Universities

October 2003

# Site Security Awareness

## Safeguarding Against Terrorism

### Introduction

Emergency planning and management are increasingly recognized as critical to the operations of colleges and universities, and require closer partnerships with first responders at the federal, state and local levels. More than ever before, emergency planning requires close coordination among the responding departments within an institution including: public safety, Environmental Health and Safety, public information officers, residence hall directors, student life, information technology, and managers of facilities housing hazardous materials. The purpose of this fact sheet is to provide security suggestions and to increase awareness on security matters that may impact your campus, its stability, and your community.

### Site Security: Are you a target for terrorism?

Physical security measures will deter adversaries. Consider the following:

- Identify campus assets that could be used as a weapon of mass destruction (WMD);
- Provide layers of security, starting at the campus's perimeter and then assess other critical operations such as food services; residence halls; research facilities; laboratories; recreation areas; and critical valves, filters, and pumps;
- Perimeter protection measures include fences and exterior walls, bollards, personnel gates and turnstiles, vehicle gates, and security lighting;
- *Employ skilled security personnel to aid in access control and emergency response;*
- Access control measures, such as signs, locks, alarm systems, security doors and windows, card-based access control systems, and biometric systems;
- Surveillance and monitoring through close circuit television (CCTV)/surveillance cameras in critical or restricted areas; digitized card reader; faculty, staff, student and contractor ID badges; visitor pass/badge; and/or entry log book;
- Protect and secure electricity, communications, and other utilities with uninterrupted and backup power source, such as a generator.

*"Homeland security is now one of our nation's highest priorities. We must all take part in safeguarding against emergencies and disasters."*

### Faculty, Staff, Students and Contractor Security

Threats that "come from within" are the most difficult to detect.

- ⇨ Restrict access and allow only authorized employees who work in sensitive or restricted areas (Scientist, Service Personnel, Visitors, Vendors, Contractors, etc.);
- ⇨ Establish background screening policies for all faculty, staff and contractor;
- ⇨ Evaluate screening processes for students, especially those who may have access to restricted areas;
- ⇨ Ensure that individuals in the laboratories are aware of restrictions on storage, transferring, receiving, and use of materials with chemicals, biohazards, explosives, or radiological hazards.
- ⇨ Maintain inventory control of all materials with chemicals, biohazards, explosives, or radiological hazards on your campus.
- ⇨ Implement prohibition policies and reporting procedures for faculty, staff, student and/or contractor regarding physical violence, verbal abuse, willful destruction of property, and intimidation.

## Management Issues

In today's society, security is everyone's responsibility. The following is a list of "risk-based management decisions" that must be considered in planning:

- Integrate site security into your campus's Emergency Response Plan;
- Security should be given consideration as one of the university's core values. Establish written university policies and procedures pertaining to security;
- Use a risk-based approach to assess and select the right security control measures;
- Survey workforce skills;
- Assign the oversight of security (e.g., physical, personnel, and information systems) to top managers;
- Include security in all appropriate training and courses;
- Work with local, state, and federal law enforcement and other public safety agencies;
- Be an active member of your Local Emergency Planning Committee (LEPC);
- Assess and periodically reassess your campus security systems. Identify any existing or potential threats, targets, vulnerabilities, hazards, risks, as well as mitigation and countermeasures;
- Evaluate faculty, staff, students and contractors identification procedures;

*"Maintain communication links with local and state law enforcement agencies to stay up-to-date on potential threats within your community"*

- EXERCISE THE PLAN;
- Consider just-on-time management of extremely hazardous substances. Keep and use the least amount of chemicals on-site as possible. Explore product substitution, especially in your laboratories.
- Review suppliers' transportation security procedures;
- Regularly update written security policies and procedures, including the following:
  - ⇨Physical security systems;
  - ⇨Results of vulnerability and/or risk assessment;
  - ⇨Procedures for referring suspicious incidents to campus police or appropriate authorities;
  - ⇨Protection of university information, computers, and networks;
  - ⇨Procedures for emergency response, crisis management, and shutdown;
  - ⇨Recognition of security breaches and proper actions to be taken;
  - ⇨A system for collecting and analyzing reports of security incidents;
  - ⇨List of contact names and information for reporting security incidents.

## Information, Computer, and Network Security

Information, computer, and network security are distinguished from physical security because information protection goes beyond proprietary information and university procedures. Potential adversaries can obtain information on chemical processes, list of hazardous materials, and databases that relate to biohazard research from a university's computer and network systems. The following tips should be considered in establishing information security:

- ☑ Use protective hardware and software;
- ☑ Establish procedures for protecting and destroying sensitive documents;
- ☑ Change codes and passwords following a termination of employment;
- ☑ Back up all critical information and data at an alternate location;
- ☑ Don't leave personal planning/scheduling devices unattended;
- ☑ Be aware that sensitive information conveyed by telephone conversations, radio communications, and network communications can be intercepted. Consider using voice encryption;
- ☑ Periodically analyze University computer transaction histories to look for irregularities that might indicate variances in normal procedures and/or security breaches.
- ☑ Develop screening process or procedures for computer repairs if equipment may contain sensitive information.

## Weapons of Mass Destruction (WMD)
## Examples at Campuses and Their Consequences

**Explosives:** Picric Acid (Dry and crystallized); Ammonium Nitrate; Hydrazine Compounds; Diazo Compounds; Nitrocellulose (Dry); Peroxide forming agents such as: Diethyl Ether; Tetrahydrofuran; Isopropyl Ether Dioxanes; Aldehydes; Compounds with benzylic hydrogens; Compounds with allyl groups

**Chemical:** Poison gas, blister gas

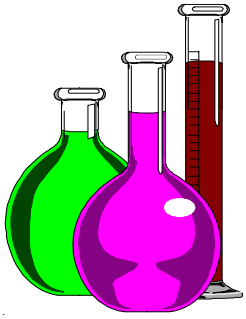
**Biological:** Anthrax; Small Pox; Ricin; Botulinum Toxin; Human Immunodeficiency Virus (HIV); Plague; Viral Hemorrhagic Fever(VHF)

**Nuclear:** Any equipment or weapon that is designed to release radiation or radioactivity at a level dangerous to human life

Note: In addition to the obvious consequences (e.g., deaths, injuries, damaged structures, possible contamination, possible long-term effects, far-reaching geographic effects), universities may also consider the economic consequences to the institution and the potential physcological ramifications throughout the campus.

Did you know that under the proper conditions...?

- 4 oz can of ethyl ether is equivalent to 1 stick of dynamite.
- 8 oz of picric acid is equivalent to 1 stick of dynamite.

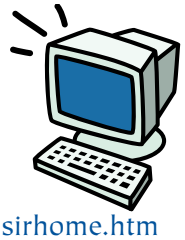


### Federal Offices

| | | | |
|---|---|---|---|
| DHS (Watch & Warning Unit): | 1.888.585.9078 | FBI - Boston, MA | 617.742.5533 |
| EPA New England Environmental Emergency | 800.424.8802 | FBI - New Haven, CT | 203.777.6311 |

**Non-Emergency**
EPA New England Customer Call Center 888.372.7341or 617.918.1111

### Web Resources for Emergency Planning



| | |
|---|---|
| Agency for Toxic Substances and Disaster Registry | http://www.atsdr.cdc.gov/ |
| American Red Cross | http://www.redcross.org |
| Education Resources Information Center (ERIC) | http://www.eric.ed.gov/ |
| Federal Emergency Management Agency (FEMA) | http://www.fema.gov/ |
| FBI/Awareness of National Security Issues & Response | http://www.fbi.gov/hq/ci/ansir/ansirhome.htm |
| Lawrence Berkeley National Laboratory | http://securebuildings.lbl.gov/ |
| National Response Team (NRT) | http://www.nrt.org/ |
| Office of Domestic Preparedness (ODP) | http://www.ojp.usdoj.gov/odp/ |
| US Department of Education | http://www.ed.gov/ |
| US Department of Homeland Security (OHS) | http://www.whitehouse.gov/homeland/ |

This is a selected list of sites that provide timely and useful information about emergency planning and counter-terrorism; it is not an exhaustive list of all parties with a role or interest in the subject matter. Inclusion here does not mean an endorsement of the site.

**For additional information, please visit EPA's web site at:**
**http://yosemite.epa.gov/oswer/ceppoweb.nsf/content/index.html**

## Homeland Security Presidential Directive (HSPD) - 5

### National Incident Management System (NIMS)

In response to the terrorist attacks on September 11, 2001, the President issued Homeland Security Presidential Directive (HSPD)-5 which called for the development of a National Response Plan (NRP) to integrate Federal Government domestic prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan under the authority of the Secretary of Homeland Security. This directive also called for the creation of a National Incident Management System (NIMS), which would provide a standardized system for implementing the NRP.

NIMS provides a consistent yet flexible nation-wide framework within which local, State, and Federal levels of governments and the private sector will work effectively and efficiently to be aware of, to prepare for, to prevent, to respond to, and to recover from domestic incidents, regardless of their cause, size, or complexity. To provide for seamless cooperation among Federal, State, and local capabilities, the NIMS includes the following core concepts and principles:

- NIMS standardizes incident management systems for all hazards and all levels of government.
- NIMS extends incident management into the awareness, prevention, and preparedness domains.
- NIMS facilitates the flow of (financial and physical) resources in pre-incident planning and post-incident execution.
- NIMS establishes a common operating picture that promotes useful information flow (Communications, Intelligence, and Information Management) at all levels of government.
- NIMS promotes the strategic development of new technologies and provides scientific support to enhance pre- and post-incident operations at all levels of government.

By December 31, 2003, all Federal departments and agencies shall adopt the NIMS within their departments and agencies and provide support and assistance to the Secretary in the development and maintenance of the NIMS. The Federal Agencies are currently reviewing the requirements under this Presidential Directive and providing input as necessary. This process will ultimately result in the development of a full NRP, including the NIMS, that ensures a national approach to domestic incident management and a process that places similar emphasis on awareness, prevention, and preparedness as traditionally has been placed on response and recovery.

Beginning in Fiscal Year 2005, Federal departments and agencies shall make adoption of the NIMS a requirement, to the extent permitted by law, for providing Federal preparedness assistance through grants, contracts, or other activities. The Secretary of Homeland Security will coordinate with the private and non-governmental sectors to ensure adequate planning, equipment, training, and exercise activities and to promote partnerships to address incident management capabilities and will also develop standards and guidelines for determining whether a State or local entity has adopted the NIMS.

## Suspicious Activities

Since most campuses are open to the public, it is important to always remain alert to any suspicious activities. Follow campus security procedures whenever such an event arises. When encountering a suspicious individual, make clear observations so you can record a physical description of the individual including any unique identifying features. If possible, document other pertinent information including vehicle description, license number and egress direction. **Never put yourself at risk.** Report the incident to either the campus police or local law enforcement agency immediately and write down everything you witnessed immediately;

REPORT THE FOLLOWING TO LAW ENFORCEMENT AUTHORITIES:

- ☞Suspicious activities, vehicles, or persons;
- ☞Missing chemicals, equipment, or critical blank document forms.
- ☞Break-ins



EPA United States Environmental Protection Agency New England

1 Congress Street, Suite 1100 SPP
Boston, MA 02114-2023
www.epa.gov/ne/assistance/univ/index.html

EPA 901-F-03-006
October 2003