

Site Security and Bio-terrorism¹

By

David R. MacKenzie,

Executive Director

Northeastern Regional Association of State Agricultural Experiment Station Directors (NERA)

INTRODUCTION

The Office of the Executive Director (OED) of the Northeastern Regional Association of State Agricultural Experiment Station Directors (NERA) is issuing this *Alert* as part of its ongoing effort to protect human health, agricultural production systems, and the environment. The nation is striving to learn the causes and contributing factors associated with bio-terrorism and to prevent their occurrence. Acts of bio-terrorism cannot be prevented solely through regulatory requirements and law enforcement. Rather, a sharing of understandings on the fundamental root causes, widely disseminating the lessons learned by others, and integrating these lessons learned into safe operations are also required.

It is important that State Agricultural Experiment Station (SAES) directors review this information and take appropriate steps to minimize bio-terrorism risks. This document does not substitute for federal or state regulations, nor is it a regulation itself. It is only advisory guidance. It does not impose any legally binding requirements on member institutions, or the surrounding community. And the suggested measures it describes may not, based upon circumstances, apply to your particular situation.

THE ISSUE

Because of today's increased concern about bio-terrorism and sabotage, public institutions are paying increased attention to the physical security of facility sites, storage areas, and research processes. All institutions, big and small, should have some measure of site security in place to minimize crime and to protect research assets. This is especially true for facilities that handle extremely hazardous substances.

But we need to remember that facilities that handle bio-hazardous materials have long needed to be actively engaged in managing the associated risks to ensure the safety of their workers and the community. Most of these ongoing efforts focus on ensuring that the facility is designed and operated safely on a day-to-day basis, using well-designed equipment, preventive maintenance, up-to-date operating procedures, and well-trained

¹ Based in part on a publication produced by the Environmental Protection Agency entitled "Chemical Accident Prevention: Site Security" www.epa.gov/ceppo/ February 2000. (EPA-K-550-F00-002)

staff. This fact contributes to an excellent base from which to plan bio-terrorism security measures.

PURPOSE

This document is intended as informational. It highlights security areas that State Agricultural Experiment Stations may want to review to ensure that appropriate measures are being implemented. More importantly, it provides sources of information and links to other sources to assist SAES directors that have faculty, staff and students that routinely handle bio-hazardous substances in their research efforts, so that they may have secure and accident-free operations.

TYPES OF THREATS

Aspect 1. Theft of hazardous materials: Many SAES laboratories must provide access to bio-hazardous materials so that their researchers may conduct their research activities. These materials may range from animal and plant pathogens to exotic or non-indigenous species. Some of these organisms may be human pathogens and are therefore registered with the Centers for Disease Control and Prevention (CDC) (see <http://www.cdc.gov/od/ohs/lrsat/42cfr72.htm#Appendix A>). Most of the bio-hazardous materials found at the typical SAES would not be registered with CDC. This presents a dilemma for SAES directors in that compiling inventories of bio-hazardous materials found at their station may invite theft. Additionally, databases that relate to research with bio-hazardous materials may attract “hackers”. Other terrorist groups that are interested in the destruction of certain types of research facilities (e.g., genetically modified organisms) may actually be helped by gaining access to your records and inventories. Thus, securing bio-hazardous materials, their records, and the facilities that contain them presents a challenge to us all.

It is recommended that carefully maintained records of bio-hazardous materials be maintained with adequate security. This record keeping is necessary to help investigators in the event that an attack should occur. But availability of those records to others should be carefully limited.

Aspect 2. Research Crops and Livestock as Targets: In addition to the possible theft or destruction of research facilities or research materials there is the threat that research plots and herds may become targets for terrorism. This may be especially true for research farms that are in close proximity to major interstate highways. The inoculation of livestock or crops with pathogens may represent a vulnerability that could be exploited by terrorist. This too needs to be evaluated.

However, from the viewpoint of likely targets a university research farm would seem to offer no more of a target that would a commercial farm operation. Thus, it seems unjustified to add security to a research plot or herd unless a plausible risk can be determined.

COMMON SECURITY MEASURES

Most research facility security measures are intended to prevent intruders from gaining access to the site or to limit the damage they might cause. The following sections present a number of design and procedural approaches that some research facilities have successfully implemented. The appropriateness of any one of these depends on site-specific conditions that you would need to consider in assessing any security needs for your facility.

PREVENTING INTRUSION

Most research facilities have some measures that are intended to prevent unauthorized intruders from entering farmlands or buildings. These measures may include fences, walls, locked doors, or alarm systems. The location of the facilities and the types of structures will determine how much and what type of protection a facility needs.

In addition to basic measures, some facilities also provide physical protection of site utilities at the fence perimeter. Security lighting (good lighting around buildings, storage tanks, and storage areas) can also make it very difficult for someone to enter the facility undetected.

Some facilities augment these measures with intrusion detection systems — video surveillance cameras, security guards at fixed posts, rounds/mobile patrols, alarm stations, and detectors for explosives and metal. If you have guards, it may be useful to consider augmenting their training in detection and response, and make available to them equipment for appropriate protective force.

To protect against unauthorized people coming in through normal entrances, security clearances, badges, procedures for daily activities and abnormal conditions, as well as vehicular and pedestrian traffic control, can provide efficient access for employees while ensuring that any visitors are checked and cleared before entering.

Most facilities have procedures to recover keys from employees who leave and to immediately remove the employee's security codes from systems. At times it may be wise to consider additional measures, such as changing locks, when a disgruntled employee leaves.

LIMITING DAMAGE

In addition to protecting a facility from intruders, it is important to limit the damage that an intruder (whether physically at the site or “hacking” into the station's computers) or an employee could do. Most of the steps to limit damage are probably things you already do as part of site security management, because they also limit the theft of supplies and equipment. These steps can be related to either the design of the facility and its processes or to procedures implemented.

Facility Design: A well-designed facility, by its layout, limits the quantity of biological material that could be released in the event of an accident or attack. Facility design and process design (including provisions for handling of biological materials) determine, in

turn, the need for safety equipment, site security, buffer zones, and mitigation planning. Eliminating or attenuating to the extent practicable any bio-hazardous characteristic during facility or process design is generally preferable to simply adding on safety equipment or security measures. But this may not be an option for many existing facilities. And retrofitting existing facilities may not be affordable.

The option of locating research with bio-hazardous materials into the center of a facility can thwart intruders and vandals who remain outside the facility fence line. Transportation vehicles, which are sometimes placarded to identify the contents, may be particularly vulnerable to attack if left near the fence line or unprotected. However, for some facilities and processes, the option of locating the entire process at the center of the site may not be feasible. You may need to consider external versus internal threats, such as the threat to workers if an accidental release occurs, or the access to the facility in case of an emergency.

Where feasible, providing layers of security may protect equipment from damage. These security layers could include, for example, blast resistant buildings or structures. Enclosing (e.g., behind fences or in buildings) critical valves, filters and pumps can make it less likely that an intruder will be able to reach them; that a vehicle will be able to collide with them; or that unintended releases are compounded because of damage to neighboring equipment.

HEPA filters are an example of equipment design that needs several layers of security. As many as three different tools should be needed by an intruder to breach the filter's integrity.

If bio-hazard-containing equipment is located where cars, trucks, forklifts, or construction equipment could collide with it or drop something on it, the equipment should be protected with a secure framework, or alternatively, constructed from materials that could stand some abuse. In general, you should give consideration to collision protection to any equipment containing bio-hazardous materials with, for example, collision barriers.

The idea of layers of security may also be applied to communications/computer security. Some private companies have developed alternate capabilities and systems to protect receipt and transmission of confidential information. Backup power systems and/or airconditioning systems can be important, particularly if processes are computer controlled. Access to computer systems used to control processes may need to be controlled so that unauthorized users cannot break in. Appropriate computer authentication and authorization mechanisms on all computer systems may be necessary. And entrance into controlled computer rooms may need to be monitored, and limited to authorized personnel only. For emergency communications, some institutions use radios and cell phones as a backup to the regular phone system.

Well-designed equipment will usually limit the loss of bio-hazardous materials, if part of a process fails. Excess-flow check valves, for example, will stop flow from an opened

valve if the design flow rate is exceeded. These valves are commonly installed on chlorine tank cars and some anhydrous ammonia trailers, as well as on many chemical processes. Fail-safe systems (like excess flow valve shutoffs) can ensure that if a biohazard release occurs, the valves and/or filters in the system will close, shutting off the escape. Breakaway couplings, for example, can be used to shut off flow in transfer systems, such as loading hoses, to limit the amount released to the quantity already in the hose.

If you store bio-hazardous materials, you may want to consider your containment systems. These should be designed in ways to slow the rate at which the contained material escapes, and thus provide time to respond. Double-walled vessels can protect against attempts to rupture a tank.

The installation of monitors that automatically notify personnel of off-hour releases could be important if your otherwise secure research facility is not staffed during certain periods (e.g., overnight). Such monitors, however, are not available for most biological materials and only a few chemicals. The appropriateness of monitors, and any other equipment design solutions, will depend on site-specific conditions as well.

Procedures and Policies

Your facility's policies and procedures can also limit the damage caused by a release. As with design issues, the procedural steps you routinely take to operate safely also help protect your facility from attacks. Maintaining good labor relations may protect your facility from actions by either employees or contractors. Open negotiations, workplace policies emphasizing that violence and substance abuse are not tolerated, and adequate training and resources to support these policies are important considerations. The goal is to develop a workforce and management capacity to identify and solve problems by working together. Following are some examples of specific areas where procedures and policies can prevent or limit the damage of a release.

1. As a matter of good practice, as well as site security, you may want to consider disconnecting storage tanks and delivery vehicles from connecting piping, transfer hoses, or distribution systems when not in use. Leaving the tanks linked to the process or pipeline increases the chance of a release because the hoses or pipes are often more vulnerable than the tanks.
2. In addition to accurately monitoring your inventory, another practice you may want to adopt is limiting the inventory of hazardous materials to the minimum you need for your process. This policy limits the quantity of a hazardous material that could be stolen or accidentally released. You could also consider actions such as substituting less hazardous substances when possible to make processes inherently safer.

Your written procedures are also an important tool in protecting your facility. As part of your regular operating procedures, you should probably have emergency shutdown procedures. These procedures, and workers trained in their use, can limit the quantity of biological material released. These procedures are particularly important if you have

processes that operate under extreme conditions (high or low pressures, temperature) where rapid shutdown can create further hazards if done improperly.

As you review your contingency plan, consider, if necessary, revisions that will address vandalism, bomb threats, and burglary - including an evaluation of the desirability of your facility as a target. Many universities have found that working with local law enforcement is an effective means of evaluating their security risks. This may be best done by providing planned security drills and professional biohazard security audits.

As a matter of good practice, for both research and emergency response equipment, it is important to have a program that ensures that all equipment is subject to inspection and to corrective and preventive maintenance. In this way, you can be sure that the safety systems you install will operate as designed.

SITE-SPECIFIC DECISIONS

The steps you take to operate safely will often serve to address security concerns as well. Considering inherent safety in the design and operation of any facility will have the benefit of helping to prevent and/or minimize the consequences of any release. Before taking steps to improve site security, you may want to evaluate your current system and determine whether it is adequate. Factors you might consider include:

- The types and amounts of bio-hazardous materials stored at your site, as some materials may be particularly attractive targets because of the potential for greater consequences if released.
- The location of the site, as sites in densely populated areas may need more security than those at a distance from populations.
- The accessibility of the site, as the existing security systems (e.g., fences, security lighting, security patrols) may not be adequate to limit access to the site.
- The age and type of buildings, as older buildings may be more vulnerable because they have more windows, and whereas some newer buildings are designed for easy access.
- Hours of operation, as a facility that operates 24-hours day may need less security than a facility that is unoccupied at night.

Decisions about improving site security should be made after evaluating how vulnerable your site is to threats and what additional measures, if any, are appropriate to reduce your vulnerability. Each station should make its own decision based on its circumstances.

SOME POINTS-TO-CONSIDER:

- The cost of providing adequate security should be balanced against the worth of the intended research. In these times of uncertain risks it may be a good choice to discontinue research activities that represent a major risk, if the site cannot be adequately secured.

- Some research projects can be conducted with “disarmed” organisms. During the early years of genetic engineering disarmed bacteria were the only organisms that were permitted under the National Institutes of Health’s biotechnology guidelines. By disarming the research organism, should a laboratory’s containment fail, the organism could not survive outside of containment.
- Alternate locations may be found to continue research activities that present a security threat. This might be an inconvenience for the moment, but might avoid a major consequence.
- You should eschew interviews with the popular press unless you are absolutely sure that your comments will be not only accurate, but assuring to the public as well. Any misstatements to the general public during a period of panic should be avoided. Likewise, any lack of sureness in your Experiment Station’s security might contribute to further panic.
- The right to participate in scientific research has shifted in recent times (a.k.a. 9/11) from an “unalienable right” to a privilege that needs to be carefully monitored. As an SAES director you have an obligation to assure public confidence that all participants in your Experiment Station’s research activities are legal, safe and fully accountable.

Regarding student visa compliance, any public institution has an obligation to monitor immigration compliance, albeit with sufficient safeguards that constitutional and civil rights are not violated. Some universities are participating in a model program with the U.S. Immigration and Naturalization Service to identify students not in compliance with visa requirements. But many other universities are not involved in immigration enforcement whatsoever. This presents a dilemma to a responsible SAES director in that should something go wrong that involves an undocumented graduate student, recriminations will no doubt fly. Thus, a word of advice. Be alert.

INFORMATION SOURCES

Web Sites:

www.asmta.org/pcsrc/bioprep.htm

The American Society of Microbiology’s Office of Public Affairs and their Office of Communications have prepared a compendium of online resources and information relevant to Biological Weapons Control and Bio-terrorism Preparedness issues. The new site will be updated as additional information becomes available.

www.nsc.org

The National Safety Council provides general safety information on chemical and environmental issues.

www.asisonline.org

www.securitymanagement.com

The American Society for Industrial Security develops educational programs and materials that address security concerns. Its Security Management Magazine site provides an online version of its magazine.

www.siaonline.org

The Security Industry Association provides general security information.

www.atsdr.cdc.gov

The Agency for Toxic Substances and Disease Registry site provides a 10-step procedure to analyze, mitigate, and prevent public health hazards resulting from terrorism involving industrial chemicals and infectious agents.

www.aiche.org/ccps

The Center for Chemical Process Safety (CCPS) is an industry-driven, non-profit professional organization affiliated with the American Institute of Chemical Engineers (AIChE). It is committed to developing engineering and management practices to prevent or mitigate the consequences of catastrophic events involving the release of chemicals that could harm employees, neighbors and the environment.

www.cdc.gov/niosh

The National Institute for Occupational Safety and Health provides multiple resources on workplace violence prevention.

Publications:

The Complete Manual of Corporate and Industrial Security, by Russell L. Bintliff (Prentice Hall, 1992) provides detailed discussions of the advantages and disadvantages of various security systems as well as checklists for security inspections.

The Handbook of Loss Prevention and Crime Prevention, 3rd Edition, L.J. Fennelly, Ed., (Butterworth-Heinemann, 1996) includes information on conducting security surveys as well as chapters on a broad range of security subjects.

Guidelines for Investigating Chemical Process Incidents. (AIChE/CCPS). These Guidelines establish a basis for successful investigation of process incidents to determine causes and implement changes, which can prevent recurrence. Primary focus is on incidents with catastrophic potential but the concepts should also be used for investigating environmental incidents, minor injuries, less significant property damage events, or near misses.

Process Plants: A Handbook for Inherently Safer Design, by Trevor Kletz. (Taylor & Francis 1998) illustrates the principles of inherent safety and demonstrates the advantages of considering safety approaches in the design stages of a process.

Inherently Safer Chemical Processes: A Life Cycle Approach. (AIChE/CCPS) This book presents the principles and strategies for applying inherently safer thinking from the start of the life cycle to the very end.