FAS: Threat Assessment

Threat assessment

Threats may be actual or perceived, and may relate to past incidents, current facility conditions, or postulated event scenarios. Identifying all possible threats and their likelihood is crucial to the overall success of the security plan.

Primary threat categories

The primary threat to the laboratory and building occupants are by intrusion to perform theft, physical attack, vandalism, or sabotage.

Any of these threats can be planned and executed by persons within the building or organization who have some degree of approved access to the facility, or by persons external to the organization that are able to gain access into the facility or onto the building site.

The most common threat types are terrorism, criminal, environmental, infrastructure failure, or service interruption.

Intrusion

The laboratory has taken reasonable steps for the protection of the facilities from intrusion by employing the following precautions:

- exterior lighting and signage
- fence surrounding the property
- controlled access hardware, software, and camera system supported by procedures to control entry of individuals
  - onto the laboratory site
  - at the main lobby and criminalist entrance doors
  - at the vehicle entrance/exit gates into parking areas
  - at the shipping and receiving entrance
- landscaping design that allows clear unobstructed views around the building
- an electronic data system that monitors, records, and controls all doors and allows flexibility to change the limits of access to any function or space for any person at any time

Continued on next page

FAS: Threat Assessment, Continued

Terrorism threats

Types of terrorism threats and characteristics

Threat Type	Characteristic
Explosive	• vehicle outside the site perimeter • vehicle within the site perimeter, adjacent to the building • mail, package, or supply bombs
Forced entry	• at the site perimeter • at the building exterior • at internal laboratory space
Weapons	• use of firearms
Chemical, biological and radiological weapons, and agents	• airborne contamination external to the facility • airborne contamination internal to the facility
Visual, acoustic, and electronic surveillance	• cameras, wiretaps, computer hacking
Aerial attack	• airplanes as weapons or delivering weapons

Criminal threats

Criminal threats may be identified as

- theft of evidence, personal property and information
- assault
- vandalism
- protestors
- employees and workplace violence
- forged identifications
- arson
- kidnapping and hostage taking

Continued on next page

FAS: Threat Assessment, Continued

Environmental threats

Environmental threats may be identified as

- fire
- earthquakes
- floods
- chemical or biohazard spills

Infrastructure or service interruption threats

Infrastructure refers to the underlying critical support utilities for a facility, loss of which would result in mission failure, and loss of security protection. Infrastructure failure or service interruption threats my be identified as

- electrical systems – routine service, emergency generator , or UPS power
- cooling systems
- heating systems
- water supply disruption or contamination
- telecommunications
- natural gas

Continued on next page

FAS: FAS: Threat Assessment, Continued

Threat remediation

In the event of a threat, a threat mediation plan will be developed.

The intent of threat remediation is to note all physical elements and evaluate them against types of threats, determine potential security vulnerabilities, and take corrective action to remediate the threat.

A successful threat remediation plan ensures that all aspects of the threat are investigated and are the result of a collaborative effort among laboratory management, laboratory staff, county telecommunications, county general services, and the District Attorney's Investigations Bureau.

Components of a threat remediation plan include

- formulating options and potential solutions
- coordinating efforts
- providing flexibility for change, special circumstances, one time situations, or occasional events
- assessing capital and operational costs of all options
- determining priorities and phasing plan as needed

The Laboratory Director is responsible for ensuring that threat remediation efforts are successfully concluded.