

University of Washington RBL

Project # X35320

December 22, 2004

1. Project Description and Intent

The intent of this document is to describe contemplated security measures for the University of Washington Regional Biocontainment Laboratory (RBL) that will operate at the South Campus site.

Threats to the Lab:

- Criminal threats to include terrorist attacks, acts of aggression/vandalism by animal rights extremists or genetic-testing opponents, theft by employees/authorized visitors
- Accidents

Goals of the Security Plan:

- Ensure employee safety
- Ensure public safety
- Complement sound laboratory procedures by providing an efficient, user-friendly security system
- Deter criminal acts and minimize the impact of such an act
- Deter acts of employee/visitor misconduct
- Compliance with the NIH physical security requirements.

2. Security Standards and Requirements

2.1 References

- The National Institutes for Health (NIH) Physical Security Guidelines for NIAID National and Regional Biocontainment Laboratories (RBL), latest edition.
- Interagency Security Criteria (ISC) for New Federal Office Buildings and Major Modernization Projects, latest edition

2.2 Synopsis of Standards and Requirements

Security System Requirements: Biocontainment facilities and research support laboratories must be designed to maximize safety in the work space and surroundings. Stringent security and access control must be provided for the building and coordinated with existing security system infrastructure and operations, as appropriate. The NIAID's primary security objectives for the program are the safety and protection of the general public and environment, security of the select agents, and preserving the integrity of biocontainment. The safety and security of personnel; protection of the property, research and animals; and potential damage or destruction to the facility, must all be addressed. It is the awardee's responsibility to ensure that these objectives are satisfied. In preparation for submitting an application, the applicant institution should conduct a preliminary security assessment to be utilized in developing security measure for the proposed building.

Post-award, each grantee will be required to perform a site-specific and project-specific Threat and Risk Assessment (TRA) to develop a security plan in accordance with a statement of work provided by Associate Director for Security and Emergency Response (ADSER) through the NIAID. This TRA shall include using the services of a qualified TRA professional. The TRA will become the basis for addressing individual security issues. The TRA should identify and quantify potential threats, both internal and external to the building, its contents, the personnel working in it, and the general public. The analysis should include a thorough examination and evaluation of the physical aspects of the proposed facility, along with operational issues. Based on the TRA, the awardee shall establish security measures to ensure that the security objectives of the NIAID's National Biodefense Program are achieved. A copy of the TRA along with a list of the proposed security measures shall be submitted to the NIAID.

The security measures, as established by the TRA, for each will be incorporated into the design and operation plan for the facility. The NIAID will review these documents during the regular design submittals for compliance. NIAID also will monitor construction and the certification process for conformance with the security measures established by the awardee to assure the facility is safe and secure when completed and in operation.

- **The NIH also offer the following Biosafety in Biomedical and Microbiological Laboratories (BMBL) security guidelines.**

The following are offered as guidelines for laboratories using biological agents or toxins capable of causing serious or fatal illness to humans or animals. However, research, clinical, and production laboratories working with newly identified human pathogens, high-level animal pathogens, and/or toxins not covered by BSL-3 or -4 recommendations, should also follow these guidelines to minimize opportunities for accidental or intentional removal of these agents from the laboratory.

- 1. Recognize that laboratory security is related to but different than laboratory safety.**
 - Involve both safety and security experts in evaluation and development of recommendations for a given facility or laboratory.
 - Review safety policies and procedures regularly. Management should review policies to ensure that they are adequate for current conditions and consistent with other facility-wide policies and procedures. Laboratory supervisors should ensure that all laboratory workers and visitors understand security requirements and are trained and equipped to follow established procedures.
 - Review safety policies and procedures whenever an incident occurs or a new threat is identified.
- 2. Control access to areas where biologic agents or toxins are used and stored.**
 - Laboratories and animal care areas should be separate from the public areas of the buildings in which they are located.
 - Laboratory and animal care areas should be locked at all times
 - Card-keys or similar devices should be used to permit entry to laboratory and animal care areas.
 - All entries (including entries by visitors, maintenance workers, repairmen and others needing one-time or occasional entry) should be recorded, either by the card-key device (preferable) or by signature in a log book.

- Only workers required to perform a job should be allowed in laboratory areas, and workers should be allowed only in areas and at hours required to perform their particular job.
 - a. Access for students, visiting scientists, etc., should be limited to hours when regular employees are present.
 - b. Access for routine cleaning, maintenance, and repairs should be limited to hours when regular employees are present.
 - Freezers, refrigerators, cabinets, and other containers where stocks of biological agents, hazardous chemicals, or radioactive materials are stored should be locked when they are not in direct view of workers (e.g., when located in unattended storage areas).
- 3. Know who is in the laboratory area.**
- All workers should be known to facility administrators and laboratory directors. Depending on the biological agents involved and the type of work being done, a background check and/or security clearance may be appropriate before new employees are assigned to the laboratory area.
 - All workers (including students, visiting scientists, and other short-term workers) should wear visible identification badges. Identification badges should include, at a minimum, a photograph, the wearer's name, and an expiration date. It may be useful to use colored markers or other easily recognizable design symbols on the identification badges to indicate clearance to enter restricted areas (e.g., BSL-3 or -4 laboratories, animal care areas).
 - Guests should be issued identification badges, and escorted or cleared for entry using the same procedures as for regular workers.
- 4. Know what materials are being brought into the laboratory area.**
- All packages should be screened (visually) before being brought into the laboratory area.
 - Packages containing specimens, bacterial or virus isolates, or toxins should be opened in a safety cabinet or other appropriate containment device.
- 5. Know what materials are being removed from the laboratory area.**
- Biological materials/toxins for shipment to other laboratories should be packaged and labeled in conformance with all applicable local, federal, and international shipping regulations.(9)
 - a. Required permits (e.g., PHS, DOT, DOC,) should be in hand before materials are prepared for shipment.
 - b. The recipient (preferably) or receiving facility should be known to the sender, and the sender should make an effort to ensure that materials are shipped to a facility equipped to handle those materials safely. Hand-carrying of microbiological materials and toxins to other facilities is rarely appropriate. If biological materials or toxins are to be hand carried on common carriers, all applicable regulations must be followed.
 - Contaminated or possibly contaminated materials should be decontaminated before they leave the laboratory area. Chemicals and radioactive materials should be disposed of in accordance with local, state, and federal regulations.
- 6. Have an emergency plan.**
- Control of access to laboratory areas can make an emergency response more difficult. This must be considered when emergency plans are developed.

- a. An evaluation of the laboratory area by appropriate facility personnel, with outside experts if necessary, to identify both safety and security concerns should be conducted before an emergency plan is developed.
 - b. Facility administrators, laboratory directors, principal investigators, laboratory workers, the facility safety office, and facility security officials should be involved in emergency planning.
 - c. Police, fire, and other emergency responders should be informed as to the types of biological materials in use in the laboratory areas, and assisted in planning their responses to emergencies in the laboratory areas.
 - d. Plans should include provision for immediate notification of (and response by) laboratory directors, laboratory workers, safety office personnel, or other knowledgeable individuals when an emergency occurs, so they can deal with biosafety issues if they occur.
- Laboratory emergency planning should be coordinated with facility-wide plans. Such factors as bomb threats, severe weather (hurricanes, floods), earthquakes, power outages, and other natural (or unnatural) disasters should be considered when developing laboratory emergency plans.
- 7. Have a protocol for reporting incidents.**
- Laboratory directors, in co-operation with facility safety and security officials, should have policies and procedures in place for reporting and investigation of incidents or possible incidents (e.g., undocumented visitors, missing chemicals, unusual or threatening phone calls).

2.3 Preliminary Specific Facility Security Assessment and Requirements

The security of the University of Washington RBL shall consist of technical security systems supporting the operational staff in executing the requisite security level at this facility.

The University of Washington RBL Security Management System shall be utilized to cover this new RBL facility. The system shall provide access control with proximity technology, intrusion detection and video surveillance systems for this facility. The monitoring of these systems shall be executed and managed from the Security Monitoring and Reception areas at the main entry to the building. There will be a need for a University of Washington Security Management System workstation to be located in the security monitoring room of the facility to provide facility control of access rights management. The biometric data that is captured by the University of Washington Security will be transferred to the RBL Security Management System computer via a CD which is hand delivered.

As required by the NIH, all workers (including students, visiting scientists, and other short-term workers) should wear visible identification badges. Identification badges should include, at a minimum, a photograph, the wearer's name, and an expiration date. It is envisioned that Health Sciences standard photo ID will be utilized.

As required by the NIH guidelines, all personal packages should be screened before being brought into the laboratory. All package deliveries will be handled through the dock. It is envisioned that physical inspections shall be executed at the entrance of the building, prior to passage through the Sally Port.

The technical security systems of the University of Washington RBL consist of four basic zones of protection:

- "0" for the entry
- "1" for the open office areas
- "2" for mechanical space
- "3" Labs and all locations of select agents

2.3.1 The Entry

The outer perimeter consists of the area outside the laboratory, but immediately adjacent to the laboratory and clean corridor. This area should be the location for screening the packages exiting the laboratory area. There should be video cameras viewing and recording the entry doors into the laboratory.

2.3.2 The Open Office Areas

Access into the Open Office Areas shall require an authorized proximity card. There should be a card reader at each of the entrances from the corridor. Within the corridor there should be video cameras providing general surveillance of the traffic in the corridor.

2.3.3 The Mechanical Space

Access into the mechanical, dock and support areas shall require an authorized proximity card. There should be a card reader at each of the doors to these areas.

2.2.4 The Specific Interior Labs and All Locations of Select Agents

From the Clean Corridor, there should be biometric and proximity combination access control card readers controlling access into each of the specific restricted access areas.

- a) BSL-2
- b) BSL-3
- c) ABSL-3
- d) Select Agent
- e) Labs

There should be a card reader in and card reader out controlling access into each of the Ante-Room and Changing Room doors from the Clean Corridor. The biometric readers should be controlling the interior doors leading from the Ante-Rooms and Changing Rooms into the Preparation or Lab rooms. In addition to the card readers, there should be door contacts on each of the doors to provide for intrusion detection. There should be video surveillance of each of the select agent storage areas, preparation rooms, labs and animal rooms. The video system shall be provided with video motion detection for intrusion detection. There should also be a duress button in each of the areas.

3. Estimate of Probable Cost

The below estimate include the installation of the above described system, including cable, conduit, training and programming to initialize the system.

Project: <i>University of Washington RBL</i> Project No.: <i>X35320</i> Site: <i>Seattle, WA</i> Type: <i>Summary</i> Date: <i>December 21, 2004</i> Submission: <i>Preliminary Estimate</i> Proj. Manager: <i>LVF</i> Equip. Contingency <i>10%</i> Sales Tax <i>7.00%</i> Installation RT/HR <i>\$85</i> Supervision RT/HR <i>\$95</i> Training RT/HR <i>\$100</i>				
Item	Abr/Acr	System Description	Cost	Percent
1	ACMS	ACCESS CONTROL AND ALARM MONITORING	\$306,113	70.1%
2	CCTV	CLOSED CIRCUIT TELEVISION SYSTEM	\$130,712	29.9%
SECURITY SYSTEMS TOTAL			\$436,825	100%

Item	Quantity	System Description	Unit	Unit Ext	Labor	Labor Ext
1	1	ACCESS CONTROL SERVER	\$ 3,500.00	\$ 3,500	8.00	8.00
2	1	NETWORK EQUIPMENT	\$ 500.00	\$ 500	2.00	2.00
3	2	WORKSTATION/ADMINISTRATIVE	\$ 2,500.00	\$ 5,000	4.00	8.00
4	1	CCTV INTERFACE	\$ 1,000.00	\$ 1,000	8.00	8.00
5	12	MULTIPLEX FIELD PANEL	\$ 3,500.00	\$ 42,000	4.00	48.00
6	12	MFP POWER SUPPLY	\$ 250.00	\$ 3,000	1.00	12.00
7	50	LOCK POWER SUPPLY	\$ 50.00	\$ 2,500.00	1.00	50.00
8	50	ELICTRIFIED HARDWARE	\$ 650.00	\$ 32,500.00	4.00	200.00
9	500	MULTITECHNOLOGY CARD	\$ 5.00	\$ 2,500		
10	25	CARD READER w/PIN	\$ 575.00	\$ 14,375	1.00	25.00
11	25	CARD READER/PROXIMITY	\$ 500.00	\$ 12,500	1.00	25.00
12	5	REQUEST TO EXIT	\$ 110	\$ 550	0.50	2.50
13	25	DOOR POSITION SWITCH/FLUSH	\$ 25	\$ 625	0.50	12.50
14	6	DURESS BUTTON/WALL	\$ 80	\$ 480	0.50	3.00
15	1	PACKAGE SCREENING DEVICE	\$ 50,000	\$ 50,000	24.00	24.00
16	1	WALK THROUGH METAL DETECTOR	\$ 6,000	\$ 6,000	1.00	1.00
17	1	CONDUIT	\$ 18,000	\$ 18,000	3.00	3.00
18	3000	Wire And Cable	\$ 0	\$ 600	0.02	60.00
TOTAL EQUIPMENT				\$ 195,630		
EQUIPMENT CONTINGENCY				\$19,563		
SALES TAX				\$15,064		
EQUIPMENT SUBTOTAL				\$230,257		
FIELD INSTALLATION LABOR RATE/HR				\$85		
FIELD INSTALLATION LABOR HOURS				492.00		
FIELD INSTALLATION SUBTOTAL				\$41,820		
PROJ. MANG, ENG. & SUPERVISION RATE/HR				\$95		
PROJ. MANG. AND ENGINEERING HOURS				73.8		
FORMAN SUPERVISION HOURS (10% Labor Hours)						
PROJ. MANG. AND ENGINEERING SUBTOTAL				\$7,011		
TRAINING AND DATABASE INIT. RATE/HR				\$100		
TRAINING AND DATABASE INIT. HOURS				40		
TRAINING AND DATABASE INIT. SUBTOTAL				\$4,000		
MISC. SHOP FABRICATION COST				\$23,026		
TOTAL SYSTEMS COST				\$306,113		

Item	Quantity	System Description	Unit	Unit Ext	Labor	Labor Ext
1	1	VIDEO MATRIX SWITCHER CARD CAGE	\$ 2,800.00	\$2,800	1.00	1.00
2	2	VIDEO MATRIX SWITCHER INPUT CARD (16)	\$ 1,500.00	\$3,000	8.00	16.00
3	1	VIDEO MATRIX SWITCHER OUTPUT CARD (32)	\$ 1,200.00	\$1,200	2.00	2.00
4	1	VIDEO KEYBOARD REMOTE POWER SUPPLIES	\$ 400.00	\$400	1.00	1.00
5	1	VIDEO KEYBOARD	\$ 1,500.00	\$1,500	1.00	1.00
6	1	CODE GENERATOR	\$ 1,600.00	\$1,600	1.00	1.00
7	2	DIGITAL VIDEO RECORDER 16 CAMERA	\$ 15,000.00	\$30,000	4.00	8.00
8	28	CAMERA POWER SUPPLY	\$ 50.00	\$1,400	0.50	14.00
9	4	14" COLOR MONITOR	\$ 4,500.00	\$18,000	2.00	8.00
10	1	20" COLOR MONITOR	\$ 2,000.00	\$2,000	1.00	1.00
11	28	Dome Camera & Housing	\$ 1,300.00	\$36,400	1.00	28.00
12	1000	Wire	\$ 0.50	\$500	0.02	20.00
TOTAL EQUIPMENT				\$98,800		
EQUIPMENT CONTINGENCY				\$9,880		
SALES TAX				\$7,608		
EQUIPMENT SUBTOTAL				\$116,288		
FIELD INSTALLATION LABOR RATE/HR				\$85		
FIELD INSTALLATION LABOR HOURS				101.00		
FIELD INSTALLATION SUBTOTAL				\$8,585		
PROJ. MANG, ENG. & SUPERVISION RATE/HR				\$95		
PROJ. MANG. AND ENGINEERING HOURS				15		
FOREMAN SUPERVISION HOURS (10% Labor Hours)						
PROJ. MANG. AND ENGINEERING SUBTOTAL				\$1,439		
TRAINING AND DATABASE INIT. RATE/HR				\$100		
TRAINING AND DATABASE INIT. HOURS				24		
TRAINING AND DATABASE INIT. SUBTOTAL				\$2,400		
MISC. SHOP FABRICATION COST				\$2,000		
TOTAL SYSTEMS COST				\$130,712		