SCOPE OF WORK

Security Upgrade Study

NJ Public Health Environmental and Agricultural Laboratory
Ewing, Mercer County, N.J.

Project No. A1359-00

STATE OF NEW JERSEY

Honorable Philip D. Murphy, Governor
Honorable Sheila Y. Oliver, Lt. Governor

DEPARTMENT OF THE TREASURY

Elizabeth Maher Muoio, Treasurer

DIVISION OF PROPERTY MANAGEMENT AND CONSTRUCTION

Christopher Chianese, Director

Date: December 6, 2021

Document Format Revision 5-26-21

TABLE OF CONTENTS

SECTION **PAGE**

I. OBJECTIVE

The objective of this project is to study the existing security systems at the New Jersey Public Health Environmental and Agricultural Laboratory in Ewing, New Jersey and provide a plan with cost estimates to upgrade the current hardware, software, protocols and biometric components at the site.

II. CONSULTANT QUALIFICATIONS

A. CONSULTANT & SUB-CONSULTANT PRE-QUALIFICATIONS

The Consultant shall be a firm pre-qualified with the Division of Property Management & Construction (DPMC) in the following discipline(s):

- **P048 Security Systems**

The Consultant shall also have in-house capabilities or Sub-Consultants pre-qualified with DPMC in:

- **P025 Estimating/Cost Analysis**

As well as, **any and all** other Architectural, Engineering and Specialty Disciplines necessary to complete the project as described in this Scope of Work (SOW).

III. PROJECT BUDGET

A. PROJECT COSTS

The Consultant shall determine the construction cost estimate (CCE) and current working estimate (CWE) for each recommended facility improvement. Project cost items shall include, but not be limited to: construction costs, Consultant design and construction administration fees, Construction Management Firm (CMF) fees (if recommended), testing costs, DPMC management fees, contingencies, permits, allowances, and escalation factors for the anticipated construction year of the recommended facility improvement.

B. PROFESSIONAL COST ESTIMATOR

The Consultant or Sub-Consultant developing the cost estimates must be pre-qualified with DPMC in the P025 Estimating/Cost Analysis Professional Discipline and demonstrate that they have experience in the preparation of cost estimates for Facility Condition Assessments that are similar in size and scope to that described in this document. A description of at least three (3)

similar projects completed by their firm shall accompany the technical proposal for evaluation by the Consultant Selection Committee.

All cost estimates shall be adjusted for regional location, site factors, construction phasing, and building use group, location of work within the building, temporary swing space, security issues, and inflation factors based on the year in which the work is to be performed.

All cost estimates must be submitted on a DPMC-38 Project Cost Analysis form for each recommended facility improvement along with a detailed construction cost analysis in CSI format for all appropriate divisions and sub-divisions.

C. CONSULTANT'S FEES

The construction cost estimate for this project ***shall not*** be used as a basis for the Consultant's fees. The Consultant's fees shall be based on the information contained in this Scope of Work document and the observations made and/or the additional information received during the pre-proposal meeting.

IV. PROJECT SCHEDULE

A. SCOPE OF WORK DESIGN & CONSTRUCTION SCHEDULE

The following schedule identifies the estimated design and construction phases for this project and the estimated durations.

PROJECT PHASE	ESTIMATED DURATION (Calendar Days)
1. Site Access Approvals & Schedule Kick-off Meeting	**14**
2. Security Upgrade Study Phase	**90**
• *Project Team & DPMC Plan/Code Unit Review & Comment*	14
3. Initial Reporting Phase - 50% Completion	**21**
• *Project Team & DPMC Plan/Code Unit Review & Comment*	14
4. Final Reporting Phase - 100% Completion	**21**
• *Project Team & DPMC Plan/Code Unit Review & Comment*	14
5. Close-Out Phase	**14**
TOTAL	**202**

For scheduling purposes, a two (2) week period has been allotted for the review of each submission by the Project Team, after which a meeting will be convened to discuss all comments with the Consultant. However, any delays caused by the Project Team's review process shall not be sufficient reason for additional compensation to the Consultant.

It is specifically noted herein that the document review process by the Project Team or its representatives is intended to be a review of the documents in a general manner. Submission reviews and comments by the Project Team or its representatives shall not be construed as a comprehensive review or detailed checking of the Consultant's work. It remains the Consultant's professional responsibility to prepare the documents in accordance with proper engineering criteria and sound professional engineering judgment. The Consultant is completely responsible for all documents they and their Sub-Consultants prepare and it remains the Consultant's responsibility to ensure the integrity of the analysis and their work.

B. CONSULTANT PROPOSED STUDY SCHEDULE

The Consultant shall submit a project bar chart schedule with its technical proposal that is similar in format and detail to the schedule depicted in **Exhibit 'A'**. The bar chart schedule developed by the Consultant shall reflect its recommended project phases, phase activities, activity durations.

The Consultant shall estimate the duration of the project Close-Out Phase based on the anticipated time required to complete each deliverable identified in Section XI of this document entitled "Contract Deliverables - Project Close-Out Phase" and include this information in the bar chart schedule submitted.

A written narrative shall also be included with the technical proposal explaining the schedule submitted and the reasons why and how it can be completed in the time frame proposed by the Consultant.

This schedule and narrative will be reviewed by the Consultant Selection Committee as part of the evaluation process and will be assigned a score commensurate with clarity and comprehensiveness of the submission.

C. CONSULTANT STUDY SCHEDULE

Based on the Notice to Proceed, Consultant shall update its approved schedule and shall distribute it at the kickoff meeting. Note that this schedule shall be submitted in both paper format and on compact disk in a format compatible with *Microsoft Project*. This schedule will be binding for the Consultant's activities and will include the start and completion dates for each activity. The Consultant and Project Team members shall use this schedule to ensure that all milestone dates are being met for the project. The Consultant shall update the schedule to reflect performance periodically (minimally at each phase) for the Project Team review and approval.

Any recommendations for deviations from the approved schedule must be explained in detail as to the causes for the deviation(s) and impact to the schedule.

V. PROJECT SITE LOCATION & TEAM MEMBERS

A. PROJECT SITE ADDRESS

The location of the project site is:

NJ Public Health Environmental and Agricultural Laboratory
3 Schwarzkopf Drive
West Trenton, NJ 08628

See **Exhibit 'B'** for the project site location map.

B. PROJECT TEAM MEMBER DIRECTORY

The following are the names, addresses, and phone numbers of the Project Team members.

1. DPMC Representative:

Name:	Joseph Polizzi, Design Project Manager
Address:	Division of Property Management & Construction 20 West State Street, 3rd Floor Trenton, NJ 08608-1206
Phone No:	(609) 218-0260
E-Mail No:	Joseph.Polizzi@treas.nj.gov

2. NJ Department of Health:

Name:	Kevin Jennings, Director, Office of Administrative Services Division of Management and Administration
Address:	New Jersey Department of Health 55 North Willow Street – 1st Floor Trenton, NJ 08608
Phone No:	(609) 376-8651
E-Mail No:	Kevin.Jennings@doh.nj.gov

3. NJ Public Health Environmental and Agricultural Laboratory:

Name:	David Markunas, Facilities Operations Manager
Address:	NJ Public Health Environmental and Agricultural Laboratory 3 Schwarzkopf Drive West Trenton, NJ 08628
Phone No:	609-406-6864
E-Mail No:	david.markunas@treas.nj.gov

VI. PROJECT DEFINITION

A. BACKGROUND

The New Jersey Public Health, Environmental and Agricultural Laboratory (PHEAL) is a five story steel framed building that houses the Department of Health and the Department of Agriculture's laboratories. The PHEAL is located on the same campus as the New Jersey State Police Division Headquarters and Regional Operations Intelligence Center (NJ ROIC)

The PHEAL is seeking an upgrade of its building security systems, emphasizing modernization/update/replacement of current hardware and software, protocols and biometric components.

B. FUNCTIONAL DESCRIPTION OF THE BUILDING

1. General:

The facility (PHEAL) is a 191,000 sf building comprised of 157,000 sf of open laboratory space. Initially opened in May 2011, services were gradually moved from the old facility in Trenton over the course of approximately one year, with the last program to move in August 2012. Drawings were completed under Project A0984-04 and will be provided to the Consultant.

The Department of Health is the largest tenant in the building followed by the Department of Agriculture. The smallest tenant is the Department of Environmental Protection.

Office space for the Department of Environmental Protection's (DEP) Bureau of Air Monitoring and Pesticide Evaluation and Monitoring was created under Project A1246-01 to allow for relocation of these functions from leased space. Drawings will be provided to the Consultant.

Department of Health (DOH) services within the facility include Public Health Laboratory Services (PHLS), Environmental Chemical Laboratory Services (ECLS), Office of Policy,

Planning and Regulatory Compliance (OPPRC) and the Clinical Laboratory Improvement Services (CLIS).

Department of Agriculture Laboratory Services within the facility include Animal Health Laboratory Services and Plant Industry Laboratory Services.

2. Biological Safety Levels (BSL):

Biosafety levels (BSL) are used to identify the protective measures needed in a laboratory setting to protect workers, the environment, and the public. The four biosafety levels are BSL-1, BSL-2, BSL-3, and BSL-4, with BSL-4 being the highest (maximum) level of containment. There are no BSL-4 laboratories at the PHEAL Lab. The facility has had challenges with some of the BSL-3 laboratories and air lock systems. Personnel have gotten stuck in these areas due to improper functioning of the security system and had to be released via manual override.

3. Mass Notification System:

The State Police have a mass notification system from ATI Systems that uses redundant communications, UHF radio frequency and IP communication to provide emergency communication for the New Jersey State Police Division Headquarters and Regional Operations Intelligence Center (NJ ROIC) on the campus. The PHEAL would like to be integrated into this system.

Pursuant to this goal, the PHEAL reached out to a vendor for a proposal. This proposal is shown in **Exhibit 'C'** and describes how the system would work. The proposal is provided for background. No further action on the proposal was taken. It was decided that the best approach would be a mass notification system that would be integrated with other security upgrades as recommended in this project prior to integrating with the State Police.

VII. CONSULTANT RESPONSIBILITIES

A. GENERAL INFORMATION

This section of the Scope of Work is intended as a guide for the Consultant to understand the overall basic requirements of the project and is not intended to identify each specific component of the facility condition assessment. It will be the Consultant's responsibility to provide all of the required detail necessary to complete a comprehensive security upgrade study that will provide a context that will allow decisions to be made when resource improvements are required based on the Client Agency needs or other factors.

The consultant must be familiar with and knowledgeable of all aspects of the anticipated services and have a thorough understanding of the project requirements, including all applicable codes and regulations.

The Consultant shall ensure that all of the requirements identified in this section of the scope of work are addressed and included in the final security upgrade study where appropriate.

B. PROJECT COMMENCEMENT

A pre-study meeting shall be scheduled with the Consultant and the Project Team members at the commencement of the project to obtain and/or coordinate the following information:

1. Project Directory:

Develop a project directory that identifies the name and phone number of key designated representatives who may be contacted during this project.

2. Site Access:

Develop procedures to access the project site and provide the names and phone numbers of approved escorts when needed

3. Project Coordination:

Review and become familiar with any current and/or future projects at the site that may impact the scheduling requirements of this project.

4. Existing Documentation:

Copies of the following documents will be provided to each Consulting firm at the pre-proposal meeting to assist in the bidding process.

- DPMC Project A0984-04: **New Jersey Public Health Environmental and Agricultural Laboratory,** January 28, 2011, HOK NY
- DPMC Project A1246-01: **New Jersey Public Health Environmental and Agricultural Laboratory** (New Laboratory and Office Renovations), 10/15/2019, HDR Architects and Engineers P.C.

Review these documents and any additional information that may be provided at a later date such as reports, studies, surveys, equipment manuals, as-built drawings, etc. The State does not attest to the accuracy of the information provided and accepts no responsibility for the consequences of errors by the use of any information and material contained in the documentation provided. It

shall be the responsibility of the Consultant to verify the contents and assume full responsibility for any determination or conclusion drawn from the material used. If the information provided is insufficient, the Consultant shall take the appropriate actions necessary to obtain the additional information required.

All original documentation shall be returned to the provider at the completion of the project.

5. Scope of Work:

Review the administration responsibilities and the submission requirements identified in this Scope of Work with the Project Team members. Items such as: special hours for the study based on Client Agency programs or building occupancy and security needs at the site shall be addressed.

6. Project Schedule:

Review and update the project schedule with the Project Team members.

C. DATA GATHERING & INTERVIEWS

The Consultant shall meet with the Project Team Members and representatives of the PHEAL to schedule the site visits and approve the procedures necessary to assess the site and security systems and related equipment.

Surveys, measurements, photographs and other data collection methods shall be performed in such a way to minimize disruption to the building occupants and operation of the facility. A structured process shall be developed that will document the condition of each facility component assessed.

D. SECURITY UPGRADE STUDY REQUIREMENTS

1. Areas of Concern:

In general, a new security system in and around the building shall address the following physical and surveillance security measures. Areas of concern are as follows:

Restricted access and/or controlled access by Security regarding gate arms and loading dock(s).

Restricted access and/or controlled access by Security to all exterior portals to main building and out-buildings.

Restricted access to specific laboratories or other areas of the laboratories.

Heightened security devices/measures and restricted access to Biosafety Level (BSL3) laboratories and/or Registered Spaces

Supported software for programming access cards including to BSL3 and Registered Spaces.

Compatible Cameras and other hardware for printing IDs.

Software which allows Security at central station to track/monitor all mobility activities among Lab employees.

Inclusion of compatible Visitor Management System used daily by Security for recording and historical references.

System which promotes and facilitates all recorded surveillance from motion sensor cameras for specific time periods.

Integration with the State Police Mass Notification System.

2. Additional Items:

In addition to the above mentioned areas of concern, the following shall be reviewed and evaluated with recommended changes or improvements.

Physical locks and keys, as well as key control procedures.

Security staffing plans, post orders, personnel utilization and scheduling, etc.

Perimeter security features, including active and passive design elements, for overall effectiveness in maintaining the security of the facility.

A "man-down" notification system, as well as a "lone-worker/staff-duress notification system, for safety of laboratory personnel.

An asset tracking/protection system (similar to an RFID tag system) to safeguard valuable equipment or supplies from theft or loss.

A facility notification system for emergency communications through a unified system that includes pop up messages on desktop computers, text messaging, desk telephones, public address, fire alarm interface, etc.

3. Bio-Containment Areas:

Focused analyses must be performed on the bio-containment areas and registered spaces (currently utilizing bio-metrics functionality) and include an intrusion alarm system, both locally visible and audible with outreach notification capabilities. These systems must be designed to comply with CDC regulations regarding standard and emergency access and employee safety as well as operational reliability. In addition, integration of this future state system with NJ State Police mass notification system currently on campus should be studied.

4. Recommendations:

Recommendations will include at minimum, employee access (programmed locally/remotely) and embedded in issued ID cards; central review of employee movement and control of all exterior portals and features (such as gate arms); as well as control of surveillance cameras and interior doors by front desk Security station; integration of ID generation software and hardware into security system. Exterior and interior surveillance cameras must possess recording capability with easy access for review and download as needed for investigations or other purpose. The need for maintenance and repair services by qualified Vendor should be evaluated.

5. Security Plan Guidance:

A copy of the Security Plan Guidance document from the CDC's Federal Select Agent Program is shown in Exhibit 'D'. This document references all of the security plan requirements for facilities subject to select agent regulations.

E. SECURITY UPGRADE STUDY

The Security Upgrade Study shall be a compilation of all the information requested in this Scope of Work and identified in Section XI of this document entitled "Contract Deliverables". It is suggested that the document be divided into the following sections:

- Executive Summary
- Purpose, Limitations and Process
- Existing Conditions
- Security Upgrade Plan
  - Recommendations
  - Construction and Project Budget Estimates
- Exhibits & Addendums
  - Site Location Maps
  - Photographs
  - Floor Plans
  - Security System Schematic Drawings

The document shall contain a narrative of the surveys, inspections, and investigations conducted for each item listed. Recommendations to replace, repair and/or upgrade each building component shall be described and prioritized. All recommendations shall include estimates of costs. All floor plan drawings, surveys, utility schematics and colored photographs related to the buildings and their components shall be included for reference. All survey data, interviews, field notes, cost savings calculations, review comments, etc. shall be included in the Security Upgrade Study as an addendum.

The Consultant shall make an oral presentation of the Security Upgrade Study to the Project Team members at the 50% and 100% completion of the study. All Study evaluations and recommendations and the Security Upgrade Plan shall be discussed in detail at each oral presentation.

F. MEETINGS & PRESENTATIONS

1. Meetings:

Conduct the appropriate number of review meetings with the Project Team members during each phase of the project so they may determine if the project meets their requirements, question any aspect of the contract deliverables, and make changes where appropriate. The Consultant shall describe the philosophy and process used to meet the project objectives. Special considerations shall also be addressed such as: Contractor site access limitations, schedule requirements, security restrictions, etc.

It shall also be the responsibility of the Consultant to arrange and require all critical Sub-Consultants to be in attendance at the review meetings.

Record the minutes of each meeting and distribute within **five (5) calendar days** to all attendees and those persons specified to be on the distribution list by the Project Manager.

2. Presentations:

The minimum number of presentations required for each phase of this project is identified below for reference:

Security Upgrade Study Phase

One (1) working meeting halfway through phase at PHEAL
One (1) oral presentation at PHEAL at phase completion.

Initial Reporting Phase - 50% Completion

One (1) oral presentation at PHEAL at phase completion.

Final Reporting Phase – 100% Completion

One (1) oral presentation at PHEAL at phase completion.

VIII. PERMITS & APPROVALS

A. REGULATORY AGENCY PERMITS & APPROVALS

Identify all State and Federal Regulatory Agency approvals and permits that will govern and affect the work proposed in the Study. An itemized list of these approvals and permits shall be included for each facility and the total amount of the application fees should be included as part of the CWE.

IX. GENERAL REQUIREMENTS

A. SCOPE CHANGES

The Consultant must request any changes to this Scope of Work in writing. An approved DPMC 9c Consultant Amendment Request form reflecting authorized scope changes must be received by the Consultant prior to undertaking any additional work. The DPMC 9c form must be approved and signed by the Director of DPMC and written authorization issued from the Project Manager prior to any work being performed by the Consultant. Any work performed without the executed DPMC 9c form is done at the Consultant's own financial risk.

X. SOW SIGNATURE APPROVAL SHEET

This Scope of Work shall not be considered a valid document unless all signatures appear in each designated area below.

The Client Agency approval signature on this page indicates that they have reviewed the design criteria and construction schedule described in this project Scope of Work and verifies that the work will not conflict with the existing or future construction activities of other projects at the site.

SOW PREPARED BY: James W. Wright 12/6/2021

JAMES WRIGHT, MANAGER — DATE
DPMC PROJECT PLANNING & INITIATION

SOW APPROVED BY: 12-6-21

KEVIN JENNINGS, DIR., OFFICE OF ADMIN. SERVICES — DATE
NJ DEPARTMENT OF HEALTH

SOW APPROVED BY: 12/6/21

DAVID MARKUNAS, FAC. OPERATIONS MANAGER — DATE
NJ PUBLIC HEALTH ENVIRONMENTAL AND
AGRICULTURAL LABORATORY

SOW APPROVED BY: Joseph J. Polizzi III 12/6/2021

JOSEPH POLIZZI, PROJECT MANAGER — DATE
DPMC PROJECT MANAGEMENT GROUP

SOW APPROVED BY: Richard S. Flodmand 12/7/21

RICHARD FLODMAND, DEPUTY DIRECTOR — DATE
DIV PROPERTY MGT & CONSTRUCTION

XI. CONTRACT DELIVERABLES

The following is a listing of Contract Deliverables that are required at the completion of each phase of this project. The Consultant shall refer to the DPMC publication entitled, "Procedures for Architects and Engineers," Volumes I and II, 2nd Edition, dated January, 1991 to obtain a more detailed description of the deliverables required for each item listed below.

The numbering system used in this "Contract Deliverables" section of the scope of work corresponds to the numbering system used in the "Procedures for Architects and Engineers" manual and some may have been deleted if they do not apply to this project.

SECURITY UPGRADE STUDY PHASE

One (1) working meeting halfway through phase at PHEAL
One (1) oral presentation at PHEAL at phase completion.

INITIAL REPORTING PHASE

Security Upgrade Study Report (10 hardcopies and electronic disk)
- Executive Summary
- Purpose, Limitations and Process
- Existing Conditions
- Security Upgrade Plan
  - Recommendations
  - Construction and Project Budget Estimates
- Exhibits & Addendums
  - Site Location Maps
  - Photographs
  - Floor Plans
  - Security System Schematic Drawings

One (1) oral presentation at PHEAL at phase completion.

FINAL REPORTING PHASE

Security Upgrade Study Report (10 hardcopies and electronic disk)
- Executive Summary
- Purpose, Limitations and Process
- Existing Conditions
- Security Upgrade Plan
  - Recommendations

Construction and Project Budget Estimates
Exhibits & Addendums
Site Location Maps
Photographs
Floor Plans
Security System Schematic Drawings

One (1) oral presentation at PHEAL at phase completion.

PROJECT CLOSE-OUT PHASE

11.1 Responsibilities: Plan, Schedule and Execute Close-Out Activities

11.2 Commencement: Initiate Close-Out w/DPMC 20A Project Close-Out Form

11.5 Determination of Substantial Completion

11.7 Initiation of Final Contract Acceptance Process

11.8 Submission of Close-Out Documentation

11.9 Final Payment

11.9.2 A/E Invoice and Close-Out Forms for Final Payment

11.10 Final Performance Evaluation of the A/E

11.12 Submission Forms

Figure 11.2	Project Close-Out Documentation List DPMC 20A
Figure 11.3-a	Certificate of Substantial Completion DPMC 20D
Figure 11.3-b	Final Acceptance of Consultant Contract DPMC 20C
Figure 11.5	Request for Contract Transition Close-Out DPMC 20X
Figure 11.7	Final Contract Acceptance Form DPMC 20
Figure 11.8.3-a	Final Cost Analysis
Figure 11.8.4	Submission Checklist

XII. EXHIBITS

The attached exhibits in this section will include a sample project schedule, and any supporting documentation to assist the Consultant in the project such as maps, drawings, photographs, floor plans, studies, reports, etc.

A. SAMPLE PROJECT SCHEDULE FORMAT
B. PROJECT SITE LOCATION MAP - PHEAL
C. MASS NOTIFICATION PROPOSAL
D. SECURITY PLAN GUIDANCE

END OF SCOPE OF WORK

February 7, 1997
Rev.: January 29, 2002

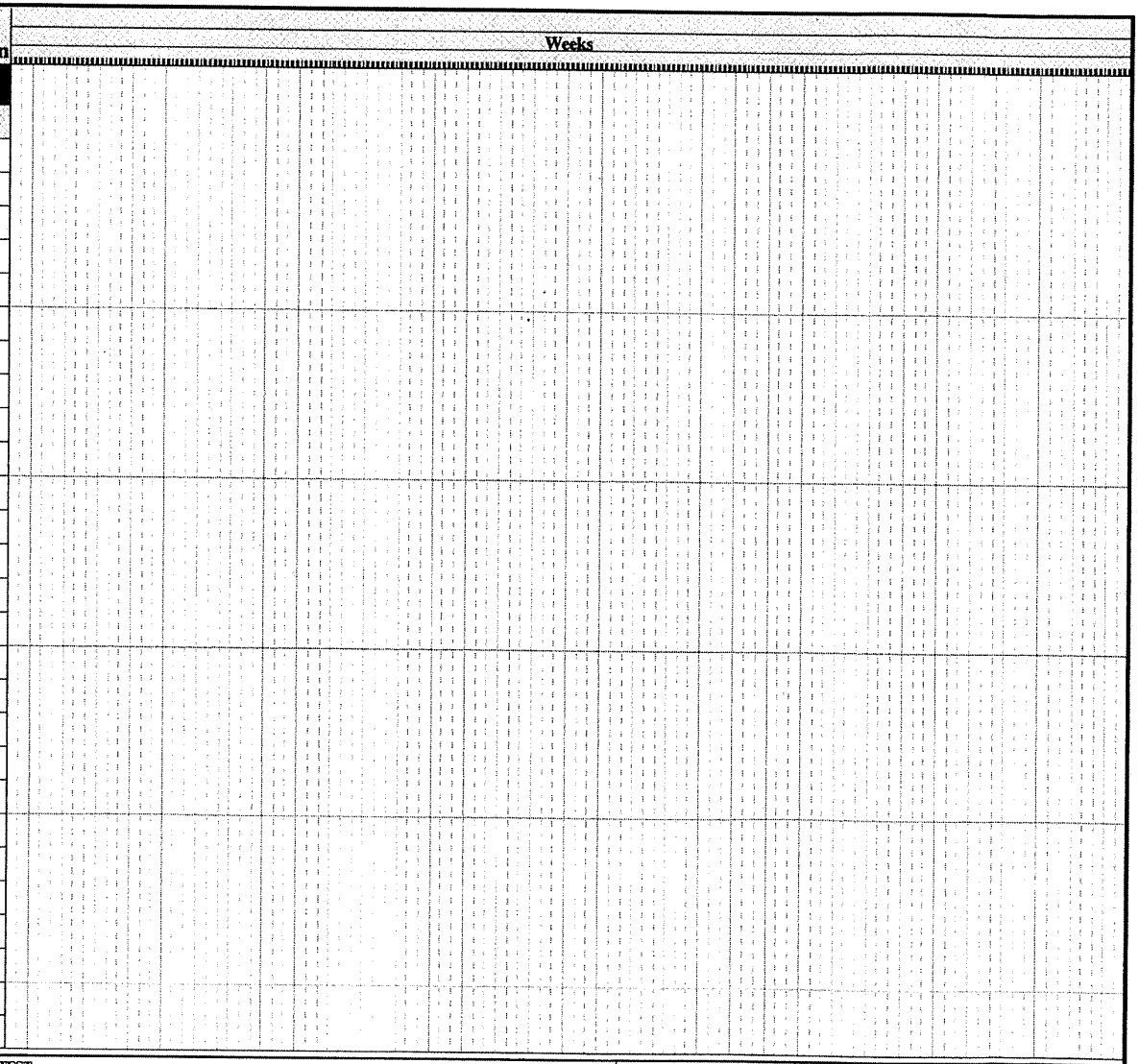
Responsible Group Code Table

The codes below are used in the schedule field "GRP" that identifies the group responsible for the activity. The table consists of groups in the Division of Property Management & Construction (DPMC), as well as groups outside of the DPMC that have responsibility for specific activities on a project that could delay the project if not completed in the time specified. For reporting purposes, the groups within the DPMC have been defined to the supervisory level of management (i.e., third level of management, the level below the Associate Director) to identify the "functional group" responsible for the activity.

CODE	DESCRIPTION	REPORTS TO ASSOCIATE DIRECTOR OF:
CM	Contract Management Group	Contract Management
CA	Client Agency	N/A
CSP	Consultant Selection and Prequalification Group	Technical Services
A/E	Architect/Engineer	N/A
PR	Plan Review Group	Technical Services
CP	Construction Procurement	Planning & Administration
CON	Construction Contractor	N/A
FM	Financial Management Group	Planning & Administration
OEU	Office of Energy and Utility Management	N/A
PD	Project Development Group	Planning & Administration

EXHIBIT 'A'

Activity ID	Description	Rspn
<PROJ>		
Design		
CV3001	Schedule/Conduct Predesign/Project Kick-Off Mtg.	CM
CV3020	Prepare Program Phase Submittal	AE
CV3021	Distribute Program Submittal for Review	CM
CV3027	Prepare & Submit Project Cost Analysis (DPMC-38)	CM
CV3022	Review & Approve Program Submittal	CA
CV3023	Review & Approve Program Submittal	PR
CV3024	Review & Approve Program Submittal	CM
CV3025	Consolidate & Return Program Submittal Comments	CM
CV3030	Prepare Schematic Phase Submittal	AE
CV3031	Distribute Schematic Submittal for Review	CM
CV3037	Prepare & Submit Project Cost Analysis (DPMC-38)	CM
CV3032	Review & Approve Schematic Submittal	CA
CV3033	Review & Approve Schematic Submittal	PR
CV3034	Review & Approve Schematic Submittal	CM
CV3035	Consolidate & Return Schematic Submittal Comment	CM
CV3040	Prepare Design Development Phase Submittal	AE
CV3041	Distribute D. D. Submittal for Review	CM
CV3047	Prepare & Submit Project Cost Analysis (DPMC-38)	CM
CV3042	Review & Approve Design Development Submittal	CA
CV3043	Review & Approve Design Development Submittal	PR
CV3044	Review & Approve Design Development Submittal	CM
CV3045	Consolidate & Return D.D. Submittal Comments	CM
CV3050	Prepare Final Design Phase Submittal	AE
CV3051	Distribute Final Design Submittal for Review	CM
CV3052	Review & Approve Final Design Submittal	CA
CV3053	Review & Approve Final Design Submittal	PR
CV3054	Review Final Design Submitl for Constructability	OCS



NOTE:
Refer to section "IV Project Schedule" of the Scope of Work for contract phase durations.

DBCA - TEST

Sheet 1 of 3

Bureau of Design & Construction Services
Routine Project

Exhibit "A"

Activity ID	Description	Rspn	Weeks
CV3055	Review & Approve Final Design Submittal	CM	
CV3056	Consolidate & Return Final Design Comments	CM	
CV3060	Prepare & Submit Permit Application Documents	AE	
CV3068	Prepare & Submit Bidding Cost Analysis (DPMC-38)	CM	
Plan Review-Permit Acquisition			
CV4001	Review Constr. Documents & Secure UCC Permit	PR	
CV4010	Provide Funding for Construction Contracts	CA	
CV4020	Secure Bid Clearance	CM	
Advertise-Bid-Award			
CV5001	Advertise Project & Bid Construction Contracts	CP	
CV5010	Open Construction Bids	CP	
CV5011	Evaluate Bids & Prep. Recommendation for Award	CM	
CV5012	Evaluate Bids & Prep. Recommendation for Award	AE	
CV5014	Complete Recommendation for Award	CP	
CV5020	Award Construction Contracts/Issue NTP	CP	
Construction			
CV6000	Project Construction Start/Issue NTP	CM	
CV6001	Contract Start/Contract Work (25%) Complete	CON	
CV6002	Preconstruction Meeting	CM	
CV6003	Begin Preconstruction Submittals	CON	
CV6004	Longest Lead Procurement Item Ordered	CON	
CV6005	Lead Time for Longest Lead Procurement Item	CON	
CV6006	Prepare & Submit Shop Drawings	CON	
CV6007	Complete Construction Submittals	CON	
CV6011	Roughing Work Start	CON	
CV6012	Perform Roughing Work	CON	
CV6010	Contract Work (50%+) Complete	CON	
CV6013	Longest Lead Procurement Item Delivered	CON	
CV6020	Contract Work (75%) Complete	CON	

NOTE:
Refer to section "IV Project Schedule" of the Scope of Work for contract phase durations.

DBCA - TEST

Sheet 2 of 3

Bureau of Design & Construction Services
Routine Project

Exhibit "A"

Activity ID	Description	Rspn	Weeks
CV6014	Roughing Work Complete	CON	
CV6021	Interior Finishes Start	CON	
CV6022	Install Interior Finishes	CON	
CV6030	Contract Work to Substantial Completion	CON	
CV6031	Substantial Completion Declared	CM	
CV6075	Complete Deferred Punch List/Seasonal Activities	CON	
CV6079	Project Construction Complete	CM	
CV6080	Close Out Construction Contracts	CM	
CV6089	Construction Contracts Complete	CM	
CV6090	Close Out A/E Contract	CM	
CV6092	Project Completion Declared	CM	

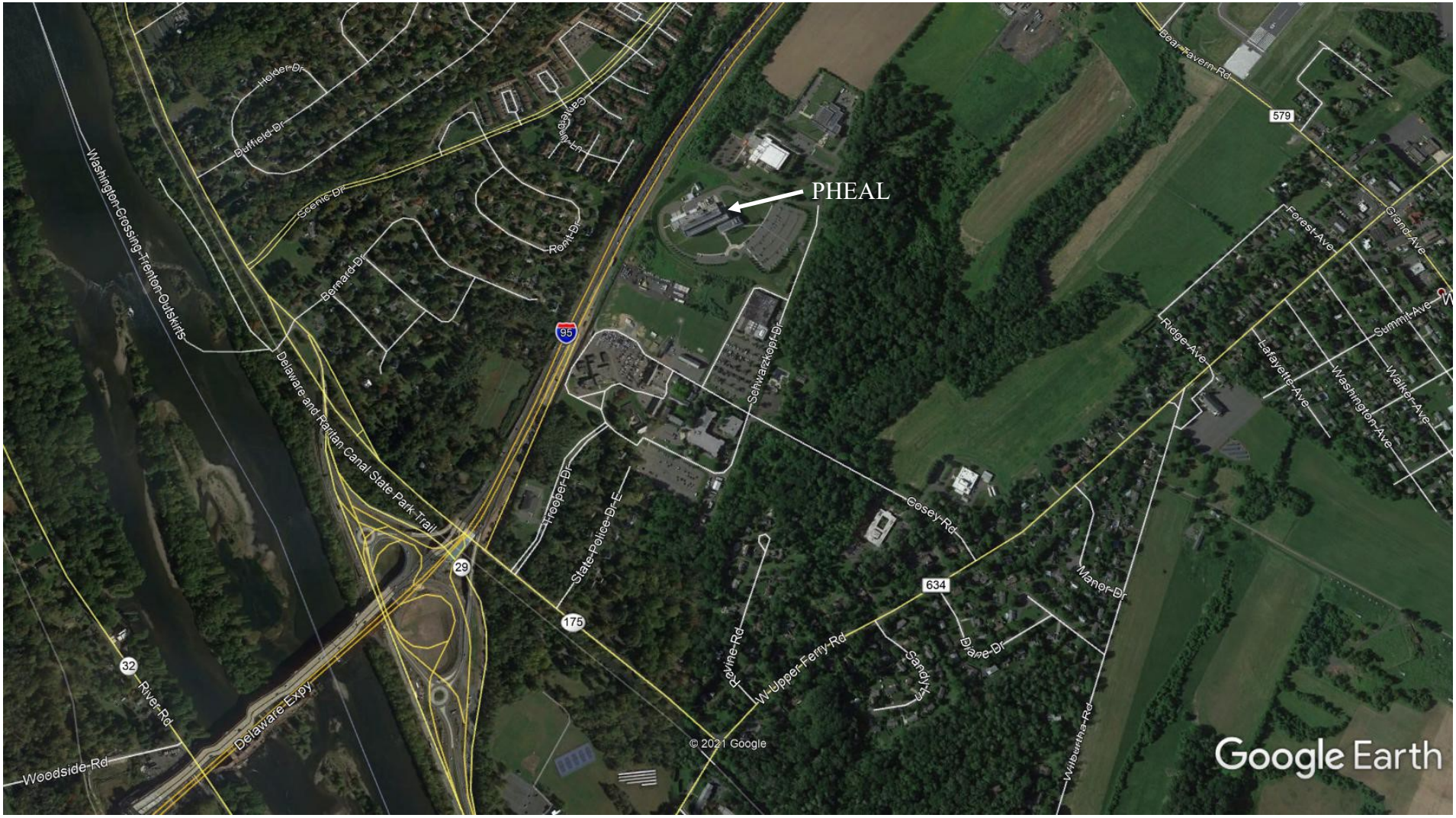
NOTE:
Refer to section "IV Project Schedule" of the Scope of Work for contract phase durations.

DBCA - TEST

Sheet 3 of 3

Bureau of Design & Construction Services
Routine Project

Exhibit "A"



Project Site Location Map - PHEAL

EXHIBIT ‘B’

VENTURE
ELECTRIC INC.

December 30, 2020

Mr. David Markunas
Facility Operations Manager
NJPHEAL
3 Schwarzkopf Drive
West Trenton, NJ 08628

Re: In-Building Mass Notification Proposal

Mr. Markunas,

Venture Electric is pleased to forward to you and your organization a "menu" style proposal for your In-Building Mass Notification System.

Due to the complex nature of the structure and the operations within, Venture Electric developed a base proposal to cover full control and activation of visual notification thru computer "Pop-Ups", SMS texts and emails while communicating with the NJSP Wide Area Mass Notification System.

There are expansion items such as adding one way voice communication throughout the common areas of the occupancy. Venture Electric excluded the environmentally controlled Lab Areas, as installation of voice messages in these areas would be costly. The lab areas may be entertained if funds are available.

Please review the attached information and feel free to reach out if you have any additional questions or concerns.

Respectfully Submitted,

James Falk
President
Venture Electric, Inc.

EXHIBIT 'C'

Venture Electric, Inc. hereby proposes to Engineer, Design, Furnish, Install and Program the following In-Building Mass Notification equipment:

The equipment below shall be installed at the Main Security Desk in Lobby:

(1) ATI REACT5000 Central Control Unit (CCU) provides enhanced control and monitoring of ATI remote units such as the Indoor Speaker Unit (ISU) and the High Power Speaker Station (HPSS).

It serves as a key component in the creation of a powerful and flexible Mass Notification System (MNS).

An intuitive touch screen interface allows for the activation of tone alerts, pre-recorded voice messages, or live PA, and displays the status of remote units. It may be used in conjunction with ATI's MassAlert® software for complete control of complex multi-location Mass Notification System applications, but may also be used as a standalone controller for smaller systems.

The REACT5000 supports multiple simultaneous communication paths to provide the most robust notification system available. It supports a wide variety of I/O protocols for simple interfacing to 3rd party systems and optional accessories. IPv4/IPv6 support with improved security features to provide the most secured communication link between the REACT5000 and other ATI units.

Multiple form factors are available for maximum flexibility in mechanical mounting and battery back-up power allows complete control of your system in the event of electrical outages.

(1) ATI SOFT-A MASSALERT SOFTWARE MassAlert® is an advanced software program for the overall control and monitoring of ATI emergency notification system. It is a highly interoperable application that seamlessly integrates with distributed data collections, sensing devices, and existing emergency communication systems, to reach everyone in the shortest time utilizing a wide variety of notification channels including sirens, paging systems, social networks, emails, text, and phone calls.

MassAlert® supports high-reliability and fault-tolerant deployment scenarios, ensuring high availability during man-made or natural disasters. It utilizes a highly scalable architecture that can support any notification system scale from large nation-wide mass notification system to an individual city or building. MassAlert® provides our clients with the capabilities to customize a specific robust solution that meets their needs.

EXHIBIT 'C'

Its client-server architecture is based on leading-edge technologies that allow access through a desktop, the web or a mobile application. It provides an intuitive, easy to use graphical user interface with multiple interactive maps that allows the system operator to easily monitor and control the entire system, being a 1-siren system or a large distributed system with thousands of sirens that are geographically dispersed.

MassAlert® employs a layered security strategy that involves combining several security controls to form a comprehensive multi-layered defense against cyber security threats. Layered security provides inherent redundancy; If one layer of security fails, another layer keeps the system and its data secure.

(1) ATI ICG Intelligent Control Gateway The ICG replaces the existing Advanced Communication Board (ACB) to provide more processing power, additional interfaces, and enhanced protocol support. It easily integrates into ATI's proven High Power Speaker Station (HPSS), Indoor Speaker Unit (ISU) and other ATI Systems interface units, such as the fire alarm and PA interface Remote Terminal Units (RTU).

One of the key features of the ICG is an ultrafast CPU with increased memory. It includes the support for IPv6 and the enhanced security over IP by integrating SSL/TLS security standards including 256 AES, RSA, 3DES, ARC4, SHA1, SHA2, MD2, MD4 and MD5. Another key feature is added network and communication ports including Ethernet, USB, CANbus, RS232, RS485, analog radio and telephone line.

Extremely reliable remote diagnostics are available with the ICG including support for SNMP traps and a secure web-based interface using the HTTPS protocol to make configuration changes and diagnostic. The ICG minimizes the electrical load for longer run times during power outages.

The ICG firmware is developed to comply with MISRA C:2012 which is one of the most trusted coding standards to ensure that the running code is safe, reliable, error-free and has no vulnerabilities that can lead to devastating consequences for the safety and security of our system.

(1) ATI DMRT Digital Message Record Time. Approximately (10) to (15) individual messages available. Typical message is (1) to (3) minutes.

(1) ATI MASSALERT Desktop Alerting providing "pop-up" notifications for up to 1500 users.

(1) ATI MASSALERT Mobile Device Alerting providing text and emails to Android and iOS mobile devices up to 1500 users.

EXHIBIT 'C'

(1) ATI MASSALERT Web Portal Mobile Application allows emergency personnel to instantly access, activate and monitor the Mass Notification System (MNS) from their Smartphone or tablet.

The mobile application is an integrated component of the MassAlert® Software, allowing authorized users to activate the system from anywhere without the need to go to the MassAlert® Control Station. As an administrator, you will be able to notify thousands of people within seconds, from your Smartphone, keeping those people safe and informed of critical events with a single tap!

Maximum users of (10) for Web Portal.

Supply (1) Motorola OTS radio with external antenna installed within the REACT 5000 enclosure.

Provide additional license for said radio on existing NJSP FCC license for NJSP WAMNS system.

Provide and install (1) complete Dell Precision 3240 Workstation with 24" Touch screen LED monitor for MASSALERT software installation and control.

Provide and install (1) complete Dell PowerEdge R640 server in the Security Rack located adjacent to the Security Office.

Provide and install all grounding and mounting systems and hardware required for antenna, LMR 400 cable and #2 copper bonding loop for all radio and network connected equipment.

Provide and install all 120VAC emergency circuit wiring from existing spare circuits in NJPHEAL infrastructure.

Provide necessary battery backup for REACT 5000, workstation and server.

NJPHEAL IT Department shall provide necessary firewalls (equipment, installation and commissioning) and shall provide (4) programmed and configured Ethernet ports to connect to the NJPHEAL network on a secure VLAN to transmit desktop pop-ups, mobile device alerting, and MASSALERT communication.

NJPHEAL to provide access to existing 3rd party text messaging platforms and email blast platforms to transmit mobile device alerting.

There shall be no licensing fees except those related to necessary FCC licensing for Motorola radios.

EXHIBIT 'C'

System includes one (1) year warranty on equipment, hardware and labor from date of system acceptance. Warranty does not include damage from Acts of God, and maintenance or repairs by anyone not employed by Venture Electric. All routine maintenance (necessary testing in accordance with NFPA 72 and battery replacement) is not included during warranty period.

There shall be (8) hours total training provided to key NJPHEAL employees, of which a Train the Trainer program shall occur within the allotted 8 hours.

TOTAL COST FOR ABOVE: $160,000.00

NOTE: Server and workstation may be supplied by NJPHEAL for a savings of $15,000.00

ADD/ALTERNATE #1: Venture Electric hereby proposes to Engineer, Design, Furnish, Install and Program the following In-Building Mass Notification equipment:

(3) ATI ISU Indoor Speaker Units combines our highly configurable Remote Terminal Unit (RTU) with 400 Watts (optional upgrade to 800 Watts) of audio output power for the delivery of reliable alert tone notification, pre-recorded messages and public address in emergency situations. It is capable of driving multiple zones of audible and visual alerts such as speakers and strobes. The unit is monitored, controlled, and activated by an ATI central control unit, such as the REACT5000, or can operate standalone using the Local Operating Console (LOC) option.

ISUs can support multiple simultaneous communication paths to ATI control units to provide the most robust, reliable notification system available. In addition, our ISUs include battery backup systems as AC power is often lost during an emergency.

Integration with external Public Address (PA), Fire Alarm Control Panel (FACP), and/or Heating, Ventilation, and Air Conditioning (HVAC) systems made simple using our flexible, configurable interface.

(350) System Sensor White Ceiling Mount 70.7vdc MNS Speakers with multi-watt selections for lower or higher sound output levels to control voice intelligibility. More ceiling mount devices at a lower wattage setting provides greater voice intelligibility than wall devices or less ceiling devices at a higher wattage setting.

(3) ATI ICG Intelligent Control Gateway The ICG replaces the existing Advanced Communication Board (ACB) to provide more processing power, additional interfaces, and enhanced protocol support. It easily integrates into ATI's proven High Power Speaker Station (HPSS), Indoor Speaker Unit (ISU) and other ATI Systems interface units, such as the fire alarm and PA interface Remote Terminal Units (RTU).

One of the key features of the ICG is an ultrafast CPU with increased memory. It includes the support for IPv6 and the enhanced security over IP by integrating SSL/TLS security standards including 256 AES, RSA, 3DES, ARC4, SHA1, SHA2, MD2, MD4 and MD5. Another key feature is added network and communication ports including Ethernet, USB, CANbus, RS232, RS485, analog radio and telephone line.

Extremely reliable remote diagnostics are available with the ICG including support for SNMP traps and a secure web-based interface using the HTTPS protocol to make configuration changes and diagnostic. The ICG minimizes the electrical load for longer run times during power outages.

The ICG firmware is developed to comply with MISRA C:2012 which is one of the most trusted coding standards to ensure that the running code is safe, reliable, error-free and has no vulnerabilities that can lead to devastating consequences for the safety and security of our system.

Supply (3) Motorola OTS radio with external antennas installed within the ISU enclosure.

Provide additional licenses for said radios on existing NJSP FCC license for NJSP WAMNS system.

Provide and install all grounding and mounting systems and hardware required for antenna, LMR 400 cable and #2 copper bonding loop for all radio and network connected equipment.

Provide and install all 120VAC emergency circuit wiring from existing spare circuits in NJPHEAL infrastructure.

Provide necessary battery backup for ISU's.

Provide and install necessary backboxes, fittings, hardware, support and 14/2 shielded FPLP NYC 150 degree Celsius certified wire for MNS speakers.

NJPHEAL IT Department shall provide necessary firewalls (equipment, installation and commissioning) and shall provide (3) programmed and configured Ethernet ports to connect to the NJPHEAL network on a secure VLAN for MASSALERT communication.

There shall be no licensing fees except those related to necessary FCC licensing for Motorola radios.

System includes one (1) year warranty on equipment, hardware and labor from date of system acceptance. Warranty does not include damage from Acts of God, and maintenance or repairs by anyone not employed by Venture Electric, Inc. All routine maintenance (necessary testing in accordance with NFPA 72 and battery replacement) is no included during warranty period.

There shall be (8) hours total training provided to key NJPHEAL employees, of which a Train the Trainer program shall occur within the allotted 8 hours.

TOTAL COST FOR ADD/ALTERNATE #1: $111,285.00

ADD/ALTERNATE #2: Venture Electric, Inc. hereby proposes to Engineer, Design, Furnish, Install and Program the following In-Building Mass Notification equipment:

(1) ATI LOC Local Operating Console is used to locally control, monitor, and activate a remote terminal unit such as an HPSS, ISU or PA unit. A simple menu system includes the capabilities to view status feedback and diagnostics, initiate alert tones, pre-recorded messages, and make live public address (PA) announcements using the attached microphone.

An LOC may be located up to 200 feet from any ISU in a secure room to initiate MNS messages or Live Voice Messages across the network.

TOTAL COST FOR ADD/ALTERNATE #2 per LOC: $6,000.00

COMPUTER WORKSTATION SPECIFICATION

Intel Core i7-10700 (8 Core, 16M cache, base 2.9GHz, up to 4.8GHz) DDR4-2933

Windows 10 Pro 64bit English, French, Spanish

Precision 3240 Compact Chassis

16GB 2X8GB DDR4 2666MHz or 2933MHz (2933MHz requires Intel Core i7 or above) SoDIMM Non-ECC Memory

NVIDIA Quadro P620, 2GB, 4 mDP to DP adapter

C2 M.2 PCIe Boot SSD

512GB PCIe NVMeClass 40 M.2 SSD

vPro - Manageability

Dell KB216 Wired Keyboard English

Dell MS116 Wired Mouse

ENERGY STAR Qualified

EPEAT Registered

240W A/C Adapter

EXHIBIT 'C'

SERVER SPECIFICATION

PowerEdge R640 Server

Trusted Platform Module 2.0

2.5” Chassis with up to 8 Hard Drives and 3PCIe slots

PowerEdge R640 CE, CCC, BIS Marking

Intel Xeon Silver 4208 2.1G, 8C/16T, 9.6GT/s, 11M Cache, Turbo, HT (85W) DDR4-2400

Intel Xeon Silver 4208 2.1G, 8C/16T, 9.6GT/s, 11M Cache, Turbo, HT (85W) DDR4-2400

Standard Heatsink for 2 CPU

3200MT/s RDIMMs

Memory Mirroring

8GB RDIMM, 3200MT/s, Single Rank

C3, RAID 1 for 2 HDDs or SSDs (Matching Type/Speed/Capacity)

PERC H740P RAID Controller, 8GB NV Cache, Minicard

1.2TB 10K RPM SAS 12Gbps 512n 2.5in Hot-plug Hard Drive

Windows Server® 2019 Standard,16CORE,FI,No Med,No CAL, Multi Language

Windows Server 2019 Standard,16CORE,Digitally Fulfilled Recovery Image, Multi Language functionality only

iDRAC9, Express

iDRAC Group Manager, Disabled

iDRAC,Factory Generated Password

Riser Config 4, 2x16 LP

Broadcom 57414 Dual Port 10/25GbE SFP28, rNDC

SFP+ SR Optic, 10GbE, High Temperature, for Broadcom 57414 rNDC at 10gb functionality only

DVD +/-RW, SATA, Internal

8 Performance Fans for R640

Dual, Hot-plug, Redundant Power Supply (1+1), 495W

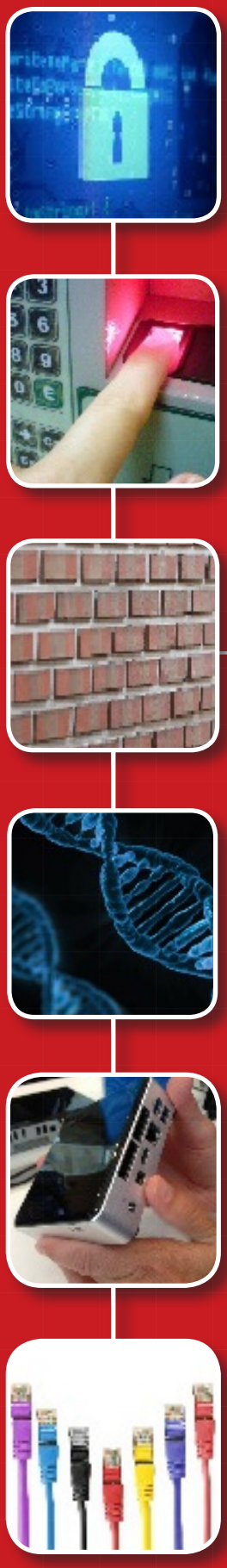
NEMA 5-15P to C13 Wall Plug, 125 Volt, 15 AMP, 10 Feet (3m), Power Cord, North America

Performance BIOS Setting

Legacy BIOS Boot mode with GPT for Data Partition

Microsoft SQL Server 2019 Standard,OEM, Incl. 5 USER CALs, NFI with SQL2017/2016 DWGD Media,ENGLISH

EXHIBIT 'C'



SECURITY PLAN GUIDANCE

42 CFR § 73.11, 7 CFR § 331.11, and 9 CFR § 121.11

FEBRUARY 2020

Centers for Disease Control and Prevention
Division of Select Agents and Toxins

Animal and Plant Health Inspection Service (APHIS)
Division of Agricultural Select Agents and Toxins

EXHIBIT 'D'

Contents

EXHIBIT 'D'

Changes and Highlights

Revisions: This is a living document subject to ongoing improvement. Feedback or suggestions for improvement from registered select agent entities or the public are welcomed. Submit comments directly to the Federal Select Agent Program (FSAP) at:

CDC: LRSAT@cdc.gov

APHIS: DASAT@usda.gov

Revision History:
October 12, 2012: Initial posting
April 11, 2013: The revisions are primarily changes to correct editorial errors from previous version. July 3, 2013: Appendix added to document.
September 2017: Added Tier 1 requirements.
February 2020 (Revision 4): Revised Inventory language to match Inventory Guidance and to correct editorial errors from previous version.

EXHIBIT 'D'

Introduction

Section 11 of the select agent regulations (42 CFR § 73.11, 7 CFR § 331.11, and 9 CFR § 121.11) requires a registered entity to develop and implement a written security plan that is:

1. Sufficient to safeguard the select agents or toxins against unauthorized access, theft, loss, or release, and
2. Designed according to a site-specific risk assessment, providing graded protection.

The purpose of this guidance document is to assist an entity in developing and implementing its site-specific security plan. As used in this document, the word "must" means a regulatory requirement. The use of either "should" or "consider" signifies a suggested method that has requirements based on generally recognized security "best practices." Implementation is performance-based and entities may find other ways to meet a regulatory requirement.

This document addresses the select agent regulations (SAR) with regard to security with one exception: Entities with Tier 1 BSAT have pre-access suitably and ongoing suitability assessment requirements which are addressed in the Guidance for Suitability Assessments.

Section 11(a) – Creating a Site-Specific Written Security Plan

Section 11(a) of the select agent regulations require entities to develop and implement a written site-specific security plan. A security plan is a documented, systematic set of policies and procedures to achieve security goals that protect BSAT from theft, loss, or release. Plans may also include agreements or arrangements with extra-entity organizations, such as local law enforcement. Plans may be a single document, or incorporate other documents, policies, and procedures that work to achieve those security goals.

Entities should establish specific policies that support their plan. Security policies should document strategies, principles, and rules which the entity follows to manage its security risks. Effective policies provide a clear means of establishing behavioral expectations and cover the spectrum from directives, to standard operating procedures (SOPs). As part of security program management, the entity should consider formally documenting security policies covering all operational controls.

Background checks and other personnel security measures should be vetted through the entity's legal and human resources department. See the FSAP Guidance for Suitability Assessments for additional information.

An effective security plan should be based on the following principles:

- It should result from collaboration between entity management, scientific, facilities, safety and security personnel.
- It is built upon tested, well documented operational processes.
- It should account for and secure all biological select agents or toxins from creation or acquisition to destruction.
- It complements other plans such as biosafety, disaster recovery, continuity of operations, and others.
- It does not violate any laws. Laws to consider when creating the security plan include the Americans with Disabilities Act, OSHA Safety Standards, and local building and fire codes.
- The entity should provide security plan training to ensure every person understands his or her responsibilities.
- It requires reporting of all suspected security incidents and suspicious activities.
- It is reviewed at least annually and updated whenever conditions change.
- It is based on a site-specific risk assessment.

Security Plan Roles and Responsibilities

The security program should define each individual's roles and responsibilities and solicit their input for improvements.

An entity should be aware of, and collaborate with, the personnel responsible for and/or impacting security. This may include:

- Responsible Official (RO)/Alternate Responsible Official (ARO)
- Facility key control and/or access control personnel
- Alarm companies

EXHIBIT 'D'

- Campus security personnel
- Security personnel who observe video
- Local law enforcement or other response forces
- FBI – Weapons of Mass Destruction (WMD) coordinator

Key Entity Leadership

Certain parties should be involved in the process of designing and implementing the security plan. These include, but are not limited to:

- Owner/Controller
- Principal Investigator (PI)
- Responsible Official (RO)
- Alternate Responsible Official (ARO)
- Human Resources
- Biosafety staff
- Security staff
- Institutional Biosafety Committee
- Laboratory Management

Security Plan Team

Each person brings an important perspective as a subject matter expert (SME) in their own specialty. This group should collaborate to develop a site-specific security plan. Plans should also include agreements or arrangements with extra- entity organizations, such as local law enforcement.

Entities should form a team of entity SMEs, supporting security professionals, and stakeholders. The team should include entity professionals who are experts on the potential consequences of a theft, loss, or release of a select agent or toxin and the daily operations of the entity. Entities are also encouraged to include federal partners (i.e., the FBI) as well.

Entity personnel should provide knowledge of:

- SOPs, policies, and other organizational controls which can reinforce or be affected by security measures
- Public health consequences of the select agents and toxins
- Biosafety
- Operational requirements
- Value of the select agent or toxin work to the organization
- Knowledge of current security systems

Facility and support personnel should provide knowledge of:

- Facility wide security measures
- Personnel hiring practices (background checks, reference checks, education verification)
- Planned upgrades to the facility

EXHIBIT 'D'

- Constraints which affect security (biosafety, fire code, ordinances, federal laws)

Local, state, and federal law enforcement and security personnel members may be able to provide knowledge of:

- Known threats to the entities
- Assistance with identifying vulnerabilities
- Assistance with designing or vetting the mitigating factors
- Economic and psychological impacts of the select agents or toxins

Once the team is formed, members should be consulted on a regular basis, including during the plan development and implementation. The team should meet annually as part of the security plan review.

EXHIBIT 'D'

Section 11(b) – Site-Specific Risk Assessment

Section 11(b) of the select agent regulations states: "The security plan must be designed according to a site-specific risk assessment and must provide graded protection in accordance with the risk of the select agent or toxin, given its intended use." Graded protection is a result of mitigating the hazards (threat and natural) and the vulnerabilities based on the consequences of a select agent or toxin in its current form.

The cornerstone of a good security plan is a current site-specific risk assessment. It forms the logical basis for physical and personnel security measures employed to achieve graded security. It should indicate what risks have been identified, and of those identified, which have been mitigated and any residual risks acceptable to the entity. It does not necessarily have to account for accidental hazards accounted for in a biosafety plan. **Risk** comes from the interaction of threats/hazards, vulnerabilities, and consequence (**Figure 1**).

There are many methods to capture these interactions, including qualitative, quantitative, or probabilistic analysis, among others. Any assessment that accurately captures and relates these interactions is sufficient.

Figure 1: Determining Risk

EXHIBIT 'D'

Conducting a Risk Assessment

Understand and Assess Threats

A threat is a person or organizations whose actions may cause the theft or release of a select agent or toxin. The threat may target the agent directly (e.g. theft), cause damage to the entity as the result of their action (e.g. extremists and terrorists damaging containment), and act on their own or collude with others. Threats can be captured as a 'probability of attack.'

Threats are generally determined in 3 different ways:

- Entities are encouraged to reach out to law enforcement and other experts to understand, assess, and determine threats.
- An expert or group of experts model 'threats' in general, often using Design Basis Threat (DBT)[1]. This capability is most common in federal and state facilities but may be available in larger entities.
- Historical data, including statistics on past local events (crimes), terrorist events worldwide, social science research into terrorists' behavior, official accounts, and/or terrorists own writings about motivation and intent.

Insider Threats

An insider threat comes from personnel within the organization who have inside information regarding the organization's security, data to include Select Agent and Toxin inventory, access to biocontainment and computers. The goals of such threats often involve fraud, information theft, intellectual property theft, theft and/or misuse of Select Agents and toxins, and computer system sabotage.

External Threats

An external threat originates outside of the organization. These threats may include hackers, outages, and other emergencies.

Natural Hazards

See the Incident Response Guide for resources to help you to determine if you are in a risk area for natural hazards. As with threats, entities should assess the impacts of the hazard to its people, select agent or toxin inventories as well as the entity as whole.

Understand and Assess Vulnerabilities

Vulnerability is the relative susceptibility of select agents or toxins to a threat or natural hazard. Vulnerabilities are a threat capability that can be applied which results in the theft or release of the agent or a natural hazard that can impact safety of staff and security of select agents or toxins. Vulnerabilities are often captured as "probability of effectiveness" (PE) of a particular system. Below are some best practices in conducting vulnerability assessment:

- Exercises/after action reviews
- Assessments by subject matter experts (SMEs)
- Scenarios and path development with SMEs and entity members
- Modeling (primarily with natural hazards)
- Simulations (primarily with natural hazards)

EXHIBIT 'D'

[1] A profile of the type, composition, and capabilities of an adversary.

Understand and Assess Consequence

Consequence is the impact of the theft or release of the agents. It is the impact on public, animal, or plant health and safety, and the potential for economic and psychological impacts. Entities should consider:

- The communicability of the agent.
- The agent's mortality and morbidity rates.
- Present availability of known countermeasures to the agent or toxin.
- The type of work being conducted on the select agent or toxin:
    - **Low risk** generally includes select agents or toxins that are handled in a diagnostic, non-propagative manner (e.g., single specimen, no culture). This may also include small quantities of select agents or toxins that are endemic in the environment.
    - **Moderate risk** includes select agents or toxins that are propagated or in amounts greater than a diagnostic sample. This risk level includes activities that work only with the amounts necessary for experiments at hand (e.g., specimen cultured for diagnostic purposes or produced only in amounts required for the research or experiments being conducted).
    - **High risk** includes select agents or toxins that are handled in large or highly purified quantities. It would also include those select agents or toxins used in higher risk procedures such as aerosolization, centrifugation, animal inoculation, or restricted experiments (as defined by section 13 of the select agent regulations).

Key point: Unless there is sufficient data available to project a particular threat's capability to enhance an agent, entities do not have to consider hypothetical threats that would make an agent more virulent. Current characteristics are sufficient for this assessment.

Assess Risk

A sufficient risk assessment should reflect the interactions of threat, vulnerability and consequence. In implementing a risk assessment, threat, vulnerability, and consequence may be captured as discrete variables, dependent variables (i.e., probability), or other methods. Also, entities may use a quantitative or qualitative means depending on the amount of information available. See Risk Analysis Methods for more information and examples of qualitative risk assessment. For guidance on mitigating the impacts of a natural hazard, see the Incident Response Guide.

Communicating Risks

After the risk assessment is completed, the key entity leadership should determine if the current risk level is acceptable. If the risk level is deemed unacceptable, then the entity should develop a means to mitigate the risk. Some common risk mitigation measures are given below. It should be noted that any activity involving a select agent or toxin will involve some level of unmitigated risk. The only way to eliminate risk completely would be to not undertake this work.

Manage the risk: Mitigation measures

If the risk is not acceptable, the entity has multiple paths to mitigate the risks. Options include:

- Employ additional security measures.
- Change the work with the select agent or toxin to reduce risk.

- Decrease the quantity of toxin on hand, possessing only the amounts necessary for the work.
- Change how the select agent or toxin is stored (e.g., not lyophilized).
- When a toxin is a by-product of a larger process, immediately autoclave the agent or destroy the toxin.
- Document any risks which have not been mitigated and why.

Document and Update the Risk Assessment

The entity should document the risk assessment and review it as threats change. The security plan should be updated to reflect the changes based on the risk assessment, as should any drills and exercises that are impacted by the change.

EXHIBIT 'D'

Section 11(c) – Planning Requirements

Section 11(c)(1) of the select agent regulations requires the security plan to describe procedures for physical security, inventory control, and information systems control. These descriptions should reflect the policies implemented at the entity. This section explains different methods for ensuring that the entity's security plan complies with the regulations.

Effective inventory control measures for select agents and toxins can deter and detect a variety of insider threats. How the inventory audits are conducted and inventory is maintained must be described in the entity's security plan and inventory records must meet the requirements of section 17 of the select agent regulations. The security requirement includes:

- Current accounting of any animals or plants intentionally or accidentally exposed to a select agent.
- An accurate and current inventory for each select agent or toxin in long-term storage.
- Labeling and identifying select agents and toxins in the entity inventory in a way that leaves no question that the entity's inventory is accurately reflected in the inventory records.
- Accounting for select agents and toxins from acquisition to destruction.
- See Inventory Audits for more detailed instructions on maintaining effective inventory control.

Access Control

Section 11(c)(2) – Provisions for Access and Safeguarding

Section 11(c)(2) of the select agent regulations require the security plan to describe how the select agent or toxin is physically secured against unauthorized access. The security plan is performance based and should complement the Incident Response Plan and Biosafety Plan. An effective physical security plan deters, detects, delays, and responds to threats identified by the site-specific risk assessment. A successful security plan creates sufficient time between detection and the completion of an attack for response force to arrive. The physical security plan should include:

- Security barriers that both deter intrusion and deny access (except by access approved personnel) to the areas containing select agents and toxins:
    - Perimeter fences
    - Walls
    - Locked doors
    - Security windows
    - Trained person (e.g., security guard, trained laboratorians, or escorts)
- Biosafety measures and other environmental factors that increase security such as:
    - Access or locking system which denies access to BSAT, e.g. mechanical locks, card key access systems or biometrics
    - Tamper-evident devices for select agents and toxins held in long-term storage
- A balanced approach so that all access points, including windows and emergency exits, are secured at the same level
- A procedure or process to keep the number of alarms to a minimum

EXHIBIT 'D'

Create a system that limits access to select agents and toxins to those approved by the HHS Secretary or APHIS Administrator for access to select agents and toxins. The access control system should:

- Include provisions to limit unescorted/unrestricted access to the registered areas to those who have been approved by the HHS Secretary or APHIS Administrator to have access to select agents and toxins.
- Include provisions for the safeguarding of animals and plants exposed to or infected with select agents.
- Regularly review and update access logs.
- Be modified when access requirements change or be responsive to changes in personnel's access requirements during personnel changes.

Remain flexible enough so non-approved personnel can be escorted if needed. See Non-Tier 1 Barrier Scenarios for a visual representation of adequate physical security barriers. See Intrusion Detection Systems for a chart that defines and explains the use of various IDS options.

Section 11(c)(3) – Provisions for Cleaning, Maintenance, and Repairs

The security plan must state how cleaning, maintenance, and repairs will be accomplished in areas where BSAT are stored or used. When allowing maintenance, cleaning, or repair personnel (whether in-house or contract services) into a registered area, an entity should practice one or more of the following:

1) Use only access approved individuals.
2) Provide an access approved individual as an escort to the non-approved individual.
3) If the non-approved individual will not be escorted, install additional security measures (e.g., additional lock and key, cipher lock, or tamper alarms interfaced with the facility intrusion detection system) to prohibit access to select agents and toxins by non-approved individual; or
4) Remove the select agent or toxin to a different area that is appropriately registered.

Section 17 (Records) of the select agent regulations requires that access logs must be in place to record the name and date/time of entry into the registered area, including the name of an escort.

Section 11(d)(2) – Escort Provisions

The security plan must contain provisions that allow non-approved persons access to registered spaces that store BSAT only when escorted by an access approved person. The escort must be dedicated to observing the escorted person. No other duties may be performed during the time that the individual is serving as an escort. The escort must understand what to observe for (e.g., accessing select agents and toxins). Non-approved persons are not allowed to have access to an agent, even if escorted by an access approved person. The escort's responsibilities include:

- Serving as a physical barrier between the non-FSAP approved person and select agents and toxins.
- Being knowledgeable about the entity's security policies.
- Training non-FSAP approved persons on emergency protocols and risks related to the BSAT before they enter the registered space.
- Executing safety protocols as necessary.
- Receive approval for escorted access and notifying the RO when escorted entry has concluded.

See the Security Risk Assessment FAQs for more information about escort provisions.

EXHIBIT 'D'

Section 11(d)(6) – Prevent Sharing Access Credentials

The security plan must state that any person accessing select agents and toxins will not share their unique means of access (such as key cards and passwords) with any other person. This should include how the entity prevents:

- "Piggybacking" or "tailgating" on another access approved person's access card.
- Key card, password or badge sharing.

Challenge all individuals who tailgate or piggyback a secured access entry point.

Section 11(c)(5) – Identification, Key, Keycard, Combination, and Password Management

The security plan must describe the procedures for changing access after personnel changes in order to prevent access by personnel who have previous approved access to select agents and toxins. This can include:

- Deactivating card key access.
- Deactivating email, network, and local machine computer accounts which provide access to information.
- Surrendering key cards and badges.
- Surrendering keys and key cards when people leave or change duties.

The security plan must indicate that the following incidents must be reported to the RO:

- Any loss or compromise of keys, passwords, and combinations.
- Any suspicious persons or activities.
- Any loss or theft of a select agent or toxin.
- Any release of a select agent or toxin.
- Any sign that inventory or use records for select agents and toxins have been altered or otherwise compromised.

EXHIBIT 'D'

Unauthorized or Suspicious Persons

Section 11(c)(4) – Reporting and Removing Unauthorized or Suspicious Persons

An "unauthorized person" is not approved to have access to select agents and toxins or is not authorized by the entity to be in a particular area or be involved in particular conduct. A "suspicious person" is any individual who has no valid reason to be in or around the areas where select agents and toxins are possessed or used.

The security plan must describe the process for identifying and removing unauthorized and suspicious persons. It must also require follow-up actions such as reporting the information to the RO; and the RO reporting the information to entity security personnel, and possibly contacting local law enforcement agencies or FSAP, as appropriate.

Unauthorized and suspicious persons attempting to gain entry into registered areas without proper credentials should be identified, challenged and removed immediately. The RO must be notified immediately (see Section 11(d)(7) for more details).

The entity should consider:

- Integrating an access control measure (e.g., card key) into an alarm system that notifies a responder when an unauthorized person attempts to gain access (similar to an IDS, but does not involve an actual break in).
- Having a badge system that clearly identifies who does and does not have approved access to select agents and toxins.
- Provide training on how to remove unauthorized personnel (e.g., procedures for notification of security personnel and/or local law enforcement).

See RO Reporting for more detailed instructions for what activities should be reported to the RO.

Access Approval

Section 11(c)(7)

Section 11(c)(7) requires the entity to ensure that all individuals with access approval from the HHS Secretary or APHIS Administrator understand and comply with the security procedures. All approved individuals should undergo training that covers general security as well as security training as it applies to their specific work. See the Training Requirements guidance document for general information on training provisions.

Section 11(d)(1)

Create a system that limits access to select agents and toxins to those approved by the HHS Secretary or APHIS Administrator for access to select agents and toxins. Individuals must have passed a security risk assessment and have approval from either the HHS Secretary or APHIS administrator before they obtain access to any select agents or toxins.

RO Reporting

Section 11(c)(8) – Suspicious Activities

The security plan must describe procedures for how the RO will be informed of suspicious activity that may be criminal in nature and related to the entity, its personnel, or its select agents and toxins. Individuals with access

EXHIBIT 'D'

to select agents and toxins must be aware of the protocol for reporting suspicious or criminal activity. The plan must also describe procedures for how the entity will notify the appropriate federal, state, or local law enforcement agencies of such activity. Identify who best can respond to the circumstances during the security portion of the risk assessment.

The security plan must include procedures for how the entity will notify the appropriate Federal, State, or local law enforcement agencies of any suspicious or criminal activity.

Suspicious activity of a criminal nature includes:

- Those activities so identified in the site-specific security risk assessment.
- Insider:
    - Attempts to create additional select agent or toxin inventory not authorized or required.
    - Attempts to conceal or hide and not report select agent or toxin inventory discrepancies.
    - Attempts to remove select agent or toxin inventory without authorization.
    - Attempts by "restricted" persons to intentionally access registered areas containing a select agent or toxin.
- Outsider:
    - Indirect threats against the entity receives by email, letter, telephone, or website postings.
    - Unauthorized attempts to purchase or transfer a select agent or toxin.
    - Attempts to coerce entity personnel into a criminal act.
    - Intimidation of entity personnel based on their scientific work (for example, eco-terrorism).
    - Requests for access to laboratories for no apparent legitimate purpose or for purposes that do not appear legitimate.
    - Unauthorized attempts to probe or gain access to proprietary information systems particularly access control systems (for example, attempts by unauthorized individuals to gain physical or electronic access to systems).
    - Theft of identification documents, identification cards, key cards, or other items required to access registered areas.
    - Personnel representing themselves as government personnel (federal, state, local) attempting to gain access to the facility or obtain sensitive information that cannot or will not present appropriate identification.
    - Use of fraudulent documents or identification to request access.

Section 11(d)(7) – Reporting to the RO

Require that individuals with access approval from the HHS Secretary or Administrator immediately report any of the following to the Responsible Official:

- Any loss or compromise of keys, passwords, combination, etc.
- Any suspicious persons or activities.
- Any loss or theft of select agents or toxins.
- Any release of a select agent or toxin.
- Any sign that inventory or use records for select agents or toxins have been altered or otherwise compromised.
- Any loss of computer, hard drive or other data storage device containing information that could be used to gain access to select agents or toxins.
- Any security breach of containment laboratory containing select agents and toxins

EXHIBIT 'D'

Information Systems Security Controls

Section 11(c)(9) – Information Systems Security Controls

Please see the Information Systems Security Controls Guidance for details about meeting the requirements of this section of the regulations.

Shipping and Transfers

Section 11(c)(10) Shipping and Transfers

The security plan must contain provisions and policies for shipping, receiving, and storage of select agents and toxins. This includes procedures for receiving, monitoring, and shipping of all select agents and toxins.

With exception of exports out of the country, shipments containing select agents and toxins between entities must be authorized by FSAP, coordinated through an APHIS/CDC Form 2, and tracked so the receiving entity knows when the shipment will arrive. Both the sender (unless the sender is outside of the United States) and the recipient (unless the recipient is outside the United States) of the package must be approved for access to select agent or toxins.

The individual who packages the BSAT for shipment must have an SRA approval and appropriately trained.

The package containing select agents and toxins is not considered "received" by the entity until the intended recipient takes possession of the package. The intended recipient must have SRA approval and, if the agent is Tier 1, have gone through the entity's pre-access suitability and is subject to the entity's ongoing assessment.

When received by the intended recipient, the shipment should immediately be secured in a registered space. Ideally, the shipment is taken to the receiving laboratory; however, the package may be temporarily stored in other registered spaces.

Shipping and receiving areas must be registered if the select agents or toxins packages are identified or accessed. For example:

- If packaging or un-packaging of a select agent or toxin is performed in these areas.
- If the plan to temporarily store identified select agents.

If select agent or toxin packages are not identified or accessed, the shipping and receiving area may not need to be registered.

The entity must also have a written contingency plan for receipt and security for unexpected shipments. An "unexpected shipment" is when an entity receives a legitimate shipment of a select agent that it had neither requested nor coordinated for. The entity must have a contingency plan to have approved personnel gain control of the unexpected shipment of BSAT without delay and secure it in a registered area.

Section 11(d)(5) – Intra-Entity Transfers

An intra-entity transfer is a physical transfer of select agents or toxins that takes place between two individual with access approval, preferably two FSAP approved PIs, at the same registered entity, and e.g., a PI removes a select agent or toxin from his long term storage and gives it to another PI at the same entity.

EXHIBIT 'D'

Entities that conduct intra-entity transfers must describe in their security plan how these transfers will take place, including chain-of-custody documents and provisions for safeguarding the select agents and toxins against theft, loss, or release. Please see the example intra-entity transfer form to see what information should be captured according to section 17 (Records) of the select agent regulations. Transfers must include a chain-of-custody document and ensure that select agents and toxins will not be left unattended. See the Intra-Entity Transfer Template. The entity is not required to cover intra-entity transfers in the security plan if they do not conduct them.

Section 11(d)(4) – Inspection of Suspicious Packages

A suspicious package is any package or item that enters or leaves registered areas that does not appear to be consistent with what is expected during normal daily operations.

The entity should consider the following indicators of suspicious packages:

- Misspelled words
- Addressed to a title only or an incorrect title
- Badly taped or sealed
- Lopsided or uneven
- Oily stains, discolorations, or crystallization on the wrapper
- Excessive tape or string
- Protruding wires
- Return address does not exist or does not make sense

The security plan must describe how the entity will inspect packages based on the site-specific risk assessment. The entity should inspect all packages and items before they are brought into or removed from areas where select agents and toxins are used or stored (registered laboratory, etc.). Suspicious packages should be inspected visually or with noninvasive techniques before they are brought into, or removed from the area where select agents and toxins are stored or used. See the USPS guidelines for recognizing suspicious packages for more detailed information.

EXHIBIT 'D'

Section 11(d) – Security Requirements

This section describes the policies and procedures that the entity must implement in order to be in compliance with the select agent regulations.

Storage

Section 11(d)(3) – Storage Control

The entity is required to "provide for the control of select agents and toxins by requiring freezers, refrigerators, cabinets, and other containers where select agents or toxins are stored to be secured against unauthorized access (e.g., card access system, lock boxes)." See Access Control Devices for more information on methods of securing BSAT against unauthorized access.

The entity can comply with this requirement in a number of ways. Typically, physical locks, key card access, biometrics, or some combination of those provide adequate storage control. Tier 1 select agents and toxins require more stringent conditions. See the Tier 1 guidance document for more information.

Section 11(d)(8) – Separate Registered Space from Public Space

The storage or laboratories that contain select agents and toxins must not be publicly accessible. Public areas are places where the general public may congregate or transit. Areas where select agents and toxins are used or stored must be registered and personnel with access to the registered space must have approval from the HHS Secretary or the APHIS administrator.

Section 11(e) – Inventory Audits

An inventory audit is an examination of a portion of the inventory or collection sufficient to verify that inventory controls are effective. **Note:** This inventory is not a part of the requirements of section 17. Section 11(e) of the select agent regulations requires the entity to perform a complete inventory audit for all BSAT under the control of a PI whenever:

1. The BSAT is physically relocated to another registered space.
2. There is a change (departure or new arrival) of the PI in control of the BSAT.
3. There is a theft or loss of BSAT under the control of the PI.

Entities have discretion on how they conduct these audits. The depth of an audit should depend on the circumstances. Entities should consider the following when determining the depth of an entity audit:

1. The timing of the inventory audit.
2. The circumstances that require the inventory audit. For example, an 'emergency' movement to another location (freezer malfunction) may result in a focus on counting full racks and a confirmation of a targeted, smaller number of vials. In the case of a shipment to a new building or campus where there is sufficient time to plan, entities are encouraged to inventory more thoroughly.
3. The criteria used to determine which samples are audited. In the case of a large inventory, the entity may choose to focus on the most recently manipulated samples. In the case of a small inventory, the entity may choose to focus on the entire inventory.
4. Any additional storage measures. If the material is stored in tamper evident systems, the entity may choose to count the sealed containers instead of the individual vials within those containers.

5. The size of the collection being audited and the manner it is stored. Inventories which are intermixed with other samples may require a 'vial by vial' audit.

Select agent inventories should be confirmed, at a minimum, annually. For those inventories with frequent access, regardless of the number of individuals accessing, it is recommended that inventory records are confirmed semi-annually or quarterly for those specific accessed storage containers.

A suggested best practice is to have two individuals involved in confirming the inventory records to ensure counts are accurate and verified. Each individual could record their respective inventory counts on an inventory verification worksheet with initials or signatures indicating the verification. If two individuals cannot be involved in the verification count, then one individual conducting the select agent inventory confirmation could conduct two counts of the inventory and record both counts on the inventory verification worksheet to provide verification of an accurate inventory count. Sealed boxes should have the security tape identification confirmed. There should be a record available of a vial-by-vial inventory being conducted at the time of the box being sealed. If there are doubts of the sealed box contents then the box should be opened and a confirmed inventory identification and count conducted and recorded. Frequency of the inventory confirmation may vary depending upon how often inventories are accessed and the manner of storage.

For those inventories that contain a mixture of varying agent identifications, or inventories with multiple individuals frequently accessing storage areas, it is recommended that quarterly inventory confirmations are conducted for those storage containers involved in such access occurrences. During the quarterly, semi-annual, or annual inventory confirmation, those containers which are accessed and having inventory added or removed should have all vials or containers in those specific storage boxes/containers counted and confirmed. The percentage of additional inventory that is to be confirmed on an annual basis will vary with the inventory size. Laboratories with large inventory volumes should confirm inventories for any storage boxes/containers accessed throughout the year. Inventory collections containing lesser quantities of material and routine access should have the entire inventory confirmed at least on an annual basis.

See the Inventory Audit Conditions table for more detailed instructions for when an inventory audit is necessary.

Maintain audit records in accordance with section 17(c). Changes to the inventory must be recorded in accordance with section 17(a) as well.

EXHIBIT 'D'

Section 11(f) – Tier 1 Security

Tier 1 select agents and toxins require additional security measures to be implemented including the addition of pre-access suitability assessments, extra access controls, and extra barriers. These extra measures are intended to safeguard Tier 1 select agents and toxins further from theft, loss, or release. The list of Tier 1 select agents and toxins includes:

- *Bacillus anthracis*
- *Bacillus cereus* Biovar *anthracis*
- Botulinum neurotoxins
- Botulinum neurotoxin producing species of Clostridium
- *Burkholderia mallei*
- *Burkholderia pseudomallei*
- Ebola virus
- Foot-and-mouth disease virus
- *Francisella tularensis*
- Marburg virus
- Rinderpest virus
- Variola major virus (Smallpox virus)
- Variola minor virus (Alastrim)
- *Yersinia pestis*

An effective security plan for Tier 1 BSAT describes how the requirements of the regulations are met. The security plan should also discuss who manages security control measures. This may include:

- How the entity manages access controls – This management may include keys, card keys, access logs, biometrics and other access control measures for each of the security barriers in the security plan. This may be accomplished by directly controlling or interacting with a service provider (e.g., a security guard company).
- Designating personnel to manage the entity's security systems, including intrusion detection
- How the intrusion detection alarm code is managed (who has it, when it is changed)
- How the entity tests and manages the configuration of the system
- How the entity responds to an access control or intrusion detection failure (e.g., alarm)
- How the entity screens visitors

Section 11(f)(1) – Pre-Access Suitability Assessment

The entity must develop, implement, and describe in the security plan procedures for conducting a pre-access suitability assessment of persons who will have access to a Tier 1 select agent or toxin. See the Guidance on Suitability Assessments. Individuals must have a pre-access suitability assessment conducted before they are allowed access to Tier 1 select agents and toxins.

Section 11(f)(2) – Responsible Official Coordination with Other Safety and Security Professionals

Entities must describe procedures for how an entity's Responsible Official (RO) will coordinate their efforts with the entity's safety and security professionals to ensure security of Tier 1 select agents and toxins and share, as appropriate.

Ideally the entity's RO, safety, and security professionals should meet on a regular or defined basis. This may be annually in conjunction with the security plan review, after a security incident, when there is a significant entity change that affects security, or in response to a threat. See **Figure 2** for an example of the personnel who should be involved in creating a security plan for entities registered to possess or use Tier 1 BSAT.

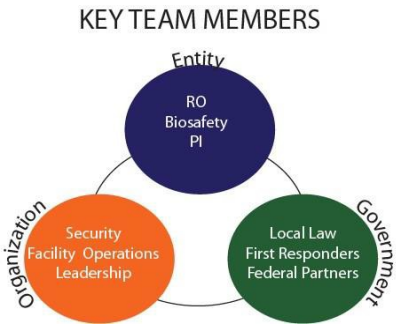


Figure 2: Tier 1 BSAT Security Plan Team

Section 11(f)(3) – Ongoing Suitability Assessments

Describe procedures for the ongoing assessment of the suitability of personnel with access to a Tier 1 select agent or toxin. See the Guidance on Suitability Assessments. The procedures must include:

- Self-Reporting – Individuals should be trained on how to report any incidents or conditions that might impact their ability to safely have access to select agents and toxins and to safeguard them from theft, loss, or release.
- Peer-Reporting – Individuals should be trained on how to report incidents or conditions that might impact the ability of others to safely have access to select agents and toxins. Peer-reporting should be safe and anonymous and protect whistle-blowers from repercussion.
- Employee Training – All employees must be trained on the entity's policies and procedures for reporting, evaluating, and corrective actions concerning suitability assessments. This type of training may include threat awareness, self- and peer-reporting, behaviors of concern, and suitability policies.
- Ongoing Suitability Monitoring – All individuals with access to Tier 1 select agents and toxins must undergo ongoing suitability monitoring. There are several ways to achieve this, including annual performance reviews, access reviews, and criminal record reviews.

Section 11(f)(4) – Security Enhancements

Entities that possess Tier 1 select agents and toxins must adhere to extra security enhancements, including access limitations, extra barriers, intrusion detection system, and visitation policies.

Section 11(f)(4)(i) requires the entity to limit access to a Tier 1 select agent or toxin to only personnel who have been approved by the HHS Secretary or APHIS Administrator, following a security risk assessment (SRA) conducted by the Attorney General, and have had an entity-conducted pre-access suitability assessment. Such individuals must also be enrolled in an ongoing suitability assessment program conducted by the entity.

- Make sure that only HHS or USDA approved individuals have access to Tier 1 BSAT.
- Conduct a pre-access suitability assessment before granting access.

- Enroll each individual to be given access to Tier 1 BSAT in an ongoing suitability assessment program.

Access Outside Normal Business Hours

Section 11(f)(4)(ii) requires the entity to limit access to registered spaces outside of normal business hours. Only individuals who have been specifically approved by the RO, or his/her designee, may be allowed to access laboratories or storage facilities containing Tier 1 select agents and toxins outside of normal business hours.

Limiting access to registered spaces outside of normal business hours does not mean that personnel cannot work outside these hours; however, they should get specific approval by the RO, or his/her designee, before doing so. The entity may choose to establish specific after-hours work policies. For example, the entity could establish a rule that states at least 2 persons should be working in the laboratory if work must be conducted after hours. This rule should consider, and implement, any necessary justification for after-hours work, such as 24 hour animal studies.

Security Barriers

Section 11(f)(4)(iv) of the select agent regulations requires a minimum of three security barriers safeguarding Tier 1 select agents and toxins against theft, loss, or release. A barrier is a physical structure designed to prevent unauthorized access. Cameras, security lighting, and IDS are not considered security barriers because, while they may monitor and detect unauthorized access, they cannot, by themselves, prevent access. These security barriers must be identified on the entity's registration (APHIS/CDC Form 1) and described in the security plan.

Examples of Acceptable Security Barrier Implementations

Ex.	Barrier 1	Barrier 2	Barrier 3 (linked to access approval)
1.	Guard/Perimeter Fence	Card-Key Access to floor	Key locked container with strong key control measures
2.	Building Card Key Access	Limited Room card-key access	Different card-key required for room
3.	Building Card Key Access	Limited Room card-key access	Card-key PIN access room
4.	Building Card Key Access	Limited Room card-key access	Biometric lock system on freezer
5.	Building Card Key Access	Card-key PIN access room	PIN access to freezer
6.	Building Card Key Access	Limited Room card-key access	Restricted card key access to registered space
7.	Floor Card Key Access	Limited Room card-key access	Restricted card key access to registered space

Security barriers should be implemented based on a site-specific risk assessment and should ensure that the following conditions are met:

- Each security barrier must add to the delay in reaching the areas where select agents and toxins are used or stored. Most security barriers, in and of themselves, do provide additional delay to forced entry.
- All access points, including emergency exits, must be secured. If there is a card key lock on the main door, the emergency exit should be secured to prevent ingress – for example, by having no outside handle.
- One of the security barriers must be monitored in such a way as to detect circumvention of established entry control measures under all conditions. This may include video cameras, monitoring access control

EXHIBIT 'D'

logs from a card key reader or other methods of regular monitoring.

- The final security barrier must limit access to the select agents and toxins to personnel approved for access by the HHS Secretary or APHIS Administrator.
- Per section 11(f)(4)(i), the entity must ensure access to the Tier 1 BSAT is limited to those who have undergone the entity's pre-access suitability and are subject to ongoing suitability assessment. Access records can be used to show that only access approved personnel have accessed the final barrier.

Personnel who are trained to identify and respond to suspicious activities can be considered a security barrier. Persons who receive 'insider threat,' 'suspicious person' or similar training along with response procedures (i.e., calling security, 911, etc.) are considered 'trained personnel.' Therefore, when they are physically present, they may be considered a security barrier.

Intrusion Detection Systems

Section 11(f)(4)(v) requires the entity to ensure that all registered spaces containing Tier 1 select agents or toxins must be protected by an intrusion detection system (IDS) unless the area is physically occupied. An IDS consists of a sensor device which triggers an alarm when a security breach occurs notifying a response force (e.g., local police, security guard force, etc.) who have the capability to respond to the alarm and stop a threat.

Section 11(f)(4)(vi) requires that personnel monitoring the IDS must be capable of evaluating and interpreting the alarm and alerting the designated security response force or law enforcement. Some response options include:

- Personnel employed by the entity (an alarm or security operations center)
- Contracted alarm company
- Local law enforcement
- Military police unit
- Dedicated entity personnel

If the IDS is monitored by a service provider with a local law enforcement response, the entity should coordinate with local law enforcement to assist them in understanding the importance of the information from the service provider. For example, due to the volume of false alarms, local law enforcement may not treat the alarm as a serious matter. Entities are encouraged to discuss the consequence of the theft of a select agent or toxin with local law enforcement so they can understand the seriousness of the threat and also understand that an alarm at an entity housing select agent requires immediate response.

Intrusion Detection Response Times

Section (11)(f)(4)(viii) requires the entity to determine response times for security forces or the local police to Intrusion Detection Systems. The response time must not exceed 15 minutes from the time that an alarm sounds or a security incident is reported to the arrival of the responders at the first security barrier.

A response force is a force capable of interrupting a threat. It may be unarmed guards, armed guards and/or local law enforcement – though law enforcement is preferable.

The target for response time, 15 minutes or less, is based on the Department of Defense adopted standards for protecting high consequence assets. However, entities are strongly encouraged to coordinate with local law enforcement and/or federal partners to assist with threat assessment to determine the appropriate response

time. Local law enforcement, especially in areas where the response time is challenging, will often assist the entity in determining how long the barriers will delay an adversary.

There are many ways to reduce response time for the response force to less than 15 minutes. One method is to perform the following steps:

- Discuss regulatory requirements and strategies with local law enforcement.
- If you have a dedicated guard force, work with them (generally, you will meet this requirement with a dedicated guard force).
- Calculate the delay time provided by entity security barriers and compare it to the expected response time of the response force. Get the typical response times from the responding personnel and compare it to the delay times determined through scenarios.
- Conduct an exercise with local responders.

Though not required, entities should consider the effect of natural hazards, such as a hurricane or blizzard, when addressing response times.

Access Control Systems

Section (11)(f)(4)(vii) requires the entity to describe procedures to ensure that security is maintained in the event of the failure of access control systems due to power disruption affecting the registered spaces.

In the event of an incident that disrupts or cuts off power to the registered space, the entity must have a plan in place to ensure that security is maintained, and three physical barriers will remain in place, until power can be restored. Some acceptable methods include:

- Fail-safe locks that are locked or remain locked when power is interrupted or there is a power outage.
- Adding personnel/guard forces at doors that acts as one of the three physical barriers but may fail and open instead of being closed/locked in the event of a power failure.
- Backup generators or batteries that will restore power to the access control systems.

For example, if power is lost and the door locks (even if it can be opened only from the inside), then it meets this requirement. If power is lost and the door unlocks (it can be opened from the outside), then it does not meet the “fail safe” requirement.

Depending upon the access control systems (ACS) and equipment, the entity should consider changing lock combinations, ACS password/PIN, intrusion detection system (IDS) password/PIN, and access approvals in which the departing personnel was assigned when they are removed from the program and/or access to Tier 1 select agents. Former employees that retain the ability to use and control the locks, ACS, and the IDS would be considered a vulnerability.

Section 11(f)(5) – Security Enhancements

Entities that possess Variola major virus, Variola minor virus (9 C.F.R. Part 121), foot-and-mouth disease virus and rinderpest virus (42 C.F.R. Part 73) must have additional security requirements as outlined in the select agent regulations.

Section 11(h) – Review and Revision

The security plan should be reviewed at least annually and revised as necessary. Some events that may necessitate the review and revision of the security document include:

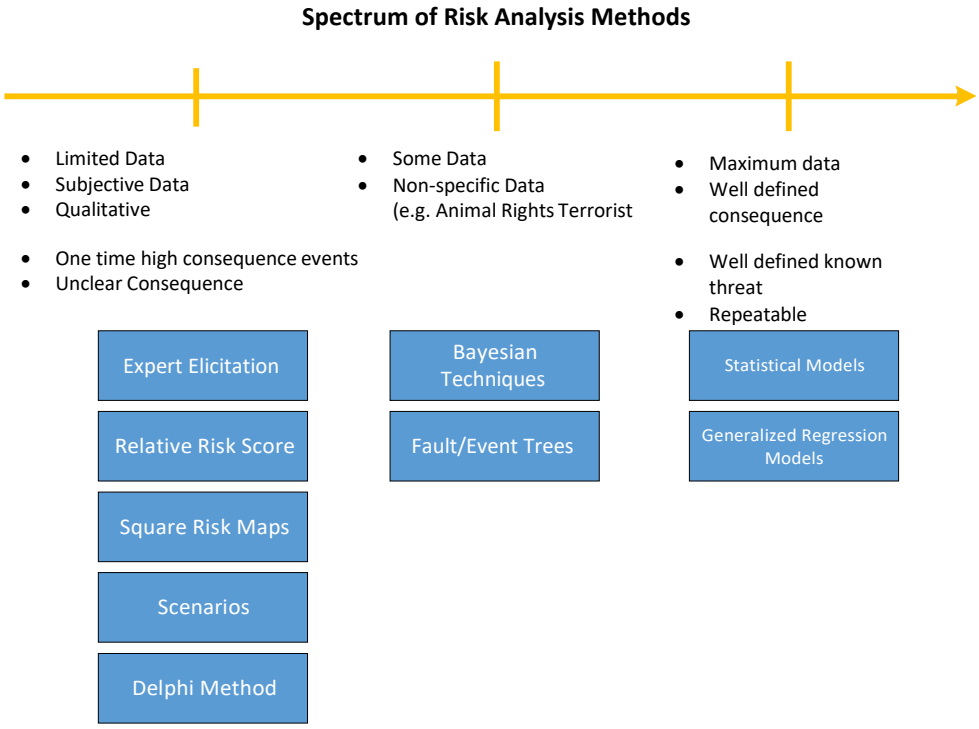
- Theft, loss, or release of a select agent or toxin
- Changes to entity registration
- Changes to the registered space
- Changes to relevant entity personnel
- Any training assessments, drills, or exercises that may change along with a change to the security plan must also be updated. In addition, all drills and exercises should be documented to include How the plan was tested and evaluated (i.e. objectives and goals for the exercise or drill)
- Problems identified in corrective action
- Names of personnel who participated i.e. sign-in sheets

For more information, see the Drills and Exercises guidance document.

EXHIBIT 'D'

Appendix I: Risk Assessment Methods

There are several methods for determining risk. Any recordable method is acceptable, as long as the entity determines risk as the intersection between threat, likelihood, and consequence. The National Academies of Science describes different methods of risk analysis as being on a spectrum, like those in the following table. More qualitative methods are on the left while quantitative, data-reliant methods are toward the right.



For example, the square risk map is a qualitative analysis method that relies on a common sense understanding of the combination of threat and vulnerability with the consequence of such an incident occurring.

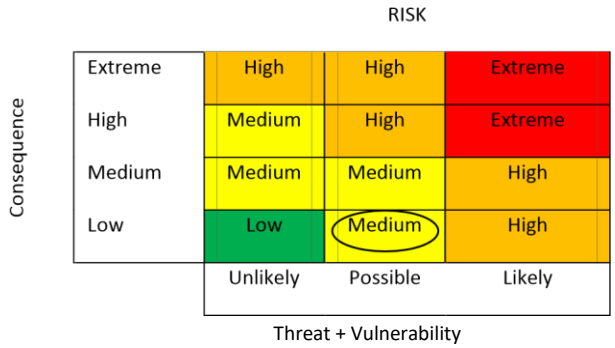


Figure 1: Square Risk Maps assess risk by comparing the threat and vulnerability of a situation to the consequence. The risk is assessed as Low, Medium, High, or Extreme.

EXHIBIT 'D'

Similarly, the relative risk score method numerically scores threats and vulnerabilities compared to the consequence of a given scenario and plots the risk according to a set range of risk levels.

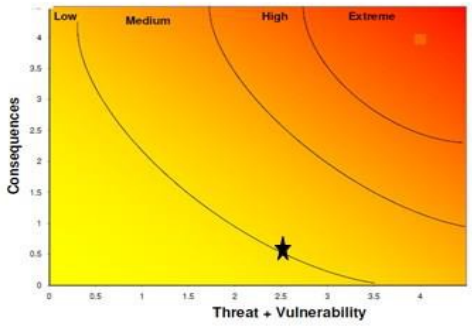


Figure 2: Example "Relative Risk Score"- This method assesses risk by numerically scoring threats and vulnerabilities compared to the consequence of a given scenario.

EXHIBIT 'D'

Appendix II: Access Control Devices

Lock Type	Physical Security Requirement	Additional SRA Requirements
Mechanical Key	• All keys must be tracked in a log. • Change locks if key is lost or compromised. • All keys must be returned when people quit or are terminated. • Log access and retain for 3 years. • If the key is secured in a key box, the key box key must meet the requirements above.	• All personnel with access to the key must have SRAs. • If in a key box, all personnel with access to the key box key must have an SRA. • If there is no IDS, the following people must have SRAs: • All personnel with access to a master key. • All personnel with access to a facility or building grand master. • Entity locksmiths if they have or can make the key and the key can be traced to the door.
Cipher Key/Combination lock	• Change the code or lock when personnel quit or are terminated. Changes must be reflected in a log. • Change the code or lock in the event of compromise. • Log access to registered areas and retain access records for 3 years.	• All personnel with the code/combination or access to the code/combination must have SRAs. • If there is no IDS, the following people must have SRAs: • All personnel who can change the code.
Card Key	• Maintain electronic or physical logs of access to registered areas for 3 years. • The log must be capable of being printed. • The access control network must meet the information security requirements.	• All personnel with card-key which can open door • (includes facility wide keys)
Card Key+ Pin	• Maintain electronic logs of access for 3 years. • The access control network must meet the information security requirements.	• No additional requirement
Biometrics	• Maintain electronic logs of access for 3 years. • The access control network must meet the information security requirements.	• No additional requirement
Multiple kinds of access control (i.e., Card Key and Mechanical Lock on same door)	• All the requirements for each type of access control systems when or if used.	• All the SRA requirements for both systems unless use of the access control device triggers the IDS (use of a mechanical key in Card-Key door will often trigger a 'forced door' alarm. The same alarm if someone broke the door down).
Remote opening (e.g., someone 'buzzes' a person in)	• Maintain electronic logs of access for 3 years. • The access control network must meet the information security requirements.	• No additional requirement
"Emergency" card key kept with First Responders	• Log of access. • Inventory of key. • Notification of the RO and FSAP in the event of its use.	• No SRA requirement for first responders
Emergency mechanical key or Card-Key in Knox Box (key stored in secured 'box' only accessible to first responders)	• Maintain electronic logs of access for 3 years. • Notification of the RO and FSAP in the event of its use.	• No SRA requirement for first responders

EXHIBIT 'D'

Appendix III: Intrusion Detection Systems

Systems	Definition	Possible Uses	Questionable Uses	Dependencies
Infrared motion detector	A device that detects a change in ambient temperature (heat sensor)	-Inside registered areas -Along a hall that leads to registered areas -Doors that lead to registered areas -Storage freezers	-Areas where things are heated (warming) - Very large areas	Ensure that system is focused at key areas and not 'randomly' located throughout entity
Contact Switches	Devices that alarm when a circuit is broken (door or window opened)	-Inside registered areas -Along a hall that leads to registered areas -Doors that lead to registered areas -Storage freezers	Areas with glass windows or doors that provide direct access to registered area	Ensure the emergency exit has an alarm and windows have sensors
Broken Glass Sensors	A device that detects the sound frequencies generated by breaking glass.	-Laboratories with glass windows which provide access to registered space	-Entities where there are frequent severe storms -Entities with synthetic windows	Ensure all the doors also have a sensor.
Acoustic Motion Sensor (emits sounds)	An active device that detects motion by transmitting sounds that reflects off objects	-Inside registered areas -Along a hall that leads to registered areas -Doors that lead to registered areas -Storage freezers	-Animal rooms -Rooms where equipment is continuously left on or after work hours (i.e., shakers, incubators) - Very large areas	Ensure that system is focused at key areas and not 'randomly' located throughout entity
Acoustic Sensor (listens for sounds)	A passive device that monitors the sounds to determine when an intrusion occurs and/or to determine the nature of the intrusion	-Inside registered areas -Along a hall that leads to registered areas	-Animal rooms - Rooms where equipment is continuously left on or after work hours (i.e., shakers, incubators) -Entities without exterior sound dampening	Ensure exterior noises do not set the alarm off (i.e., animals in the laboratory next door)

EXHIBIT 'D'

Appendix IV: Intra-Entity Transfer Template

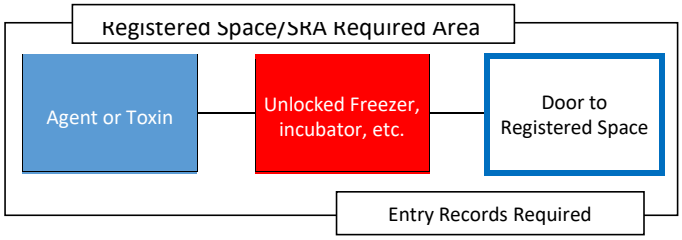
SELECT AGENT/TOXIN	STRAIN / CHARACTERISTICS	QUANTITY TRANSFERRED	DATE OF TRANSFER	SENDER	RECIPIENT

Comments:

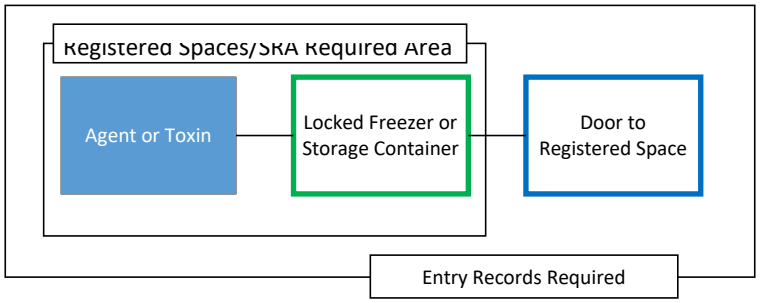
EXHIBIT 'D'

Appendix V: Scenarios (Non-Tier 1 Barriers and Access Controls):

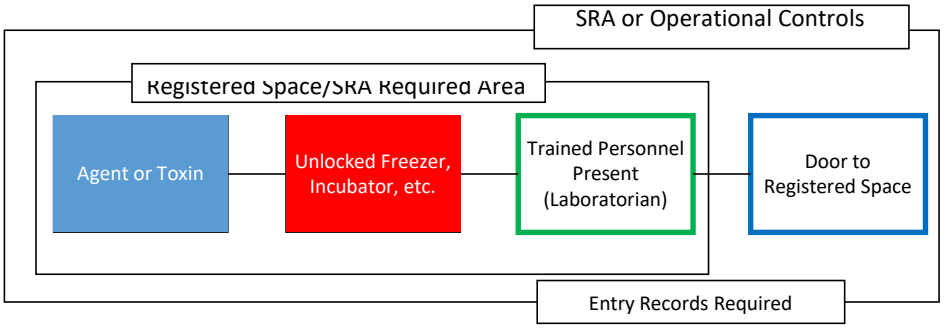
Scenario 1: Typical Working Facility



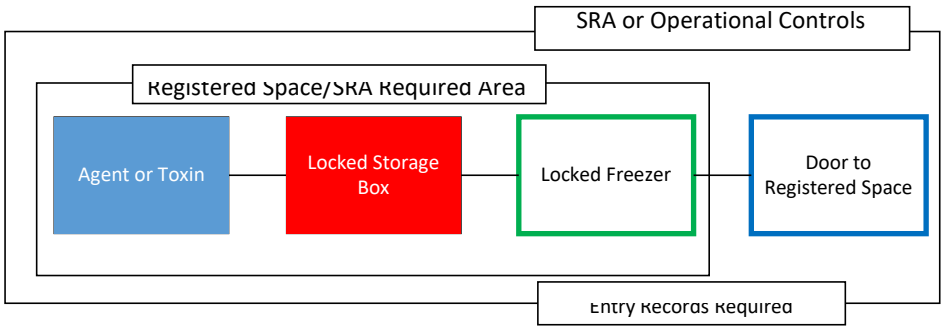
Scenario 2: Storage Only



Scenario 3: Working with Select Agent or Toxin in Shared Space



Scenario 4: Locked Box Inside Freezer



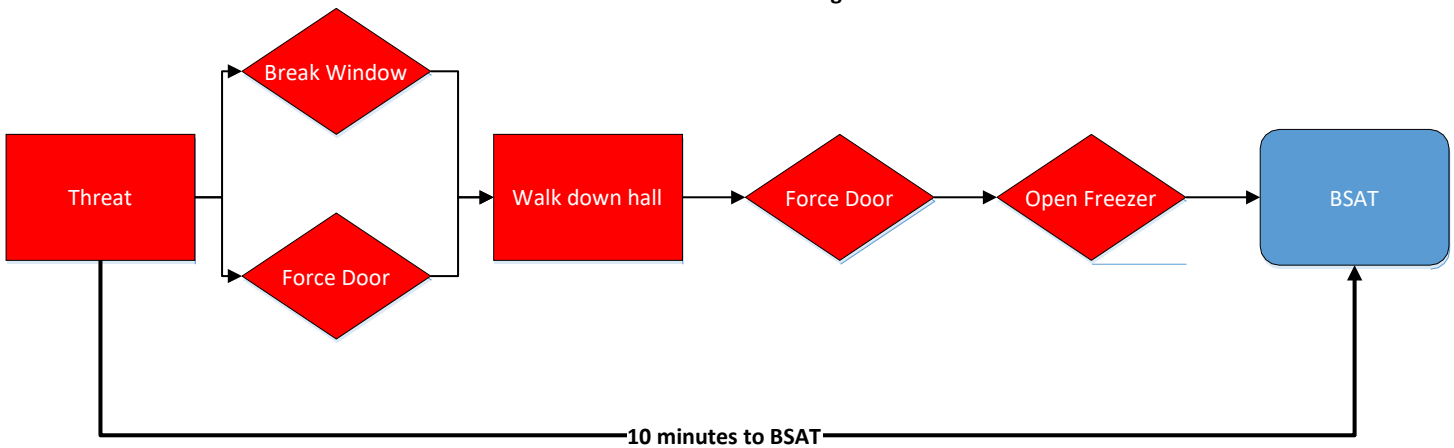
Operational controls are controls in place specifically to prevent unauthorized access to any select agent or toxin. Appropriate operational controls are based on the nature of all work in the registered area, the physical features in the area, and the entity's risk assessment.

EXHIBIT 'D'

Outsider Threat

Barriers deter but cannot be relied on to stop an outsider. The outsider cannot be stopped by locks, doors or other barriers, only delayed. The only thing that will stop an outsider is a response force.

Threat Task Time without Mitigation



Threat Task Time with Mitigation

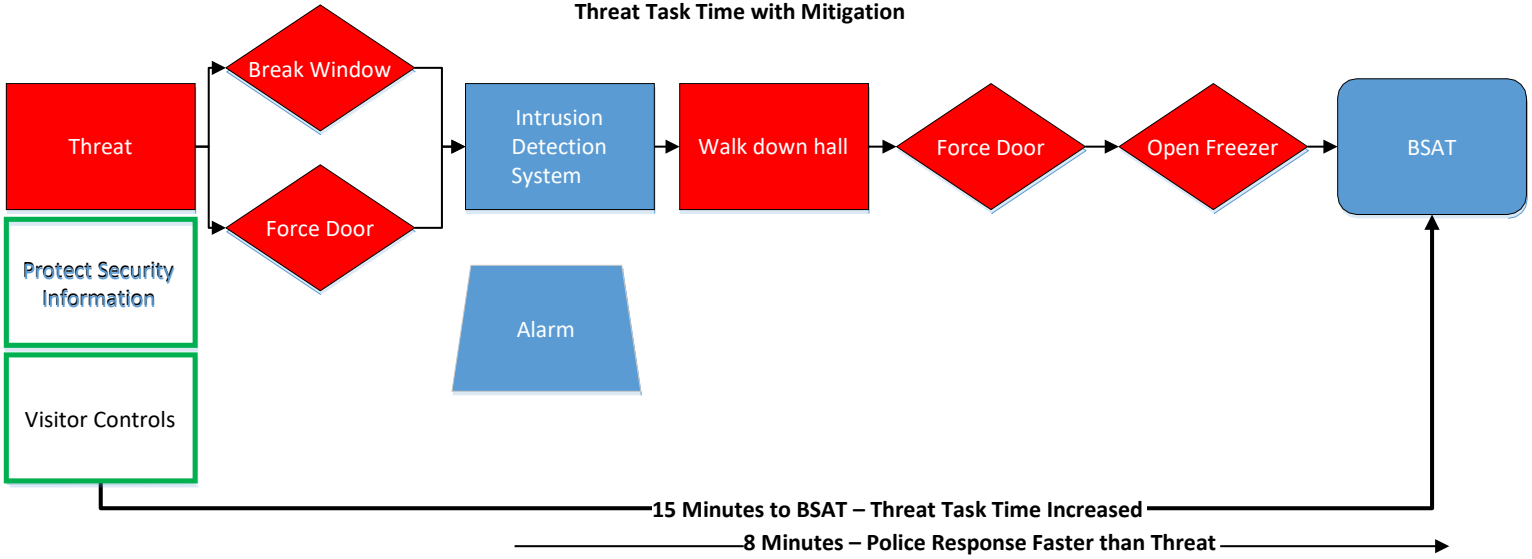


EXHIBIT 'D'

Select Agent or Toxin Inventory Template

AGENT OR TOXIN NAME: CHARACTERISTICS:

QUANTITY ACQUIRED: DATE OF ACQUISITION: SOURCE OF ACQUISITION:

INITIAL QUANTITY:

WHERE STORED:

BUILDING: ROOM: FREEZER:

INVENTORY OF USAGE

CURRENT QUANTITY	DATE REMOVED FROM STORAGE	QUANTITY REMOVED	REMOVED BY	USED BY	DATE RETURNED TO STORAGE	QUANTITY RETURNED	RETURNED BY	PURPOSE OF USE	DATE DESTROYED	QUANTITY REMAINING

Comments/Discrepancies: _____

_____

_____

_____

_____

EXHIBIT 'D'

Inventory Audit Conditions

Circumstance	Suggested audit
Emergency movement inside the same registered area	Audit not required if there is no evidence loss or theft.
Emergency movement to a different registered area	100% check of sealed containers for indication of tampering. 10% of the entire inventory which is not sealed. Audit commences after the move is complete.
Loss	100% of all samples in that PI's collection and/or any other inventory in shared freezer space. Audit commences immediately (within 48 hours) after the event.
Theft	100% of all samples in that PI's collection and/or any other inventory in the shared freezer or space. Audit commences immediately (within 48 hours) after the event.
Addition or removal of a PI from the registration. Or Transfer of inventory from or to another PI.	100% of the samples in that PI's collection. 100% check of sealed containers for indication of tampering. Audit commences as soon as possible after the arrival/removal of the investigator or as soon as practical thereafter.
Planned movement to a different registered area	100% check of sealed containers for indication of tampering. 10% of the entire inventory which is not sealed. Audit commences after the move is complete.
Planned movement to a different registered area a different building, campus, facility.	100% of all samples manipulated since the last inventory. 100% check of sealed containers for indication of tampering. Audit commences after the move is complete.

EXHIBIT 'D'

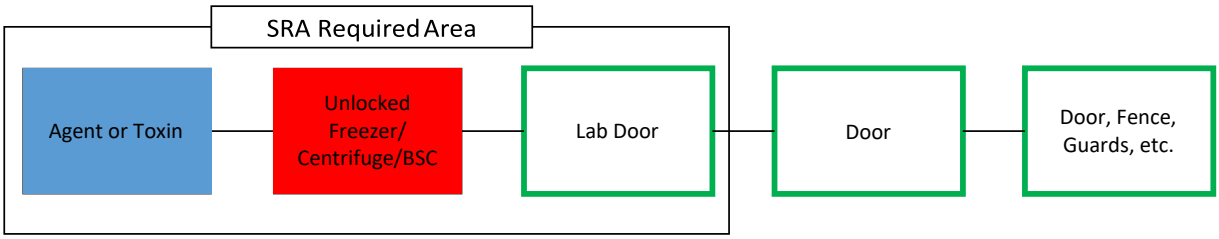
Entities may also choose to consider inventory when following conditions occur:

Condition	Inventory
Laboratorian or support staff removal from registration	10% of the samples in that PI's collection that the individual worked with. 100% check of sealed containers for indication of tampering. Audit commences as soon as practical after the person is removed.
Destruction of agents	100% of the agents being destroyed.

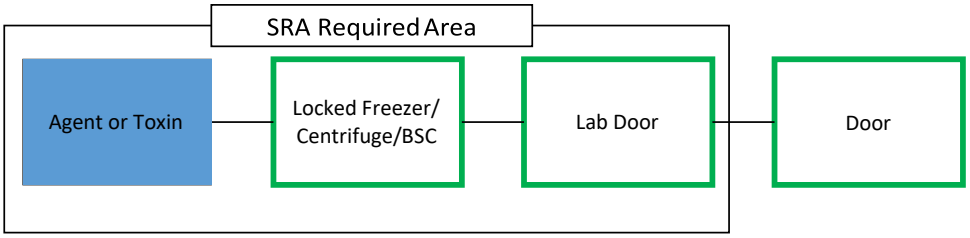
EXHIBIT 'D'

Tier 1 Barrier Scenarios

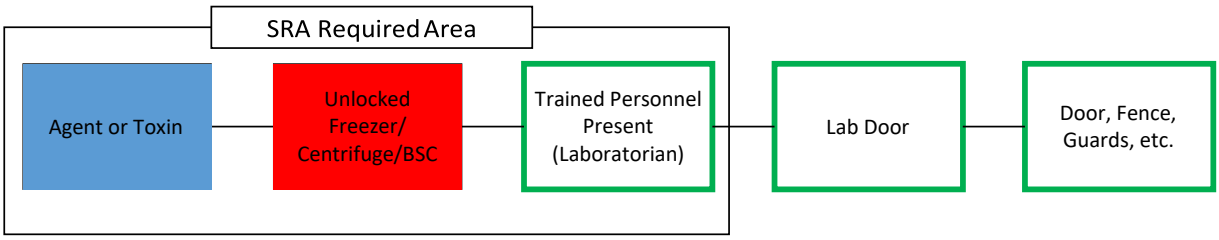
Scenario 1: Typical Working Facility



Scenario 2: When in Storage



Scenario 3: Working with Agent or Toxin



Scenario 4: Locked Box

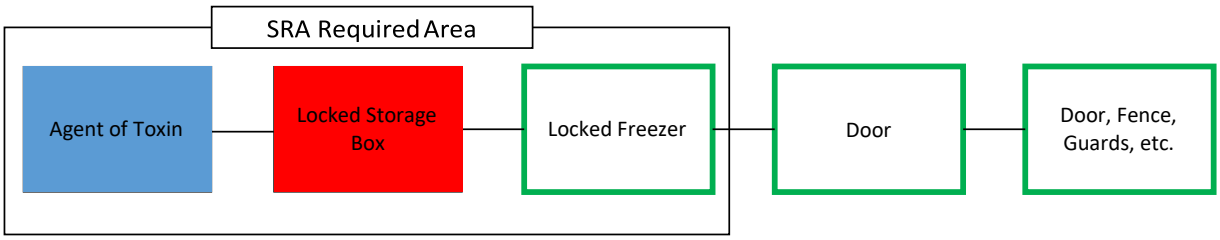


EXHIBIT 'D'