APHL ASSOCIATION OF PUBLIC HEALTH LABORATORIES

JULY 2026

Laboratory Preparedness Exercises

A Toolkit for Public Health and Clinical Diagnostic Laboratories

This toolkit is designed to equip laboratories with the knowledge and resources necessary to enhance biosecurity and preparedness practices within their facilities, strengthen existing protocols or establish new ones, and build capabilities that support effective prevention, response and recovery from a wide range of incidents, including biological threats, extreme weather events, information technology disruptions and other operational emergencies. By providing biosecurity and preparedness exercise examples and exercise design and development sections throughout the tool, the Association of Public Health Laboratories (APHL) aims to empower laboratories to proactively identify vulnerabilities, test operational capabilities and strengthen coordination across safety, security and emergency response systems. Our intent is to foster a proactive approach to laboratory operations, emphasizing prevention, preparedness, response and continuous improvement. We encourage all users to engage with the exercises, leveraging insights gained to strengthen their laboratory's readiness to manage biosecurity threats, biological incidents and other operational disruptions that could impact laboratory functions.

Contents

Background

Every laboratory must take steps to protect the environment, facility, personnel, and any samples or confidential information in its care. To ensure sufficient safeguards are in place laboratories must train personnel, assess competency in the desired knowledge and skills, and test the engineering and administrative systems designed to protect critical assets. The purpose of this toolkit is to provide guidance, preparedness resources and practice exercises for developing laboratory biosecurity and preparedness drills and exercises. These drills and exercises assist laboratories by testing their ability to prevent, detect and respond to potential threats, including the loss, theft, misuse, diversion, unauthorized access or intentional release of biological agents, as well as other incidents that may disrupt laboratory operations.

Events such as the 1984 Rasjneeshee Bioterror Attack, the 1996 Dallas biocrime committed by a clinical laboratory scientist, and the 2001 Amerithrax mailings, along with the ongoing, expressed threat of bioterrorism by terrorist groups and radicalized individuals demonstrate vulnerabilities to acts of bioterrorism and biocrimes and the importance of laboratory biosecurity training. These events have prompted laboratory leadership to evaluate the need for creating, implementing, and/or enhancing the security measures and preparedness planning for biological agents and toxins in their facilities.

To mitigate these threats, the Federal Select Agent Program (FSAP)—managed through the US Centers for Disease Control and Prevention's (CDC) Division of Select Agents and Toxins and the Animal and Plant Health Inspection Service's Agriculture Select Agent Services—regulates the acquisition, use, storage and transfer of select agents and toxins through the development, implementation and enforcement of the federal Select Agent Regulations. FSAP is currently the only federal program requiring the development of a laboratory biosecurity program; however, the list of biological materials that could be misused for malicious purposes extends beyond the list of Select Agents and Toxins. Therefore, while not all laboratories are registered under FSAP, the application of laboratory biosecurity and preparedness principles may enhance overall laboratory management, operational resilience, safety and security.

Under FSAP, registered entities are required to conduct drills or exercises once per calendar year to test and evaluate the effectiveness of their security, biosafety and incident response plans. This regulatory requirement is specified in the Select Agents and Toxins regulations (42 CFR Part 73, 9 CFR Part 121 and 7 CFR Part 331) in sections 11 (Security), 12 (Biosafety) and 14 (Incident Response).[a]

All laboratories—regardless of specific regulatory requirements—should conduct biosecurity and preparedness drills and exercises to ensure biological materials that pose a threat to public health and safety are safeguarded from malicious use. It is important for laboratories to establish training and exercise programs that educate staff on their responsibilities for maintaining biosecurity within the institution, assess staff competency and knowledge, and test critical engineering and administrative controls to minimize the risk of a biosecurity incident.[b]

a Drills and Exercises Guidance (selectagents.gov)
b Biosafety in Microbiological and Biomedical Laboratories—6th Edition (cdc.gov)

Exercise Design and Development

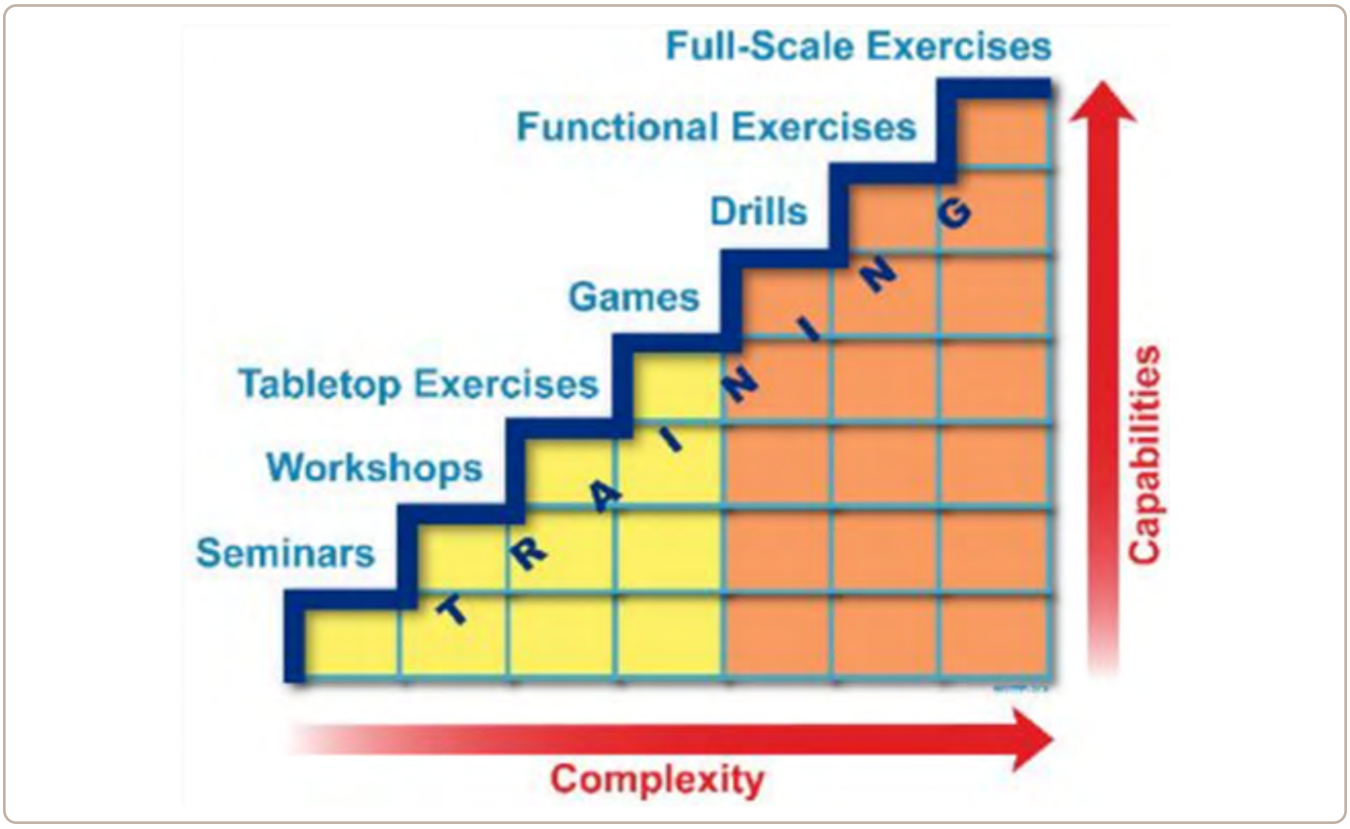
Practice exercises serve as a helpful tool for evaluating preparedness and response to a variety of scenarios, such as loss or theft of materials, emergency response to accidents and injuries, incident reporting, and identification of and response to security breaches. Importantly, exercises should provide an opportunity to identify gaps in training and knowledge, as well as inadequate procedures, capabilities and systems, without placing blame on any party for the identified shortcomings, as the goal of any exercise is to identify and minimize biosecurity vulnerabilities.

When designing institution-specific biosecurity drills and exercises, performing a threat and vulnerability assessment can be helpful to create a list of potential biosecurity scenarios that could occur at the facility. Each scenario should consider the item(s) involved, potential internal and/or external human threats, response and protective measures in place. It is important to also assess any vulnerabilities in the current protective measures and identify how they could be breached.

A thorough threat and vulnerability assessment also evaluates the probability of each scenario materializing and its associated consequences, allowing laboratory leaders to prioritize resource allocation where it is needed most. The outcome of this process may also help identify specific scenarios that warrant exercising due to the overall threat they pose to laboratory biosecurity and operational capacity.

There are multiple types of exercises that can be designed to review or validate policies and procedures within an institution. These exercises fall under the general categories of either discussion-based or operations-based. To best monitor exercise observation and data collection, it is recommended to begin conducting discussion-based exercises and gradually progress to operations-based exercises. As the exercises become more complex, the capabilities required to carry them out also increase, as seen in **Figure 1**.

FIgure 1. **Complexity vs Capabilities in Discussion- and Operations-based Trainings**



Discussion-based Exercises

Discussion-based exercises are designed to create an environment where players can present key concepts, create products, familiarize themselves with plans, policies or procedures and apply strategies. Types of discussion-based exercises include:

- **Seminars:** Seminars are useful for orienting participants on plans, policies and procedures. They can be lectures, panels or discussions to present concepts and ideas. The ultimate goal is to ensure participants retain and comprehend objectives being presented.
- **Workshops:** Workshops are used to develop plans, policies or procedures. The objective is to engage participants in a collaborative process that results in the creation of information or specific products, such as a draft plan or policy.
- **Tabletop Exercises (TTX):** TTX offer an opportunity for a facilitated discussion that drives player dialogue about a specific scenario. They are intended to facilitate a conceptual understanding, identify strengths and areas for improvement, or validate plans, policies or procedures. Equipment and resources are not used in these exercises, and time pressures are not introduced. The goal of a TTX is to apply, analyze and evaluate the plan, policy or procedure rather than the effectiveness of plans or competency of staff to carry out a physical response.
- **Games:** Games are designed for individuals or teams in a competitive or non- competitive environment. They are guided by clear rules, data and procedures, and can be used to reinforce training, stimulate team building, or enhance operational and tactical capabilities. The goal is to analyze and evaluate the impacts of decision making during an incident.

Operations-based Exercises

Operations-based exercises validate plans, policies, agreements and procedures; clarify roles and responsibilities; and identify resource gaps in real-time or in an operational environment. Types of operations-based exercises include:

- **Drills:** Drills are used to validate a single operation or function, such as evaluating a new piece of equipment or verifying new procedures. A drill is a coordinated, supervised exercise activity, and has a narrow focus to test a single specific operation or function.
- **Functional Exercises (FE):** FEs are fully simulated interactive exercises designed to assess and evaluate capabilities in a realistic, real-time environment. The exercise tests multiple functions of your emergency management and response. FEs focus on the coordination, integration and interaction of an organization's policies, procedures, roles and responsibilities before, during or after the simulated event. Functional exercises make it possible to examine and/or validate the coordination, command and control between various multi-agency coordination centers without incurring the cost of a full-scale exercise or involving outside responding agencies. A functional exercise should often be a prerequisite to a full-scale exercise.
- **Full-scale Exercises (FSE):** FSEs are the most complex and resource-intensive exercise. They often involve multiple agencies, jurisdictions or organizations, and real time movement of resources and people. They are distinguished by realistic environments intended to mirror a real and complex incident response. To accomplish this realism, it requires the mobilization and actual movement of emergency personnel, equipment and resources. Ideally, FSEs would test and evaluate most functions of your damage assessment plan on a regular basis; however, because they can be expensive and time consuming, they should be reserved for the highest priority threats and vulnerabilities.[a,b]

a Types of Training and Exercises (fema.gov)
b Homeland Security Exercise and Evaluation Program (HSEEP)

Exercise Evaluation

Once exercises have been completed, an after-action review or "hotwash," will take place to discuss the exercises performed and allow participants to provide feedback. Following the hotwash, the evaluation team will meet to analyze the data, identify strengths and areas of improvement, and adjust procedures and protocols. The information from the evaluation team helps generate information that will go into an after-action report and improvement plan (AAR/IP). The ARR/IP summarizes outcomes of exercises and provides exercise overview, observations, analysis of capabilities and corrective actions. It is critical to identify improvement strategies that are achievable in a specific timeframe so that progress can be monitored and documented.

When the ARR-IP is drafted, an after-action meeting will be held with senior leadership from the participating organizations to review and finalize the AAR/IP, generating a final consensus on strengths and areas for improvement. The AAR/IP should provide participants with draft corrective actions, concrete deadlines and implantation plans for recommended corrective actions. Corrective actions should be specific, measurable, achievable, relevant and time-bound (SMART) and tracked and reported on until completion.[a]

Upon completion of the discussion and operations-based exercises, several laboratory professional competencies will be demonstrated:

Biosecurity Competencies [b]	Preparedness Competencies [b]
• Recognizing and evaluating potential biosecurity threats • Following established biosecurity measures • Effective emergency response planning • Knowledge of biological safety procedures • Clear and effective communication among personnel • Maintenance of biosecurity equipment • Safe management of biosecurity materials • Continuous improvement of biosecurity regulations and guidelines • Documentation and recording keeping of biosecurity activities.	• Implementation and management of COOP • Evaluation of operational performance during emergency situations • Execution of laboratory emergency response protocols • Safe handling and processing of specimens during emergency events • Surge capacity planning • Clear and effective internal and external communication and coordination

a HSEEP

b Competency Guidelines for Public Health Laboratory Professionals

Training and Exercise Evaluation Form

A training and exercise form can be used during training and exercises specific to laboratory biosecurity and preparedness operations. This section includes a blank template form and an example of a completed form.

Download an editable version of the form for laboratory use.

Training and Exercise Evaluation Form Template

About the Training Exercise

Unit	
Mission	
Evaluator	
Date	
Scenario	

Training Goals and Objectives

Goals	Objectives
• *Desired, long-term outcome(s) driving the need to develop, implement, maintain and exercise a biosecurity program.* • *Goals may include the specific standards (i.e., regulations, institutional policies, competencies, etc.) intended to be met.*	• *Specific, measurable statement describing exactly what the participants must be to do after participating in the exercise to demonstrate the training was effective. Objectives comprise the individual steps to achieving a goal.* • *Training objectives are used to evaluate performance.*

Evaluator and Support Considerations

The following items will be used by evaluators to facilitate, as close as possible, a realistic, safe scenario. Adherence to the intent of the outline is of primary concern, not the item-by-item requirements.

Support Areas	Considerations
Parties Involved in Exercise	*Indicate any personnel involved in the scenario (e.g., program manager(s), biosafety/biosecurity professional(s), laboratory director, etc.).*
Observers of Scenario	*Indicate any additional parties present for or observing the scenario (e.g., security officer(s), etc.).*
Exercise Area	*Identify where the exercise takes place (e.g., secure laboratory area).*
Materials	*Indicate any special devices, training aids, supplies, special equipment required by the evaluator (e.g., SOPs, evaluation template, clip board, stopwatch, PPE, recording device, tablet, video camera, etc.).*
Key References	*Identify important reference documents (e.g., biosecurity plan, NIST cyber security framework, select agent regulations, Federal Select Agent Program security plan guidance, etc.).*
Tips for Controllers	*Provide any instructions or guidance controllers should follow.*
Safety	*Incorporate safety details by emphasizing the importance of ensuring all participants possess knowledge of procedures and the exercise environment.* *Establish a safe word and termination word and prioritize personnel safety over security assets throughout the exercise.*

Exercise/Training, Evaluation Results

Check "Yes" or "No" to indicate whether the condition was met for each task. Other important information should be documented under the comments section, as required by the exercise controllers. The overall proficiency rating for this function is based on the performance of each task, primary training and evaluation standards, and the evaluator's knowledge of procedures and functional judgment to determine if the mission would have been successful in a real situation.

Note: This section will vary based on your facility and entity policies.

Task	Condition	Yes	No

Exercise Outcomes and Comments

Area	Comments
Overall Proficiency Rating	*Indicate how well participants were able to perform the exercise using the following ratings:* ☐ *Able to perform without challenges* ☐ *Performed with some challenges* ☐ *Unable to perform*
Exercise Results	
Major Deficiencies Findings / Recommendations	
Other Significant Information	

Controller Information

Controllers plan and oversee exercise play, handling the setup and operation of the exercise site. Additionally, they assume roles representing organizations or individual not actively participating in the exercise.

Name	
Position	
Signature	
Date	

Example Training and Exercise Evaluation Form

About the Training Exercise

Unit	Special Microbiology Laboratory
Mission	Unauthorized Forcible Access/Theft
Evaluator	Dr. Anita Loop
Date	July 1, 2023
Scenario	Laboratory staff are expecting a visit by a regulatory inspection agency. One day earlier than expected, the program's senior manager arrives at the laboratory with the inspector stating they arrived a day early. Laboratory staff sense something may be wrong, as the senior manager is acting nervous and uncomfortable. Two laboratory staff follow the manager and visitor into the laboratory. The manager is noticeably skipping important steps in the laboratory's visitor entry protocols, like administering visitor training prior to entry into the laboratory. Once inside the secure laboratory the visitor demands to see the biological inventory. They reveal a firearm and demand the staff give them a freezer box of biological assets. Through nearby windows, other staff notice unusual commotion and the hostage situation in progress. They immediately call 911. Step by step scenario from "imposter" perspective: 1. Imposter arrives at laboratory facility and asks for senior manager. 2. Tells senior manager they are an inspector from the regulatory agency. 3. When senior manager questions the early arrival, imposter threatens them with firearm. 4. Imposter is led to laboratory by the senior manager. Additional staff are encountered. Imposter attempts to gain entry to secure laboratory without indicating true intent. 5. Once inside the laboratory, imposter reveals firearms to all staff and instructs them to provide access to a freezer box of biological agents. 6. Imposter intends to leave the facility with the assets, taking a hostage if needed. A getaway car is waiting nearby.

Training Goals and Objectives

Goals	Objectives
1. Laboratory and management staff ensure all unauthorized or suspicious persons are identified and removed from the laboratory as required by the policy/regulation (provide citation, if desired and appropriate). 2. Biosecurity/security provisions detailed in the institutional security plan will prevent unauthorized access, theft, loss, or release of biological materials as required by the policy/regulation (provide citation, if desired and appropriate). 3. Laboratory and management staff ensure the laboratory's security plan meets organizational goals, regulatory requirements, and established standards (SEC 2.00. Security plan. Competency Guidelines for Public Health Laboratory Professionals. (2015) CDC Morbidity and Mortality Weekly Report. Supplement/Vol. 64/No. 1).	1. Understand how to identify and assess an unauthorized or suspicious person and safely remove them from the laboratory. 2. Demonstrate their knowledge and ability to perform the following procedures required to prevent unauthorized entry to the secure laboratory: a. Check visitor credentials and issue guest ID badge. b. Perform visitor training. c. Escort the visitor into secure laboratory spaces. d. Prevent the unauthorized access to security assets (i.e., biological inventory). e. Prioritize safety over security if a dangerous situation develops. f. Notify emergency response services (i.e., 9-1-1) and leadership of the event as soon as possible. 3. Perform subcomptencies 2.01 through 2.05 at the level appropriate to their role and responsibilities (SEC 2.00. Security plan. Competency Guidelines for Public Health Laboratory Professionals. (2015) CDC Morbidity and Mortality Weekly Report. Supplement/Vol. 64/No. 1).

Evaluator and Support Considerations

The following items will be used by evaluators to facilitate, as close as possible, a realistic, safe scenario. Adherence to the intent of the outline is of primary concern, not the item-by-item requirements.

Support Areas	Considerations
Parties Involved in Exercise	Authorized laboratory staff, regulatory inspector imposter
Observers of Scenario	Biosafety officer, biothreat program coordinator, facility operations, security officer and laboratory director
Exercise Area	Secure laboratory area
Materials	No equipment needed
Key References	Biosecurity Plan and possibly other laboratory-specific plans
Tips for Controllers	• Terminate exercise if the safety of personnel, equipment or material is jeopardized in any way • Ensure that the exercise does not extend beyond the scope listed in this document and that the commands of responders are complied with
Safety	Safety of personnel should always be prioritized over security of assets Termination Code: "OAKLEY"

Exercise/Training, Evaluation Results

Check "Yes" or "No" to indicate whether the condition was met for each task. Other important information should be documented under the comments section, as required by the exercise controllers. The overall proficiency rating for this function is based on the performance of each task, primary training and evaluation standards, and the evaluator's knowledge of procedures and functional judgment to determine if the mission would have been successful in a real situation.

Note: This section will vary based on your facility and entity policies.

#	Task	Condition	Yes	No
1	**Visitor needs to enter facility**	Must complete credential check and sign-in		X
2	**Visitor needs to enter secure lab**	Must complete visitor training and follow escort commands		X
3	**Lab staff grow suspicious of possible outsider threat**	Delay/deter entry, communicate threat to others and notify authorities	X	
4	**Visitor needs to enter lab space**	Must don PPE and follow escort commands		X
5	**Visitor displays firearm and makes threats; demands access to biological inventory.**	Delay/deter access as long as possible while prioritizing safety of self and others	X	
6	**Documentation is completed**	Statements, incident report, logs completed to reflect the incident	X	

Exercise Outcomes and Comments

Area	Comments
Overall Proficiency Rating	Performed with some challenges.
Exercise Results	• Entrance into the building and secure areas was defeated by a suspect with fake credentials and an unauthorized, undetected weapon. • The security forces failed to identify suspicious nature of the adversary during entry or while waiting for doors to open. • The physical barriers protecting secure spaces did not prevent the player from gaining access by forced entry, but did cause others in the area to notice there was an issue and call 911. • **Final Assessment:** The assets were not in any immediate threat nor were they accessed due to the other staff contacting the appropriate authorities.
Major Deficiencies Findings / Recommendations	**ID Screening Procedures** • **Finding:** The screening of photo identifications failed to request ID and/or failed to identify forged credentials • **Recommendation:** All employees should be provided refresher training on the procedures for screening access credentials **Security and Emergency Response Procedures** • **Finding:** Personnel working inside security areas were not attentive to access screening, identifying suspicious activity, and emergency notification procedures. • **Recommendation:** Provide refresher training on security and emergency response procedures. Consider posting procedures near areas where they would most likely be seen prior to performance of critical tasks.
Other Significant Information	This exercise was based upon the use of an insider with inside support to attack know vulnerabilities. The likelihood of an outside actor repeating this event is improbable and should not be a factor during operational planning.

Controller Information

Controllers plan and oversee exercise play, handling the setup and operation of the exercise site. Additionally, they assume roles representing organizations or individual not actively participating in the exercise.

Name	Drew Perry
Position	Assistant Laboratory Director
Signature	*Drew Perry*
Date	July 1, 2026

Appendix: Exercise Examples

Laboratory Security Exercises

The laboratory security exercise examples below are high-level overviews of various biosecurity scenarios. These examples are designed to be adaptable to your specific laboratory, allowing you to tailor the exercises to your specific site. Each scenario is accompanied by proposed biosecurity concepts to ensure comprehensive practice of biosecurity concepts.

Scenario	Suggested Exercise Type (Discussion-based / Operational)	Primary Objectives / Concepts Exercised
1. Biological Assets Stolen by an Insider Using Stolen Credentials	Discussion-based or Functional	Adherence to biosecurity policies; management of credentials; insider threat awareness; utilization of security video review; effectiveness of physical security systems; cooperation with law enforcement; biosecurity reporting requirements
2. After-hours Response to a Security Alarm	Discussion-based	Adherence to biosecurity policies; collaboration with law enforcement; biosecurity reporting; addressing alarm fatigue; remediation of security system malfunctions
3. Forced Entry into a Secure Laboratory by an Outsider Who Has Taken a Laboratory Staff Member Hostage	Functional or Full-scale	Outsider threat awareness; recognizing unusual behavior; adherence to visitor entry protocols; law enforcement coordination; emergency communication; biosecurity reporting requirements
4. Maintaining Biosecurity During an Emergency Medical Event in the Laboratory	Discussion-based or Tabletop	Access of unauthorized responders; maintaining inventory security; adherence to biosecurity policies; mitigating outsider threats; reporting requirements
5. Unauthorized Political Demonstrators Enter the Facility After-hours	Discussion-based or Tabletop	Outsider threat mitigation; physical security effectiveness; coordination with law enforcement; adherence to procedures; reporting requirements
6. Reporting Requirements for Unattended Drones Flying Within Secured Grounds	Discussion-based	Adherence to reporting protocols; cooperation with law enforcement; security awareness; utilization of video review systems; reporting suspicious activities
7. Attempted Facility Entrance by Unauthorized Law Enforcement Personnel	Functional or Tabletop	Access control and verification; security of assets and personnel; outsider awareness and conflict resolution; emergency responder access; security response; chain of custody protocols
8. Entry Into Facility by Unauthorized Individuals Attempting to Access Results/ Drop Off Samples	Tabletop or Functional	Adherence to access control policies; security of assets and data; secure access and 24/7 protocols; system utilization; physical security evaluation; chain of custody

Scenario	Suggested Exercise Type (Discussion-based / Operational)	Primary Objectives / Concepts Exercised
9. Patient Breaks into Laboratory and Threatens Employee	Functional or Full-scale	Access of unauthorized persons; threat recognition and mitigation; adherence to policies; asset protection; staff safety; reporting requirements
10. Maintenance Accesses Laboratory Without Authority	Discussion-based	Insider threat awareness; security system utilization; physical access control effectiveness; biosecurity reporting requirements
11. Employee with Laboratory Access Damages Vaccines	Discussion-based or Tabletop	Adherence to policies; insider threat awareness; credential management; asset protection; video system utilization; law enforcement cooperation; reporting requirements
12. Active Shooter Inside the Laboratory	Functional or Tabletop	Validate the laboratory's ability to rapidly respond to an internal armed threat through lockdown, staff protective actions, emergency communications, coordination with law enforcement, and protection of sensitive biological materials.
13. Active Shooter Outside the Laboratory Facility	Tabletop or Discussion	Assess decision-making and coordination during an external armed threat, including perimeter lockdown, communication with staff inside and outside the facility, safe movement decisions, and maintenance of access control.
14. Active Shooter in a Common Area	Functional or Tabletop	Test the organization's response to a high-casualty incident in a shared space while balancing life safety, emergency communications, access control, and continuity of critical laboratory operations.

1. Biological Assets Stolen by an Insider Using Stolen Credentials

Scenario: BSL3 staff member forgets their security card at their desk late on a Friday evening. The staff member decides they will wait until Monday to ask somebody to help them get their card since nobody is around and they don't want to be an inconvenience to their co-workers. They fail to report the forgotten card to the biosecurity officer. Monday morning, staff discover that somebody has stolen biological assets from working inventory. The electronic security logs indicate the forgotten security card was used to enter the lab over the weekend. Video review reveals an IT staff member with access to employee PIN numbers used the forgotten security card to enter the lab and steal the assets. The IT staff member is motivated by increased workload due to staffing decreases, along with fear for their own job.

Biosecurity Concepts Exercised:

- Adherence to biosecurity policies and procedures by laboratory staff
- Management of security credentials
- Insider threat awareness and mitigation
- Utilization of security video review system
- Effectiveness of physical security systems to prevent unauthorized access
- Cooperation with a law enforcement investigation
- Biosecurity reporting requirements

2. After-hours Response to a Security Alarm

Scenario: A laboratory door latch hardware issue has recently caused a string of false intrusion detection alarms. The issue should be addressed by the facility management department in the coming days/weeks. On a Sunday morning at 0500 the laboratory on-call/duty officer receives a phone call from local law enforcement informing them of an intrusion detection alarm in the secure area at the laboratory. Officers are at the laboratory, and everything looks alright. The biosecurity officer is away at a conference and the duty officer is a laboratory professional who works in the area where the alarms have been occurring for the past couple weeks. They inform law enforcement of the issue and asks them to stand down.

Biosecurity Concepts Exercised:

- Adherence to biosecurity policies and procedures by laboratory staff
- Collaboration and partnership with local law enforcement agencies to uphold biosecurity practices
- Biosecurity reporting requirements
- Security alarm fatigue and importance of timely remediation of security system malfunctions

3. Forced Entry into a Secure Laboratory by an Outsider Who Has Taken a Laboratory Staff Member Hostage

Scenario: Laboratory staff are expecting a visit by a regulatory inspection agency. One day earlier than expected, the program's senior manager arrives at the laboratory with the inspector claiming they simply arrived a day early. Laboratory staff sense something may be wrong, as the senior manager is acting nervous and uncomfortable. Two laboratory staff follow the manager and visitor into the laboratory. The manager is noticeably skipping important steps in the laboratory's visitor entry protocols, like administering visitor training prior to entry into the laboratory. Once inside the secure laboratory the visitor demands to see the biological inventory. They reveal a firearm and demand the staff give them a freezer box of biological assets. Through nearby windows, other staff notice unusual commotion and the hostage situation in progress. They immediately call 911.

Biosecurity Concepts Exercised:

- Outsider threat awareness and mitigation
- Recognizing unusual behavior by a colleague
- Adherence to biosecurity policies and procedures by laboratory staff
- Collaboration and partnership with local law enforcement agencies
- Biosecurity reporting requirements

4. Maintaining Biosecurity During an Emergency Medical Event in the Laboratory

Scenario: Biosafety Level 3 (BSL3) staff member experiences emergency medical event while working in the biosafety cabinet in a select agent-registered BSL3 lab. While working alone, they lose consciousness and fall to the floor, causing a spill of biohazardous waste materials. During emergency response, biosecurity policies and precautions must be upheld.

Biosecurity Concepts Exercised:

- Access of unauthorized emergency response personnel to the victim
- Outsider threat awareness and mitigation
- Security of biological inventory and assets
- Adherence to biosecurity policies and procedures by laboratory staff
- Biosecurity reporting requirements

5. Unauthorized Political Demonstrators Enter the Facility After-hours

Scenario: A political demonstration/march is passing by the laboratory facility after normal business hours. Despite the march's peaceful intentions and no expressed threat to the laboratory, a small group of demonstrators are discovered to have entered the secure building. The COVID-19 pandemic response has drawn attention to the work of the laboratory and these individuals believe the work being performed at the laboratory is further propagating the sociopolitical policies in place throughout their local and state communities.

Biosecurity Concepts Exercised:

- Outsider threat awareness and mitigation
- Effectiveness of physical security systems to prevent unauthorized access
- Collaboration and partnership with local law enforcement agencies
- Adherence to biosecurity policies and procedures by laboratory staff
- Biosecurity reporting requirements

6. Reporting Requirements for Unattended Drones Flying Within Secured Grounds

Scenario: Laboratory staff member witnesses a drone flying outside their laboratory window which is inside a fenced in complex. They watch the drone fly close to the building and hold in position at various spots for several seconds as if it is taking pictures of the building. All suspicious activities must be reported immediately to the responsible official.

Biosecurity Concepts Exercised:

- Adherence to biosecurity policies and procedures by laboratory staff
- Biosecurity reporting requirements
- Training on how to report suspicious activities
- Cooperation with local, state and federal law enforcement
- Utilization of security video review system

7. Attempted Facility Entrance by Unauthorized Law Enforcement Personnel

Scenario: Staff performing duties as normal are made aware of an individual attempting entry into facility. Staff become aware that individual attempting unauthorized entry is a member of local law enforcement (police officer). Unbeknownst to staff, officer is on site to retrieve equipment relating to the function of one of the labs housed in the same building. Officer is insisting that staff let them into facility and refuses to leave or give explanation of their presence since they believe staff are already aware of circumstances since he routinely enters the grounds to drop off equipment/samples from the local jails. Communication between officer and staff quickly breaks down. Officer is threatening staff with criminal charges.

Biosecurity Concepts Exercised:

- Access of unauthorized personnel claiming authorization
- Security of assets
- Security of personnel
- Outsider awareness and conflict resolution
- Emergency responder access
- Security response protocols
- Security system utilization
- Inventory receipt protocol
- Law enforcement involvement in security protocols

8. Entry Into Facility by Unauthorized Individuals Attempting to Access Results/Drop Off Samples

Scenario: Staff are working extended hours due to time constraints and testing requirements. During testing, staff become aware of individuals in a low security area of the facility. Unauthorized individuals are unsuccessfully attempting to access more secure parts of facility to find staff on duty. When confronted, unauthorized individuals identify themselves as officers of the law and inform staff they are present to drop off samples and collect results. Officers are attempting to perform their job duties as they have been described to them.

Biosecurity Concepts Exercised:

- Adherence to biosecurity policies and procedures by laboratory staff
- Secure access protocols
- Security of assets, individuals, private information, etc.
- Security system utilization
- 24/7 access protocols
- 24/7 security response protocols
- Physical security system design / failure points
- Chain of Custody protocols

9. Patient Breaks into Laboratory and Threatens Employee

Scenario: Patient has blood drawn at an in-laboratory phlebotomy station. Patient asks about obtaining results and phlebotomist tells patient to call his physician in the next two days. After not hearing back, the patient comes to the lab two days later and grabs a phlebotomist and threatens to infect phlebotomist with nearby specimens if he cannot get his results now.

Biosecurity Concepts Exercised:

- Access of unauthorized persons in lab
- Outsider threat awareness and mitigation
- Security of biological inventory and assets
- Adherence to biosecurity policies and procedures by laboratory staff
- Biosecurity reporting requirements

10. Maintenance Accesses Laboratory Without Authority

Scenario: Maintenance notices water dripping from the ceiling in the cafeteria of the hospital at 2:00 am. The lab is directly upstairs but is closed for the night. The protocol is for maintenance to contact the on-call lab scientist to come in to provide escort, but she does not want to bother the scientist because she knows that the laboratory door will open if she hits it in the right spot. She proceeds to fix the water leak and is happy she did so without waking anyone. In the morning the manager asks the on-call lab scientist how long he had to stay when he came in for the water leak, the scientist says, “I didn’t get a call to come in, what are you talking about?”

Biosecurity Concepts Exercised:

- Insider threat awareness and mitigation
- Utilization of security video review system
- Effectiveness of physical security systems to prevent unauthorized access
- Biosecurity reporting requirements

11. Employee with Laboratory Access Damages Vaccines

Scenario: A new, controversial vaccine is being stored in the hospital laboratory because it has excess storage available. A nurse, who has access to the laboratory to drop off samples, is against this vaccine. The nurse goes into the laboratory on their break time and unplugs the freezer. It is not discovered until the next morning and all of the vaccines are ruined.

Biosecurity Concepts Exercised:

- Adherence to biosecurity policies and procedures by laboratory and other hospital staff
- Management of security credentials
- Security of biological inventory and assets
- Insider threat awareness and mitigation
- Utilization of security video review system
- Effectiveness of physical security systems to prevent unauthorized access
- Cooperation with a law enforcement investigation
- Biosecurity reporting requirements

12. Active Shooter Inside the Laboratory

Scenario: It is mid-morning on a normal weekday. Staff are working in their offices, laboratories, and support areas when an armed individual gains unauthorized access to the facility by following an employee through a secure door (tailgating). Once inside, the intruder moves into a main corridor and begins firing indiscriminately.

Staff near the shooter scatter, some run toward emergency exits while others retreat into offices, laboratory spaces and conference rooms.

In the confusion, some employees are unsure whether to evacuate or remain in place, and others attempt to warn colleagues in adjacent areas. As law enforcement responds, coordination is complicated by multiple reports of the shooter's movements inside the building.

Biosecurity Concepts Exercised:

- Active shooter response inside controlled laboratory environments
- Tailgating and unauthorized access prevention
- Lockdown procedures for laboratories with biological materials
- Shelter-in-place vs. evacuation protocols under imminent threat
- Coordination with law enforcement and first responders
- Rapid communication channels (mass notification systems, overhead announcements, text alerts)
- Ensuring security of sensitive materials and select agents during crises
- Training staff on securing laboratory doors, freezers, and safes during emergencies

13. Active Shooter Outside the Laboratory Facility

Scenario: It is the end of the day (or during the afternoon shift change, if laboratory operates with shifts), and staff are gathered outside in parking areas, waiting for transportation or walking to vehicles. An individual in a vehicle stops near the main entrance, exits with a firearm and begins firing at people in the lot. Employees in the open scramble for cover behind vehicles, dumpsters, landscape or other barriers. Those close to the building attempt to re-enter, causing congestion at access-controlled doors. Employees still outside must make rapid decisions: run, hide, fight or attempt re-entry. Inside, staff begin to hear about the events unfolding outside and are told to stay inside and shelter in place. Law enforcement establishes a perimeter around the facility, instructing staff to stay clear of windows and glass doors. After several minutes, confusion grows, staff inside question if they should prepare for evacuation, while staff outside debate whether it's safer to stay hidden or approach law enforcement. The external threat continues until responders neutralize the shooter.

Biosecurity Concepts Exercised:

- Situational awareness of external threats before entering/exiting laboratory facilities
- Activation of perimeter security protocols (parking lots, access roads, gates)
- Lockdown procedures triggered by external threats
- Staff training on shelter-in-place when outside vs. safe routes to re-enter secure buildings
- Coordination with law enforcement and on-site security for perimeter control
- Communication systems for staff inside and outside the facility
- Maintaining physical access control during external crises (preventing panic-driven breaches)
- Assessment of vulnerabilities in outdoor gathering points (parking lots, smoking areas, shuttle stops)

14. Active Shooter in a Common Area

Scenario: Around noon, the break areas are busy with staff on lunch breaks. An armed individual, with no authorized access, forces entry through a side service door and begins firing into the crowd. Panic erupts, employees rush toward multiple exits, while others attempt to barricade themselves inside nearby rooms, offices, and conference rooms. The shooter roams between open areas and the lobby, testing the effectiveness of access control system points. Law enforcement arrives quickly, but coordination is complicated by conflicting reports from panicked staff about the shooter's location. Meanwhile, an unrelated alarm sounds from critical equipment in a restricted area due to a temporary power interruption caused by the building lockdown system. This creates additional stress as staff debate whether to address the equipment issue or continue sheltering in place.

Biosecurity Concepts Exercised:

- Active shooter response in high-occupancy, non-lab common areas of a laboratory facility
- Rapid decision-making for staff with dual responsibilities (self-preservation vs. biosecurity)
- Testing visitor and contractor access policies
- Securing sensitive areas and biological materials under duress
- Testing effectiveness of access control systems in high-traffic zones (cafeteria, break rooms)
- Coordination of on-site security staff with external law enforcement for rapid response
- Emergency communication effectiveness across different spaces (laboratories, offices, cafeteria)
- Reinforcing policies on visitor management and access screening

Laboratory Preparedness Exercises

The exercise examples below serve as high-level overviews of potential threat and emergency scenarios relevant to public health laboratories. Each example is designed to be adaptable to your facility's and/or laboratory's specific operations, resources, and regulatory requirements. Each scenario is accompanied by proposed exercise concepts to assist with planning of the exercise. Scenarios can be implemented as discussion-based or operations-based exercises depending on objectives, available time and training goals.

Scenario	Suggested Exercise Type (Discussion-based / Operational)	Primary Objectives / Concepts Exercised
1. Receipt of a White Powder Letter by LRN-B Laboratory	Discussion or Functional	Practice sample receipt, chain-of-custody, LRN-B/LRN-C communication, risk assessment, safety review
2. *Brucella* Exposure in General Microbiology Area	Discussion or Tabletop	Conduct exposure risk assessment, staff notification, occupational health coordination
3. Emergency Evacuation While Working in Select Agent Space	Functional or Drill	Test fire alarm response, containment safety, coordination with first responders, internal emergency activation
4. Sample Transport and Testing During Severe Weather	Tabletop	Evaluate communication, COOP activation, staffing, testing prioritization, safety and reporting procedures
5. Evaluating Biosafety During Mock Ebola Testing	Operational / Hands-on	Assess Ebola testing workflow, PPE performance, contamination control, decontamination procedures
6. Person Down in BSL-3 Select Agent Registered Space	Functional Drill	Test two-person rule, emergency notification, first aid/AED/CPR, select-agent compliance during rescue
7. Maintaining Operations During Extended IT Downtime	Tabletop	Validate manual result reporting, data continuity, coordination with IT, COOP activation
8. Active Shooter Incident in a Laboratory Facility	Discussion or Functional	Practice "Run-Hide-Fight," staff communication, coordination with law enforcement, triage and first aid

1. Receipt of a White Powder Letter by LRN-B Laboratory

Scenario: The local hazmat team delivers a white powder to the LRN-B laboratory for multi-agent screening testing. Field screening indicated a negative result; however, preliminary testing suggested a possible detection of fentanyl.

Preparedness Concepts Exercised:

- Effectiveness of first responder sample collection and field screening
- Environmental sample submission protocols and acceptance protocols
- Communications between LRN-B, LRN-C and first responders
- Coordinated risk assessment by LRN-B and LRN-C to determine testing order
- Laboratory safety practices and PPE use
- Chain-of-custody procedures and documentation
- Reporting results and conducting an after-action review

2. *Brucella* Exposure in General Microbiology Area

Scenario: The laboratory receives blood culture isolates from a Sentinel Laboratory labelled as gram-positive cocci. Microbiology staff process the isolates the same day, resub them to new plates the next day, and simultaneously sent for automatic identification using a Matrix-assisted laser desorption ionization-time of flight mass spectrometer (MALDI-TOF MS). While the targets are being analyzed on the MALDI-TOF MS, plate growth and colony morphology were being assessed. The MALDI-TOF MS identified the isolates as *Brucella* species.

Note: The following activities were performed on the bench: plate streaking and reading, MALDI-TOF MS target spotting, and Gram staining.

Preparedness Concepts Exercised:

- Risk assessment and exposure determination
- Communication with Occupational Health, biosafety officers, providers and submitting laboratory
- Post exposure monitoring and serologic testing of affected staff
- Compliance with incident reporting

3. Emergency Evacuation While Working in Select Agent Space

Scenario: While staff are processing an unknown powder in a BSL-3 select agent registered space, smoke is observed near a generator room and the fire alarm sounds. Personnel working in the registered space are undecided whether the alarm is real or "just" a drill.

Preparedness Concepts Exercised:

- Fire evacuation and alarm response protocols
- BSL-3 safety practices during emergency situation
- Compliance with select agent regulations
- Communication with first responders and coordination of the fire department response
- Activation of the Internal emergency response team

4. Sample Transport and Testing During Severe Weather

Scenario: It is 3:30 in the afternoon on a Friday before a long weekend. The laboratory is notified of a high-priority specimen of significant public health importance. A courier is scheduled for pickup from a county three hours away, but ice and deteriorating weather conditions threaten timely transport. With minimal staff on-site after a long day, the laboratory must assess testing priorities, staffing needs, and continuity of operations plan.

Preparedness Concepts Exercised:

- Communications with epidemiology, leadership and first responders
- Staffing decisions and surge capacity planning
- Safe handling and receipt of specimens under adverse conditions
- Reporting of results protocol including data entry and supervisor review
- Implementation of Continuity of Operations Plan (COOP) – e.g. generator and facility power contingency

5. Evaluating Biosafety During Mock Ebola Testing

Scenario: A mock Ebola specimen (EDTA tube) is contaminated with Glo Germ both internally and externally to simulate contamination risk. Laboratory staff test the mock specimen in the BSL-3 select agent registered laboratory using the BioFire instrument under standard Ebola testing protocols. Periodic use of UV light detects contamination spread, highlighting biosafety compliance and potential weaknesses.

Preparedness Concepts Exercised:

- Ebola virus testing protocols and workflow management
- Donning and doffing of PPE and adherence to biosafety standards
- Compliance with select agent regulations
- Decontamination and waste management protocols
- Evaluation of laboratory technique and contamination control

6. Person Down in BSL-3 Select Agent Registered Space

Scenario: Two staff are processing a specimen for Bacillus anthracis in a BSL-3 select agent registered laboratory when one laboratorian collapses from a medical emergency (heart attack), striking their head and bleeding heavily. This is an extreme medical emergency and must be dealt with immediately while considering personal safety, maintaining containment, and initiating emergency notification and response procedures.

Preparedness Concepts Exercised:

- Enforcement of the two-person rule
- Communication and coordination with first responders and staff
- Internal notification procedures and emergency chain of command
- PPE requirements and safety priorities during medical emergencies
- First aid response (including AED and CPR)
- Compliance with select agent regulations during emergencies
- Pre-incident training and safety requirements
- First responder training
- Safe transport of injured individual
- Decontamination procedures

7. Maintaining Operations During Extended IT Downtime

Scenario: A burst water pipe damages a network switch, leaving the laboratory without internet connectivity for three days. Limited hotspots are unreliable and not secure. Outside IT contractors unfamiliar with the laboratory infrastructure and workflows are assigned to restore service. They must procure and install a new switch while staff determine how to continue essential functions and reporting during this outage.

Preparedness Concepts Exercised:

- Continuity of electronic test ordering and results reporting
- Management of instrument interface to LIMS and data capture during downtime
- External communications with submitters and partners
- Customer service with specimen submitters
- Coordination with agency IT and technical support
- Continuity of Operations Plan

8. Active Shooter Incident in a Laboratory Facility

Scenario: Laboratory staff are performing duties as normal midmorning when suddenly several rapid-fire shots ring out. Several staff freeze, some scatter, others try to find a hiding place and still others stand around asking each other what they heard. Unbeknownst to staff, a disgruntled former employee entered the laboratory lobby, barged past security while shooting and headed to the laboratory areas through unsecured access points. An uninjured and unarmed security guard immediately calls 911.

Preparedness Concepts Exercised:

- Evaluation of first responder response times
- Communications with staff, law enforcement, leadership
- Maintaining silence and situational awareness during a crisis
- Following the active shooter protocol
- Buddy system and staff accountability
- Triage, first aid and emergency response protocols
- Operation of the intercom system or alert notifications systems, if available
- Coordination with responding law enforcement and emergency services

Association of Public Health Laboratories

The Association of Public Health Laboratories (APHL) works to strengthen laboratory systems serving the public's health in the US and globally. APHL's member laboratories protect the public's health by monitoring and detecting infectious and foodborne diseases, environmental contaminants, biological and chemical agents, genetic disorders in newborns and other health threats.

7700 Wisconsin Avenue, Suite 1000 Bethesda, MD 20814 | 240.485.2745 | aphl.org

This project was 100% funded with federal funds from the US Centers for Disease Control and Prevention (CDC) through two Cooperative Agreements: #U60OE000104 (program total $790,552) and #NU47CD000001 (program total $145,500). Its contents are solely the responsibility of the authors and do not necessarily represent the official views of CDC.