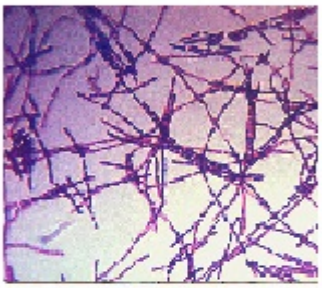
Form Approved
OMB Control No. 0920-0576
Exp. Date xx/xx/2020



Incident Response Plan Guidance

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

(May 2017)

Centers for Disease Control and Prevention (CDC)
Division of Select Agents and Toxins (DSAT)
Animal and Plant Health Inspection Service (APHIS)
Agriculture Select Agent Services (AgSAS)

Changes/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 at:

CDC: LRSAT@cdc.gov
APHIS: AgSAS@aphis.usda.gov

Revision History:
October 12, 2012: Initial posting
June 19, 2013 (Revision 1): The revisions are primarily changes to correct editorial errors from previous version.
February 10, 2014: Added "Low probability/High consequence Events" to Appendix IV.
September 4, 2014: Added information about continuing laboratory operations after incident.
May 2017: The revisions are primarily changes to the organization to improve usability from previous version.

Introduction

Under the provisions of select agent regulations (7 CFR §331.14, 9 CFR §121.14, and 42 CFR §73.14), an entity registered with the Federal Select Agent Program is required to have plans in place in the event of a natural and/or man-made disaster. This guide is to assist the regulated community in developing a site-specific incident response plan to ensure the security and safeguarding of select agents and toxins from natural and man-made disasters.

Please feel free to use the new editable Incident Response Plan Template (link to template) as the foundation for your entity's incident response plan.

Incident Response Plan Requirements

Section 14 of the select agent regulations states that every registered entity must develop, implement, and maintain a written incident response plan.

The incident response plan must fully describe the entity's response to the following events:

- Loss, theft, or release of select agents and toxins
- Inventory discrepancies
- Security breaches
- Severe weather and natural disasters
- Workplace violence
- Bomb threats and suspicious packages
- Emergencies such as fired, gas leak, explosion, or power outage
- Other natural or man-made events that may threaten the entity

The incident response plan should also account for the hazards associated with the select agents and toxins. The plan should outline containment procedures for all select agents and toxins including infected animals and plants.

Incident Response Plan Information

According to section 14(d), the incident response plan should contain the following information as applicable for the entity's organization:

- Contact information for the Responsible Official and alternate Responsible Official (RO and ARO)
- Contact information for building owner/manager
- Tenant office contact information
- Contact information for entity's physical security official
- Personnel roles and lines of authority/communication
- Planning and coordination with local emergency responders
- Procedures to be followed by employees performing rescue or medical duties
- Emergency medical treatment and first aid
- Inventory of personal protective and emergency equipment and their locations
- Site security and control
- Procedures for emergency evacuation
    - Evacuation type
    - Exit route assignments
    - Safe distances
    - Places of refuge
- Decontamination procedures

Tier 1 Incident Response Plan Requirements

Entities that possess or use Tier 1 select agents and toxins must comply with additional incident response

planning requirements:

- Fully describe the response procedures for failure of intrusion detection or alarm system
- Describe notification procedures for the appropriate Federal, State, or local law enforcement agencies for suspected criminal activity related to the entity, its personnel, or its select agents and toxins

Effective Incident Response Planning

An incident response plan is a set of standard operating procedures that prevents the theft, loss, or release of select agents and toxins and/or protects human life and animal and plant health. An effective incident response plan prioritizes:

1. Protecting of human life before property.
2. Considering the impact to the laboratory instead of just the facility.
3. Collaborating between entity leadership and responders.
4. Entity training with responder participation.
5. Addressing the primary effect of the hazard, the secondary effects, and the impact the hazard has on the facility workers.
6. Focusing on areas inside the laboratory or registered space.

There are other statutes (federal, state and local government) that address emergency and incident response. The select agent incident response plan is not intended to preempt or supersede other response agreements or written plans provided that other plans and agreements address the requirements of section 14 of the select agent regulations. If an entity chooses to use other plans as a means of meeting these requirements, section 18 of the select agent regulations requires that this information be made available to Federal Select Agent Program inspectors when on-site inspections are conducted.

Creating a Successful Incident Response Plan

FSAP has developed a six-step cycle for creating a successful incident response plan. These steps are general guidelines for creating the series of standard operating procedures (SOPs) to be in compliance with section 14 of the select agents regulations and provide a safe environment for the entity's employees and community.

Step 1: Form a Team.

The incident response planning team should include the following as applicable to the entity's organization and biosafety level (BSL):

- Entity Subject Matter Experts (SMEs) – Responsible Official, Principle Investigator, Biosafety Officer
- First Responders – Fire Department, Police, Emergency Medical
- Governmental – State, Federal, Local
- Organization – Facility Manager, Security, Leadership

Once the team is formed, it should remain engaged throughout the process. Each team member brings both skills and a unique perspective to the situation. At each step, the entity is strongly encouraged to consult team members.

Step 2: Perform a Risk Assessment.

Begin the discussion by describing the entity to the responders, with particular attention to the layout of registered spaces. Each group of SMEs in the incident response planning team provides a different perspective and key pieces of information for identifying risks and mitigation methods.

The Entity

1. Identify risks (probable hazards, high consequence events) that cannot be mitigated before a response is required. This should include those required by regulation, regional natural disasters, and other site-specific hazards.
2. Identify what protective measures/equipment is in place and where it is located.
3. Discuss SOPs which may take place during incidents, including man-down drills, evacuation procedures, and others.

First Responders

1. Identify what capabilities can be managed by first responders (HAZMAT, police).
2. Calculate response times to the entity by hazard type for multiple situations.
3. Discuss contact and communication procedures beyond calling 911.

Facility Management and Safety/Security Personnel

1. Be familiar with the physical capabilities of the building and available emergency equipment.
2. Understand the existing organizational policies and procedures for managing incidents.
3. Take responsibility for escorting or granting access to first responders.

Step 3: Analyze Facility Capabilities against Hazards

Conduct an analysis of various hazards that may result in the theft, loss, or release of a select agent or toxin. FSAP requires that the entity addresses certain specific hazards, which form the core of the incident response plan. The

entity should also analyze their capabilities against any additional hazards identified during the risk analysis.

To conduct a facility analysis, create scenarios that demonstrate a series of incident driven actions and events and provide a factual and logical framework for developing an SOP. The scenarios can assist in guiding discussion and help create an appropriate sequence response actions. Some different methods of working through incident response scenarios include:

- **Action/Response** – Each action leads to a reaction and so on until the tasks are complete.
- Functional – Each organization talks through its internal SOPs and determines where they should overlap.
- **Walk-Through** – The team physically determines what resources are available, where equipment sits, and where the clean/dirty areas are. Focus on the inside of the laboratory. Building codes will generally ensure the facility can survive likely disasters but may not address loss of primary and secondary containment, animal husbandry issues, spilled, loss of power to a freezer, etc.
- **Second Order Effects** – The team discusses and determines incidents that may lead to other incidents. For example:
    - Earthquake may cause power outage or fire.
    - Hurricane may prevent facility access.
    - Fire suppression system may flood a containment system

As the team conducts the facility analysis, consider the following questions:

- Who must do what, when, and where?
- What must team members know for each incident type?
- Who conveys incident response information to team members?
- What crucial information must be conveyed about the lab and facility?
- What equipment is needed during a given incident/incident response?
- Who is in charge at each step of the incident response? What decisions must be made?

The answers to these questions will allow the Incident Response planning team to identify the key information that forms the basis of the incident response plan:

- Condition Expectations and Assumptions – Assumptions that must be made as a part of incident response planning but may disrupt the plan if they are not met (i.e. clear roads, first responder presence).
- Logistical Constraints – Limitations of response team members (i.e. equipment access, mobility limitations).
- Capability Gaps – Required capabilities that team members do not have (i.e. missing Personal Protective Equipment, training, etc.).

Step 4: Develop Plans by Incident Type

Create a series of standard operating procedures (SOPs) based on each scenario. An SOP should be a list of simple instructions that anyone can quickly read and follow. Focus on creating plans with common steps that can be applied to various incidents to improve comprehension and reduce training.

Entities are encouraged to develop playbooks. A playbook is a series of simple plans / SOPs that cover the multiple incidents identified in the analysis stage. Instead of focusing on nuances of each event, focus on common steps

and then apply them to various incidents. This not only makes incident response easier for individuals to understand it also makes it much easier to train.

Notice Based

- No Notice
- Minimal Notice
- With Notice
- After the Fact

Risk Based

- High (Potential for serious threat/damage)
- Medium
- Low

Incident Based

- Case-by-case
- Natural Disasters
- Facility Emergencies
- Severe Weather

Each SOP should include the following crucial information:

1. What incidents the plan covers?
2. Concept (What are you trying to do? When are you done?)
3. Entity and organizational responsibilities/tasks (What will the entity do? Who does it/when? What is the entity responsible for?)
4. First responder actions/tasks (What will they/won't they do?)
5. Entity lines of authority (Who has the authority to call this kind of response? Who's next in charge?)
6. Decontamination procedures (Do you doff? If not, how do you separate contaminated personnel?)
7. Emergency equipment (Where is it? How does it apply? Who uses it?)
8. Procedures for emergency evacuation, including type of evacuation, exit route assignments, safe distances, and places of refuge (How do you get out? Where do you go once you leave the lab?)
9. Personnel accountability (Who accounts for personnel and who is notified once personnel are accounted for?)
10. Procedures to be followed by employees performing rescue or medical duties and the location (Where do you conduct immediate care? Where do you conduct follow up?)
11. Location where the first responders will pick up a patient and what amount of decontamination must be done (Doffing, showering out—consult the first responders on their requirements for transport)
12. Contacts and communication plan (Who calls 911? Who notifies the RO or management? Is anyone else notified?)
13. Site security and control (How do you manage access to the facility during and after the incident, where's the perimeter, etc.?)
14. Return procedures (Under what conditions and how do you return to the lab, check containment, etc.)

15. Select agent and toxin (and other high value items) accountability
16. Medical Surveillance (if required)

Create a Recovery Plan

Create a recovery phase for incidents that may cause damage to a laboratory. The recovery plan should include procedures for emergencies that would prevent entities from returning to normal operating conditions (i.e. laboratory is damaged and nonoperational). This section of the plan should answer the following questions:

- What happens when the laboratory cannot return to normal operations after an incident?
- When will the laboratory be able to return to normal operations?
- Will work with select agents and toxins continue in another registered space?
- Will select agents and toxins be stored in another registered space until the damaged area is operational?
- Will select agents be transferred to another registered entity until the damaged laboratory is operational?

Step 5: Review and Test the Incident Response Plan

To stay in compliance with Section 14 of the select agent regulations, review and exercise the incident response plan at least once annually. See the Drills and Exercise guidance document for FSAP recommendations for successful drills and exercises.

Step 6: Refine and Update Plans

Refine and update their plan(s) at least annually, after each exercise or after a plan is executed. Work with the incident response planning team to review the document and make any necessary changes to address the following:

- Results of training (what went well, what can be improved, changes made)
- Any changes to threats or hazards
- Any changes to expectations or assumptions from the original plan
- Any new equipment, its capabilities and locations including first responders (new PPE, new HAZMAT vehicle)
- Any changes to the entity (additional registered space)
- Any changes in key personnel or organizations, including first responders
- Changes to the agents which affect response (adding a Tier 1 agent)
- Specific threats against the entity or its personnel
- Any changes in communications
- Critical changes to regulatory requirements, including those which affect first responders

Regional Natural Disasters

Go to each of the following websites to determine if the organization is at reasonable risk for any of these incidents. Ensure that any reasonable risks are accounted for in a SOP in the Incident Response Plan.

- General: U.S. Geological Survey Website
- Flood: U.S. Federal Emergency Management for Floods
- Earthquake: Earthquake Hazard Map

- Hurricane: National Hurricane Center
- Tornado: Tornado Alley Map
- Tsunami: Tsunami Hazard Map
- Volcano: Volcano Hazard Map
- Wildfire: Wildfire Hazard Map

Low Probability/High Consequence Events

Entities are encouraged to plan for "low probability/high consequence" events. A low probability/high consequence event is any event which adversely: 1) affects the safety and security of a registered facility; 2) affects human health and safety; and 3) causes environmental degradation.

Consider not only these types of events but potential secondary incidents that may occur as a result of an incident, such as:

- System Failures
- Radioactive Leaks
- Extreme Flooding
- Power Failures
- Access Loss
- Damaged Equipment

Regulatory Requirements

Section 14 (b) Requirements:

The incident response plan must fully describe the entity's response for the following procedures in the chart below.

Incident	Definition of Incident	Examples	Incident Notice
Theft, loss or release of a select agent or toxin	**Theft:** Unauthorized removal of select agent or toxin. **Loss:** A failure to account for select agent or toxin **Release:** A discharge of a select agent or toxin outside the primary containment barrier due to a failure in the containment system, an accidental spill, occupational exposure, or a theft. Any incident that results in the activation of a post exposure medical surveillance/prophylaxis protocol should be reported as a release.	Vial containing select agent missing or stolen; spills; needle stick;	No Notice
Inventory discrepancies	Inventory discrepancies occur when inventory (e.g., vials, containers) do not match the record data.	Mislabeled vials	No Notice
Security breaches/ Suspicious Activity	A security breach occurs when there is a disruption in the established security network or a failure to follow the entity's written security policies and procedures. Breaches involve all levels of security including physical security (hardened, fixed systems), operational security (personnel reliability) and information systems (electronic and hard copy material).	Computer hacking; unauthorized personnel in laboratory	No Notice
Severe weather and other natural disasters	Severe weather and natural disasters vary from one geographic location to another within the United States. Severe weather situations and natural disasters include tropical storms, hurricanes, tornadoes, windstorms, thunderstorms, lightning, hail, floods, earthquakes, fires and winter storms (not all inclusive). To assist in determining if the entity is in an affected area, refer to Tab IV "Evaluating Natural Hazard."	Tornado Warnings; Flood Warnings	Minimal Notice for tornado, severe weather or storm, hurricane, floods No Notice for earthquakes
Bomb Threats	Bomb threats have become common means to disrupt workplace activity. Most agencies at the academic, state, and federal levels have their own bomb threat policy.	Any object that appears suspicious or looks like it might be explosive.	Minimal Notice
Gas leak	A gas leak is a non-expected release of gas that can create a potentially dangerous situation - either because the released gas is poisonous or because it can ignite and create an explosion.	Smell of gas; sound of air being released from an open gas valve	Minimal Notice
Explosion	Explosion is the sudden loud release of energy and a rapidly expanding volume of gas that occurs when a bomb detonates or gas explodes	Bomb detonates or gas explodes	No Notice

Section 14 (c) Requirements:

Emergency Contact Information – Collect and document site- specific contact information for each person identified as having an incident response role. Focus on support units that are available within the geographic region of the facility, especially if the entity is relying on local support of first responders. Entities associated with larger parent organizations (i.e., colleges, universities, federal or state campuses and research medical institutions) need to incorporate or integrate their site-specific incident response requirements with established entity-wide emergency response programs.

Personnel roles and lines of authority and communication – Assess the roles and responsibilities of each identified person ahead of time. Ensure that all participants understand the lines of authority and how information is communicated both up and down the chain of command.

Planning and coordination with local emergency responders – Meet with local emergency responders to discuss large scale disasters is important. Discuss the roles and responsibilities of each party with first responders in the event of a disaster that affects the select agent laboratory.

Procedures to be followed by employees performing rescue and medical duties – Rescue and medical duties should be limited to only those individuals that are qualified to perform these duties (paramedic, EMT, registered nurse, physician assistant, medical doctor, osteopathic physician). When qualified individuals are not available, 911 should be called. Train staff to perform emergency first aid and CPR if laboratories located in remote areas that may cause delayed ambulance response time.

Emergency medical treatment and first aid – Establish provisions for emergency medical treatment and first aid for employees injured on the job. Since occupational injuries and illnesses are work related, worker's compensation rules may apply. Check with the personnel department (human resources) to determine if employees have to report to a prearranged emergency treatment center or clinic. Inform workers of where to go or be transported for emergency medical treatment or first aid. In laboratories that are regulated by state or federal OSHA (Occupational Safety and Health Administration), an injury log (e.g., OSHA 300) will be required to record all injuries that result in lost time or in medical treatment.

List of personal protective and emergency equipment, and their locations – Identify what personal protective equipment (PPE) and emergency equipment is needed and state where it is located. Include a floor plan showing the PPE and emergency equipment locations in the incident response plan. Examples of PPE include, but are not limited to: gloves, protective eyewear, face shields, respirators, foot protection, gowns, and scrubs. Examples of emergency equipment include, but are not limited to: fire extinguishers, emergency showers, fire blankets, eye wash stations, and portable lighting.

Site security and control – Maintain site security and control to the best of your ability at all times. During incident response planning, inform first responders that access to restricted areas needs to be controlled during and after each incident. Some of the typical methods used to maintain site security control include a posted armed police officer or guard, yellow "caution" tape around the perimeter, "keep out" signs, emergency lighting, etc.

Procedures for emergency evacuation – The incident response plan should define the different types of

evacuations that may be encountered during an emergency. Post floor plans that show the primary and secondary emergency exit routes on each floor. Include these floor plans in the incident response plan. Determine safe distances for evacuation in the event of a worst case scenario. When a warning is received regarding an impending disaster, the incident response plan should designate areas for safe refuge until the warning expires or the threat no longer exists.

Decontamination procedures – Describe decontamination procedures in the incident response plan. Include decontamination procedures for spills, injured select agent workers, emergency responders and laboratory rooms and areas that require mass decontamination.

Annual Training – Provide and document annual incident response training for personnel who have access to select agents or toxins. The documentation of incident response training must include: name of trained personnel, date, name of training, and how it verified that personnel understood training goals and objectives. For entities with Tier 1 agents insider threat awareness training must be conducted annually with all personnel who have access to select agents or toxins.

Tier 1 Requirements – Entities with Tier 1 agents must provide the following additional information in the incident response plan:

- A plan for how the entity will respond to the activation of the alarm system or information on an intruder in the lab.
- Procedure for how the entity will notify the appropriate Federal, State, or local law enforcement agencies of suspicious activity that may be criminal in nature and related to the entity, its personnel, or its select agents or toxins.