(3) Contain provisions for routine cleaning, maintenance, and repairs;

(4) Establish procedures for removing unauthorized or suspicious persons;

(5) Describe procedures for addressing loss or compromise of keys, passwords, combinations, etc. and protocols for changing access numbers or locks following staff changes;

(6) Contain procedures for reporting unauthorized or suspicious persons or activities, loss or theft of select agents or toxins, release of select agents or toxins, or alteration of inventory records; and

(7) Contain provisions for ensuring that all individuals with access approval from the Administrator or the HHS Secretary understand and comply with the security procedures.

(d) An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security:

(1) Allow access only to individuals with access approval from the Administrator or the HHS Secretary;

(2) Allow individuals not approved for access by the Administrator or the HHS Secretary to conduct routine cleaning, maintenance, repairs, and other activities not related to select agents or toxins only when continuously escorted by an approved individual;

(3) 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);

(4) Inspect all suspicious packages before they are brought into or removed from an area where select agents or toxins are used or stored;

(5) Establish a protocol for intra-entity transfers under the supervision of an individual with access approval from the Administrator or the HHS Secretary, including chain-of-custody documents and provisions for safeguarding against theft, loss, or release; and

(6) Require that individuals with access approval from the Administrator or the HHS Secretary refrain from sharing with any other person their unique means of accessing a select agent or toxin (*e.g.*, keycards or passwords);

(7) Require that individuals with access approval from the Administrator or the HHS Secretary immediately report any of the following to the responsible official:

(i) Any loss or compromise of keys, passwords, combinations, etc.;

(ii) Any suspicious persons or activities;

(iii) Any loss or theft of select agents or toxins;

(iv) Any release of a select agent or toxin; and

(v) Any sign that inventory or use records for select agents or toxins have been altered or otherwise compromised; and

(8) Separate areas where select agents and toxins are stored or used from the public areas of the building.

(e) In developing a security plan, an individual or entity should consider the document entitled, ''Laboratory Security and Emergency Response Guidance for Laboratories Working with Select Agents,'' in Morbidity and Mortality Weekly Report (December 6, 2002); 51 (No. RR–19):1–6. This document is available on the Internet at *http://www.cdc.gov/mmwr*.

(f) The plan must be reviewed annually and revised as necessary. Drills or exercises must be conducted at least annually to test and evaluate the effectiveness of the plan. The plan must be reviewed and revised, as necessary, after any drill or exercise and after any incident.

§ 331.12 Biocontainment.

(a) An individual or entity required to register under this part must develop and implement a written biocontainment plan that is commensurate with the risk of the select agent or toxin, given its intended use.[4] The biocontainment plan must contain sufficient information and documentation to describe the containment procedures.

(b) The biocontainment procedures must be sufficient to contain the select agent or toxin (*e.g.*, physical structure

[4] Technical assistance and guidance may be obtained by contacting APHIS.

and features of the entity, and operational and procedural safeguards).

(c) In developing a biocontainment plan, an individual or entity should consider the following:

(1) ''Containment Facilities and Safeguards for Exotic Plant Pathogens and Pests'' (Robert P. Kahn and S.B. Mathur eds., 1999); and

(2) ''A Practical Guide to Containment: Greenhouse Research with Transgenic Plants and Microbes'' (Patricia L. Traynor ed., 2001).

(d) The plan must be reviewed annually and revised as necessary. Drills or exercises must be conducted at least annually to test and evaluate the effectiveness of the plan. The plan must be reviewed and revised, as necessary, after any drill or exercise and after any incident.

§ 331.13 Restricted experiments.[5]

(a) An individual or entity may not conduct the following experiments unless approved by and conducted in accordance with the conditions prescribed by the Administrator:

(1) Experiments utilizing recombinant DNA that involve the deliberate transfer of a drug resistance trait to select agents that are not known to acquire the trait naturally, if such acquisition could compromise the use of the drug to control disease agents in humans, veterinary medicine, or agriculture.

(2) Experiments involving the deliberate formation of recombinant DNA containing genes for the biosynthesis of toxins lethal for vertebrates at an LD_{50}<100 ng/kg body weight.

(b) The Administrator may revoke approval to conduct any of the experiments in paragraph (a) of this section, or revoke or suspend a certificate of registration, if the individual or entity fails to comply with the requirements of this part.

(c) To apply for approval to conduct any of the experiments in paragraph (a) of this section, an individual or entity must submit a written request and supporting scientific information to the Administrator. A written decision granting or denying the request will be issued.

§ 331.14 Incident response.[6]

(a) An individual or entity required to register under this part must develop and implement a written incident response plan.[7] The incident response plan must be coordinated with any entity-wide plans, kept in the workplace, and available to employees for review.

(b) The incident response plan must fully describe the entity's response procedures for the theft, loss, or release of a select agent or toxin; inventory discrepancies; security breaches (including information systems); severe weather and other natural disasters; workplace violence; bomb threats and suspicious packages; and emergencies such as fire, gas leak, explosion, power outage, etc. The response procedures must account for hazards associated with the select agent or toxin and appropriate actions to contain such agent or toxin.

(c) The incident response plan must also contain the following information:

(1) The name and contact information (*e.g.*, home and work) for the individual or entity (*e.g.*, responsible official, alternate responsible official(s), biosafety officer, etc.);

(2) The name and contact information for the building owner and/or manager, where applicable;

(3) The name and contact information for tenant offices, where applicable;

(4) The name and contact information for the physical security official for the building, where applicable;

(5) Personnel roles and lines of authority and communication;

(6) Planning and coordination with local emergency responders;

(7) Procedures to be followed by employees performing rescue or medical duties;

---

[5] For guidance, see the NIH publication, ''NIH Guidelines for Research Involving Recombinant DNA Molecules.'' This document is available on the Internet at *http://www.aphis.usda.gov/programs/ag__selectagent/index.html.*

[6] Nothing in this section is meant to supersede or preempt incident response requirements imposed by other statutes or regulations.

[7] Technical assistance and guidance may be obtained by contacting APHIS.