

Sandia National Laboratories' Comments on 42 CFR Part 73

General Comments

1. Federal oversight: The principal objectives of biological laboratory security should be defined at a federal level, to ensure consistency (Department of Homeland Security should have this responsibility). The principal objectives include the assets that require protection and the threats that those assets should be protected against. The purpose of this national oversight is to ensure that each facility containing similar agents is protected equally. Otherwise, there will be wide variation in the evaluation of threats and consequences, and a wide interpretation of what constitutes adequate security. In addition, it is only at the national level that adequate coordination with all relevant intelligence and law enforcement agencies can be made. See Section 73.11.
2. Access control: We believe that the security regulations are not adequate for the most dangerous pathogens and toxins (those that are the most likely to be diverted for use in bioterrorism). Laboratories or areas in which the most dangerous pathogens and toxins are stored and used should be secured with a modern access control system. Key locks and key control are terribly inadequate. See Section 73.11, paragraph (b)(2).
3. Diagnostic laboratory exemption: We believe that the regulations must require the exact same level of protection over a select agent at a diagnostic lab as anywhere else. An exempted diagnostic lab has seven days after identification of a select agent to destroy or transfer that agent. What protection is required over that select agent during those seven days that the agent is awaiting transfer or destruction? See Section 73.6, paragraph (a)(5).
4. Inspections: When will a certificate of registration or amendment be contingent upon inspection? What will the inspection entail? Who will the inspectors be? What level of training, in what subject areas, will they have? What will be the compliance standards used by the inspectors? Under what circumstances can those compliance standards change? See Section 73.7 and 73.16.
5. Attorney General risk assessment: This requirement addresses the prohibitions stated in the Patriot Act, but does not require much more basic personnel reliability screening. At a very minimum, every person approved to handle or use select agents should have a criminal background check and a credit check. This screening should take place at least every 5 years, or as job responsibilities change. Random drug screening should also be required. See Section 73.8.
6. Access: How is "access" defined? Many personnel within a containment space (such as a suite of laboratories) have "access" to freezers, incubators, etc. where select agents exist, even though they

do not ever handle or use the agents themselves. We recommend that “access” be changed to “handle or use” throughout the CFR. See Section 73.8, paragraph (b).

7. Information targets: Section 73.11, paragraph (b)(1) indicates that “cyber security” should be included in the security plan. What are the cyber/information security assets that should be protected? The select agents are specifically identified, but nothing similar exists for the cyber/information assets. The data related to the select agents, in many cases, are almost as valuable as the select agents themselves.

8. Escorting: What constitutes “escorting” - knowledge of location, visual contact, or close enough to make physical contact? Where must “escorting” begin and end? Can an individual who has failed the Attorney General’s screening be escorted into an area where there is “access” to select agents (where select agents are located)? We believe the answer should be “yes.” Can an individual who has failed the Attorney General’s screening be escorted while handling or using a select agent? We believe the answer should be “no.” The requirements must clarify these issues. See Section 73.11, paragraph (d)(1).

9. Package inspection: The requirement for package inspection upon entry and exit from the “area” is not at all practical, and provides almost no security value. The inspections will not be meaningful, and may very well be unsafe. What is the purpose of this requirement? What constitutes an “inspection”? Who is allowed to conduct this inspection? Where can these inspections take place? What are the inspectors supposed to look for? What allows the “inspector” to prevent the package from entering the “area”? Must an inspector be able to do diagnostic work on a sample leaving one of these laboratories to verify it is what the shipper says it is? We believe a statement requiring random inspections of packages entering or exiting the entity or laboratory would be sufficient and much more feasible. See Section 73.11, paragraph (d)(4).

10. Chain of custody: The requirements stipulate “protocols for intra-entity transfers.” This is too vague and inadequate. Intra-entity movement of select agents, when outside access-controlled laboratory areas, should follow a documented chain of custody process that minimizes any possibility of diversion. See Section Section 73.11, paragraph (d)(5).

11. Inter-entity transfers: These regulations do not address the security of shipments while in transit between entities. The current DOT requirement for external labeling on select agent packages should be eliminated. Both the shipping and receiving entities should document a chain of custody for transfers of select agents. These chain of custody documents should be securely stored with the EA-101 form at both the shipping and receiving entities. In addition, tamper-indicating procedures should be included in the packaging so that the recipient

would immediately know that the package he/she has received had been tampered with; this event should trigger an immediate report to HHS. See Section 73.14.

12. Information protection: A considerable amount of sensitive security and operational information will be collected as a result of these regulations. How will all of this information be marked, stored, and protected? Who will have access to this information? What “clearances” are required to have access to this information?

Specific Comments

Section 73.4 - Select Agents and Toxins

1. According to the summary for this section, the following criteria were used to determine which agents should appear on this list: 1) effect on human health; 2) degree of contagiousness and the methods of transmission; 3) availability and effectiveness of medical countermeasures; and 4) other criteria including needs of children and other vulnerable populations. Section 73.2 indicates that “the agents and toxins subject to requirements under this part are those that have the potential to pose a severe threat to public health and safety.” These criteria and this definition indicate that agents and toxins subject to requirements under this part are not necessarily those that are the most likely to be diverted from legitimate entities and weaponized for the purposes of bioterrorism. Arguably, the majority of the agents that appear on this list are not likely diversion or weaponization targets. And those that genuinely are targets for diversion and weaponization deserve much more comprehensive security than is required under these regulations. The security regulations should recognize that not all select agents are equal from a weaponization perspective: a set of graded protection requirements should be established such that the most dangerous pathogens and the most likely to be weaponized are protected at higher levels than the majority of the select agents.
2. Paragraph (f)(4): In regard to quantities of toxins, are these quantities of isolated toxin (i.e. toxin that has been extracted and is separate from the cell) or toxin that is in the process of being produced by living cells (and may increase in quantity)? This requires clarification. Measuring the exact quantities of toxin can only be reasonably achieved with toxins that have been isolated from the cell.

Section 73.6 - Exemptions

1. Paragraph (a)(2): The “immediate notification” list presented here is different than the “select agent” list presented in Section 73.4. Why? Does this mean that if a diagnostic laboratory determines that it has a

select agent, but not one on the list in this paragraph, then it does not have to notify HHS?

2. Paragraph (a)(5): An exempted diagnostic lab has seven days after identification of a select agent to destroy or transfer that agent. What protection is required over that select agent during those seven days that the agent is awaiting transfer or destruction? This is a significant vulnerability in the overall regulation.

Section 73.7 - Registration

1. How will HHS protect the information collected under (b)(2)?
2. How long will it take to receive a certificate of registration once an entity has submitted all the required paperwork?
3. When will a certificate of registration or amendment be contingent upon inspection? What will the inspection entail? Who will the inspectors be? What level of training, in what subject areas, will they have? What will be the compliance standards used by the inspectors?
4. When will HHS "observe" the destruction of a select agent?
5. Paragraph (d): "The RO must promptly notify the HHS in writing if ... [there are] changes in areas of work or changes in protocols or objectives of studies." This language is extremely vague. What exactly triggers a requirement to notify HHS?

Section 73.8 - Security Risk Assessment

1. "An entity may not provide an individual access to a select agent or toxin and an individual may not access a select agent or toxin, unless the individual is approved by the HHS Secretary or the USDA Secretary, based on a security risk assessment by the Attorney General." What does an entity do between now and when the Attorney General makes a decision?
2. What form must be submitted to the Attorney General? How long will it take? For new employees, must this investigation be completed prior to employment? Who will pay the cost of the investigation? How will appeals be handled? The process for personnel assurance is not well defined and does not include a timeline for completion by the Attorney General.
3. Paragraph (b): How is "access" defined? Many personnel within a containment space (such as a suite of laboratories) have "access" to freezers, incubators, etc. where select agents exist, even though they do not ever handle or use the agents themselves. We recommend that "access" be changed to "handle and use" throughout the CFR.
4. Expediting the review process is mentioned. Are the example "good causes" reasonable and are the expedited checks as thorough? If not, will an equally thorough review also be completed? Perhaps in these cases, escorting would be more appropriate than "expedited review."

5. While this “risk assessment” may address the Patriot Act personnel background issues, this section does not necessarily require much more basic personnel reliability screening. For instance, at a very minimum, every person approved to handle and use select agents should have a criminal background check and a credit check. This screening should take place at least every 5 years, or as job responsibilities change. Random drug screening should also be required.

Section 73.9 - Responsible Official

1. Paragraph (c)(2): How is “access” defined?
2. Paragraph (c)(3): How is “appropriate training” defined? What are the criteria for “appropriate” training?
3. Paragraph (c)(5): How is “timely” defined?

Section 73.11 - Security

1. Paragraph (a): "...threats are defined, vulnerabilities are examined, and risks associated with those vulnerabilities are mitigated..." should be replaced with "risks and consequences are examined, threats are defined, and vulnerabilities are identified. The security system should be designed to mitigate the identified vulnerabilities."
2. The use of the terms "risk assessment," "threat assessment," and "vulnerability assessment" are likely to be confusing to those with little experience in this area. We recommend a clarification of this terminology (and believe that these or similar definitions should appear in Section 73.1):
 - a. A target assessment must identify those agents that need protection against diversion (select agents and information related to select agents?).
 - b. A risk assessment is an evaluation of the probability and consequences of undesirable events that could affect the defined targets. It determines which of the possible (but unlikely) threats the security system should not be required to protect against. These are the risks that the facility accepts, and develops emergency response plans to address.
 - c. A threat assessment should not be an evaluation of all possible malevolent actions, but a judgment about which malevolent actions are most likely and what would be the consequences of those actions. These are the threats the security system must be designed to protect against.
 - d. A vulnerability assessment identifies only those vulnerabilities of the facility that would allow the defined threats to divert the defined targets. A security system can effectively protect the defined targets against the defined threats without mitigating every facility vulnerability.
3. How are threats defined? Is there a basic national definition that is tempered by locale, or does each facility get to define its own threats? The latter would not likely serve the interests of the U.S. Government. It is important, if not critical, that the principal objectives of biological laboratory security be defined at a federal level, to ensure consistency (Department of Homeland Security should have this responsibility). The principal objectives include the assets that require protection and the threats that those assets should be protected against. The purpose of this national oversight is to ensure that each facility containing similar agents is protected equally. Otherwise, there will be wide variation in the evaluation of threats and consequences, and a wide interpretation of what constitutes adequate security. In addition, it is only at the national level that adequate coordination with all relevant intelligence and law enforcement agencies can be made. This is also important so that local facilities are not exploited by for-profit security

organizations, whose interest is served by elevating the assessment of the threat and consequences to increase the amount of security equipment required to achieve adequate protection.

4. Paragraph (a): How is “security systems approach” defined?
5. How should the security plan be marked and protected? We recommend that security plans, and all information related to the security systems, be protected at the “Official Use Only” level.
6. Paragraph (b)(1): “Cyber security” should be replaced with “Information and cyber security”. What are the cyber/information security assets that should be protected? The select agents are specifically identified, but nothing similar exists for the cyber/information assets. Who is empowered to make that judgment?
7. Paragraph (b)(1): “The security plan must describe...physical security and cyber security.” What constitutes an adequate description of physical security and information and cyber security? Who gets to decide whether the plan is adequate? What standards will the inspectors use to judge the adequacy of the security plan?
8. Paragraph (b)(2): Why are “provisions for routine cleaning, maintenance, and repairs” called out? Access should be based on clearances and judgments about “need to access,” not job function. If these individuals have “clearances” or background checks, they are just as dependable as scientists. Instead, provisions should be called out for escorting those who have not been granted access by the Attorney General. Or perhaps this is in reference to routine cleaning, maintenance, and repairs of security equipment?
9. Paragraph (b)(2): “Protocols for changing access number or locks following staff changes”: Why? A card key access control system need not have keypad access numbers. In a modern access control system that includes PINs, changing keypad access numbers is not necessary. However, in a system based on key locks, a protocol for changing key locks and managing key control should be established. This language should be clarified. We also believe that key lock control of laboratories is not adequate security for select agents; a modern access control system should be required.
10. Paragraph (b)(5): How is “access” defined? If the container or freezer is located in an access-controlled area, which is limited to authorized personnel, what benefit is there to locking the freezer? Doesn’t the need to lock freezers depend on their physical location within the facility?
11. Paragraph (b)(6): How is “access” defined? What constitutes “training”? What qualifications must an individual have before he/she is approved to train others?
12. Paragraph (b)(7): “Establish procedures for reporting and removing unauthorized persons.” This exact language also appears in Paragraph (b)(5). Delete one.

13. Paragraph (b)(8): The wording here implies that these areas do not need to be secured when an authorized person is present. This is not appropriate. An area that contains select agents should be secured at all times, and only those authorized persons should have access to those areas. Otherwise, one authorized person will be responsible for security of an entire select agent area when he/she is present; that is a burden that individual should not have to bear alone.
14. Paragraph (d)(1): How is "access" defined? How is "escort" or "unescorted" defined? What constitutes "escorting" - knowledge of location, visual contact, or close enough to make physical contact? Where must "escorting" begin and end? Can an individual who has failed the Attorney General's screening be escorted into an area where there is "access" to select agents (where select agents are located)? We believe the answer should be "yes." Can an individual who has failed the Attorney General's screening be escorted while handling or using a select agent? We believe the answer should be "no." The requirements must clarify these issues.
15. Paragraph (d)(2): How are "escort" and "continually monitored" defined? Does this mean more rigorous escorting than required in Paragraph (d)(1)? If so, why? This paragraph is unnecessary. Either an individual is authorized to "handle or use" or he/she is not authorized. If he/she is not authorized, he/she must be closely escorted while inside an area where select agents are located.
16. Paragraph (d)(3): Why the requirement to lock freezers? If the container or freezer is located in an access-controlled area, which is limited to authorized personnel, what benefit is there to locking the freezer? Doesn't the need to lock freezers depend on their physical location within the facility? A freezer that contains select agents that is located outside an access-controlled area should be locked; a freezer that contains select agents that is located inside an access-controlled area need not be locked.
17. Paragraph (d)(3): How is "approved" defined? Is it or can it be different than "authorized"?
18. Paragraph (d)(3): The wording ("when they are not in direct view of approved staff") implies that these areas do not need to be secured when an authorized person is present. This is not appropriate. A freezer located outside an access-controlled area and containing select agents should be secured at all times, and only those authorized persons should have access to that freezer. Otherwise, one authorized person alone will be responsible for security of the select agent freezer when he/she is present; that is a burden that an individual should not have to bear alone.
19. Paragraph (d)(3): What are the criteria for determining if video surveillance is needed? Why is video surveillance called out specifically, as opposed to other technologies? Video surveillance provides no security; it is only beneficial for historical purposes.

20. Paragraph (d)(4): Package inspection upon entry and exit. The use of the term “area” in this paragraph implies that inspections must take place upon a package’s entry to and exit from a select agent laboratory area. This is not at all practical, and there is almost no security value. The inspections will not be meaningful, and may very well be unsafe. What is the purpose of this requirement? What constitutes an “inspection”? Who is allowed to conduct this inspection? Where can these inspections take place? What are the inspectors supposed to look for? What allows the “inspector” to prevent the package from entering the “area”? Must an inspector be able to do diagnostic work on a sample leaving one of these laboratories to verify it is what the shipper says it is? We believe a statement requiring random inspections of packages entering or exiting the entity or laboratory would be sufficient and much more feasible.
21. Paragraph (d)(5): A “protocol for intra-entity transfers” is extremely vague. Does this refer to transfers of select agents, or transfers of everything? The requirement as stated is too restrictive for non-select agents, and not specific enough for select agents. A “protocol” could be arrangement that allows an individual to leave a package of select agents temporarily unattended in an open air lock: that is not security. Intra-entity movement of select agents, when outside access-controlled laboratory areas, should follow a documented chain of custody process that minimizes any possibility of diversion.

Section 73.13 - Training

1. What constitutes “training”? What qualifications must an individual have before he/she is approved to train others? Who is empowered to decide whether the training is adequate?
2. Paragraph (d): “In lieu of initial training for those individuals already involved in handling select agents, the Responsible Official may certify in writing that the individual has the required knowledge, skills, and abilities to safely carry out the duties and responsibilities.” It is highly unlikely that those individuals will have the appropriate security training-since significant security changes are likely. General security awareness training must be required for all employees.

Section 73.14 - Transfers

1. This section does not seem to prohibit hand-carried transfers. This section should explicitly permit hand-carried transfers, but should impose all the same reporting requirements (e.g. completion of CDC Form EA-101) for hand-carried transfers.
2. There is no indication how long the RO must keep the EA-101 form. The requirement should state that EA-101 forms must be securely stored for five years.

3. Paragraph (h): Reporting of destruction is required within five days after destruction. This is in contradiction to Section 73.7, paragraph (h), which requires an entity to provide notice in writing to HHS at least five business days before destroying an agent or toxin.
4. There is not any requirement to ensure custody of a select agent during the transfer process. Intra-entity movement of select agents, when outside access-controlled laboratory areas, should follow a documented chain of custody process that minimizes any possibility of diversion. Both the shipping and receiving entities should document a chain of custody for transfers of select agents. These chain of custody documents should be securely stored with the EA-101 form at both the shipping and receiving entities.
5. These regulations do not address the security of shipments while in transit between entities. Currently, DOT requires labeling on the outside of packages indicating that a certain select agent is within the package. This DOT requirement should be removed for shipments of select agents. In addition, tamper-indicating procedures should be included in the packaging so that the recipient would immediately know that the package he/she had received had been tampered with; this event should trigger an immediate report to HHS.

Section 73.15 - Records

1. How will this information be marked and protected (e.g. Official Use Only)?
2. What information security requirements are there for this information (e.g. Can it be stored on an open network? Can it be transferred across the internet through unprotected email?)

Section 73.16 - Inspections

1. What training are the inspectors required to receive? How frequently must this training be updated? What level of background screening/security clearance must the inspectors possess?
2. Will there be separate security and safety inspectors, or will one inspector be empowered to assess both safety and security requirements?
3. What standards will the inspectors use to assess compliance with the regulations?
4. How will the inspectors' reports be marked and protected?

Reynolds Salerno
Sandia National Laboratories
Dept 5324 International Security Initiatives
(505)844-8971