

Sandia National Laboratories' Comments on 7 CFR 331 and 9 CFR 121

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 331.11 and 121.12.
2. APHIS vs. CDC oversight: Section 121.7, paragraph (c) indicates that APHIS and CDC will jointly review the security the applications for overlap agents. Will this joint review follow APHIS or CDC security, inspection, and compliance standards? What happens if APHIS and CDC do not concur? Sections 331.11 and 121.12, paragraph (2) reference both USDA Department Manual No. 9610-001 and NIH/CDC BMBL Appendix F for security guidance. These documents differ significantly. Will security compliance for overlap agents be based on USDA or HHS security guidelines?
3. Diagnostic lab exemption: We believe that the regulations must require the exact same level of protection over a select agent at a diagnostic laboratory as anywhere else. An exempted diagnostic lab has seven days after identification of a select agent to destroy or transfer that agent (or within 90 days of receipt for specimens submitted for proficiency testing). What protection is required over that select agent during those seven or 90 days that the agent is awaiting transfer or destruction? See Section 331.4 and 121.4/5, paragraph (2).
4. Restricting access: 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 Sections 331.10 and 121.11.
5. Access definition: 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 Sections 331.10/11 and 121.11/12.
6. 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 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 is terribly inadequate. See Section 333.11 and 121.12, paragraph (a)(2)(iii).

7. 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. Sections 331.11 and 121.12, paragraphs (a)(2)(iv)(A and B).

8. Information targets: Sections 331.11 and 121.12, paragraphs (a)(2)(iii) 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.

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 would be sufficient and much more feasible. See Sections 331.11 and 121.12, paragraphs (a)(2)(iv)(D).

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 Sections 331.11 and 121.12, paragraphs (a)(2)(iv)(E).

11. Compliance 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 Sections 331.15 and 121.16.

12. 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 had received had been tampered with; this event should trigger an immediate report to HHS. See Sections 331.13 and 121.14.

13. 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

7 CFR 331.3 and 9 CFR 121.3 - List of Biological Agents and Toxins

1. These sections state that listed agents are those which “have been determined to have the potential to pose a severe threat to plant (animal) health or plant (animal) products.” Neither section outlines the criteria used to determine which agents should appear on the list. This definition also indicates 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 listed 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. 9 CFR 121.3 Paragraph (f)(3): 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.
3. 9 CFR 121.3 Paragraph (b): This paragraph lists both “Botulinum neurotoxin producing species of Clostridium” and “Clostridium botulinum” as overlap agents and toxins. However, “Clostridium botulinum” is not listed separately in 42 CFR 73.5. Additionally, “Botulinum neurotoxins” are listed as overlap toxins in 9 CFR 121.3, but are not found in 42 CFR 73.5.

7 CFR 331.4 and 9 CFR 121.4/5 - Exemptions

1. 7 CFR 331.4 and 9 CFR 121.4/121.5 Paragraph (2): 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.
2. 9 CFR 121.4/121.5 Paragraph (2)(b): An exempted lab working with overlap agents and toxins in specimens submitted for proficiency testing is allowed 90 days from receipt to transfer or destruction of the agents or toxins. What protection is required over the overlap agent or toxin from the point of recognition until transfer or destruction? This is a significant vulnerability in the overall regulation.

7 CFR 331.5/6/7/8 and 9 CFR 121.6/7/8/9 - Registration

1. How will APHIS protect the information collected under these sections?
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 APHIS “observe” the destruction of a select agent?
5. 9 CFR 121.7 Paragraph (c): CDC and APHIS will jointly review the security for overlap agents. Will this joint review follow APHIS or CDC security, inspection, and compliance standards? What happens if CDC and APHIS do not concur? Will there be an appeals process?
6. 7 CFR 331.7 and 9 CFR 121.8 Paragraphs (a)(5): Registration may be denied if the entity does not meet the containment and security requirements prescribed by the Administrator. If registration is thus denied, APHIS may provide technical assistance and guidance. What will determine if and to what degree APHIS will provide assistance?

7 CFR 331.9 and 9 CFR 121.10 - Responsible Official

1. Paragraphs (a)(2): How is “access” defined?
2. Paragraphs (a)(3): How is “appropriate training” defined? What are the criteria for “appropriate” training? This is also ill defined in 9 CFR 121.13 and 7 CFR 331.12.

7 CFR 331.10 and 9 CFR 121.11 - Restricting Access

1. APHIS may grant, limit, or deny individual access to listed agents or toxins based on a security risk assessment by the Attorney General. How long will this process normally take and what does an entity do while awaiting the Attorney General’s decision? For new employees, must this investigation be completed prior to employment? Who will pay the cost of the investigation? What form is the individual supposed to reference? What is the appeal process for individuals denied or restricted access? This appeals process is not clarified in 7 CFR 331.15 or 9 CFR 121.17. The process for personnel assurance is not well defined and does not include a timeline for completion by the Attorney General.
2. 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.

3. Expediting the review process is mentioned. 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.”
4. While the Attorney General check may address the Patriot Act personnel background issues, this section does not 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 also take place at least every 5 years, or as job responsibilities change. Random drug screening should also be required.

7 CFR 331.11 and 9 CFR 121.12 - Security

1. Paragraph (a)(1): The reference to “inventory control” is ambiguous. Inventory control procedures are required throughout the security section of these documents, however inventory control is not defined in Sections 331.1 or 121.1.
2. Paragraph (a)(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 Sections 331.1 and 121.1):
 - a. A target assessment must identify those agents that need protection against diversion (listed agents and information related to listed 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 2, note 13: This paragraph references USDA Departmental Manual No. 9610-001 as well as CDC's Appendix F of the "Biosafety in Microbiological and Biomedical Laboratories" for security guidance. These documents differ significantly in their security approach, as well as the labs to which they are intended to apply. Will security compliance be based on USDA or CDC security guidelines for overlap agents? This reinforces the need for one central, federal set of guidelines to ensure consistency (Department of Homeland Security should have this responsibility).
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 (a)(2): "in accordance with the threat posed by the agent or toxin" should be replaced with "in accordance with the consequences posed by the agent or toxin." Please note previous comments regarding definitions.
7. Paragraph (a)(2)(i): "Risks associated with those vulnerabilities are mitigated" should be replaced with "consequences associated with those vulnerabilities are mitigated." Please note previous comments regarding definitions.
8. Paragraph (a)(2)(iii): "Cyber security" should be replaced with "Information and cyber security". What are the cyber/information security assets that should be protected? The listed agents are specifically identified, but nothing similar exists for the cyber/information assets. Who is empowered to make that judgment?
9. Paragraphs (a)(2)(iii): "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?
10. Paragraphs (a)(2)(iii): "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.

11. Paragraphs (a)(2)(iv)(A): 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 listed agents (where listed 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 listed agent? We believe the answer should be “no.” The requirements must clarify these issues.
12. Paragraph (a)(2)(iv)(B): 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?
13. Paragraphs (a)(2)(iv)(B): How are “escort” and “continually monitored” defined? Does this mean more rigorous escorting than required in Paragraph (a)(2)(iv)(A)? 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 listed agents are located.
14. Paragraphs (a)(2)(iv)(C): How is “access” defined?
15. Paragraphs (a)(2)(iv)(C): 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.
16. Paragraphs (a)(2)(iv)(C): Why the requirement to lock containers? 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 listed 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 (a)(2)(iv)(C): The wording (“when not in direct view of an approved individual”) 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.
18. Paragraph (a)(2)(iv)(D): Package inspection upon entry and exit. This paragraph implies that inspections must take place upon a package’s entry to and exit from a listed 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 would be sufficient and much more feasible.
19. Paragraph (a)(2)(iv)(E): 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-listed agents, and not specific enough for listed agents. A “protocol” could be an arrangement that allows an individual to leave a package of listed agents temporarily unattended in an open air lock: that is not security. Intra-entity movement of listed agents, when outside access-controlled laboratory areas, should follow a documented chain of custody process that minimizes any possibility of diversion.
20. Paragraphs (a)(2)(iv)(C and E and F and G): How is “approved” defined? Is it or can it be different than “authorized”?
21. Paragraph (3)(b): Who will review, performance test, and update the Biosafety/containment and Security Plans on an annual basis? What will be the performance standards and criteria used to assess compliance in this review?

7 CFR 331.12 and 9 CFR 121.13 - 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?

7 CFR 331.13 and 9 CFR 121.14 - 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 APHIS Form 2041) for hand-carried transfers.
2. There is no indication how long the RO must keep the 2041 form. This is also not found under Records sections 7 CFR 331.14 or 9 CFR 121.15. The requirement should state that 2041 forms must be securely stored for five years.
3. Notification of listed agent destruction is not required by APHIS. This contradicts HHS 73.7 and 73.14.
4. There is not any requirement to ensure custody of a listed 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 listed agents. These chain-of-custody documents should be securely stored with the 2041 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 listed agents. 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 APHIS.
6. APHIS Form 2041 does not require the sender to notify the recipient of the estimated time of package arrival (as found in the CDC's EA-101 Form for Select Agents). Rather, the actual form is sent with the package through the transport system. Form 2041 should follow the same procedures as EA-101.

7 CFR 331.14 and 9 CFR 121.15 - 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? Can it be stored on an open network? How long should it be stored? Can it be transferred across the internet through unprotected email?

7 CFR 331.15 and 9 CFR 121.16 - 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?
5. Inspectors should also be required to take site-specific safety and security training.

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