

Inspection Checklist for Security (7 CFR 331, 9 CFR 121, 42 CFR 73)

Entity Name:

Inspection Date:

Building/Rooms:

Inspectors:

When information is entered in this form, the form is to be considered "Sensitive Select Agent Information."

Section	Regulation Text	Observation	Status	Comments
10(a)	An individual or entity required to register under this part 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 Administrator, following a security risk assessment by the Attorney General.	An individual or entity required to register under this part 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 Administrator, following a security risk assessment by the Attorney General.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
10(g)(1)	An individual or entity required to register under [the select agents and toxins regulations] 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 Administrator, following a security risk assessment by the Attorney General. An individual's access approval will be denied or revoked if the individual is within any of the categories described in 18 U.S.C. 175b [or as defined in Section 10 of the select agents and toxins regulations].	An individual or entity required to register under [the select agents and toxins regulations] 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 Administrator, following a security risk assessment by the Attorney General. An individual's access approval will be denied or revoked if the individual is within any of the categories described in 18 U.S.C. 175b [or as defined in Section 10 of the select agents and toxins regulations].	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
10(k)	The Responsible Official must immediately notify CDC or APHIS when an individual's access to select agents or toxins is terminated by the entity and the reasons therefore.	The Responsible Official must immediately notify CDC or APHIS when an individual's access to select agents or toxins is terminated by the entity and the reasons therefore.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(a)	An individual or entity required to register under this part must develop and implement a written security plan. The security plan must be sufficient to safeguard the select agent or toxin against unauthorized access, theft, loss, or release.	An individual or entity required to register under this part must develop and implement a written security plan. The security plan must be sufficient to safeguard the select agent or toxin against unauthorized access, theft, loss, or release.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(a)	An individual or entity required to register under this part must develop and implement a written security plan. The security plan must be sufficient to safeguard the select agent or toxin against unauthorized access, theft, loss, or release.	Entity has implemented pre-access suitability and ongoing suitability assessments as described in plan [11(f)(1), 11(f)(3), 11(f)(4)(i)].	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	

Section	Regulation Text	Observation	Status	Comments
11(b)	The security plan must be designed according to a site-specific risk assessment and must provide graded protection in accordance with the risk of the select agent or toxin, given its intended use. A current security plan must be submitted for initial registration, renewal of registration, or when requested.	The security plan must be designed according to a site-specific risk assessment and must provide graded protection in accordance with the risk of the select agent or toxin, given its intended use. A current security plan must be submitted for initial registration, renewal of registration, or when requested.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(c)(1)	The security plan must describe procedures for physical security, inventory control, and information systems control.	The security plan must describe procedures for physical security, inventory control, and information systems control.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(c)(2)	The security plan must contain provisions for the control of access to select agents and toxins including the safeguarding of animals (including arthropods) or plants intentionally or accidentally exposed to or infected with a select agent, against unauthorized access, theft, loss or release.	The security plan must contain provisions for the control of access to select agents and toxins including the safeguarding of animals (including arthropods) or plants intentionally or accidentally exposed to or infected with a select agent, against unauthorized access, theft, loss or release.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(c)(3)	The security plan must contain provisions for routine cleaning, maintenance, and repairs.	The security plan must contain provisions for routine cleaning, maintenance, and repairs.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(c)(4)	The security plan must establish procedures for removing unauthorized or suspicious persons.	The security plan must establish procedures for removing unauthorized or suspicious persons.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(c)(5)	The security plan must describe procedures for addressing loss or compromise of keys, keycards, passwords, combinations, etc. and protocols for changing access permissions or locks following staff changes.	The security plan must describe procedures for addressing loss or compromise of keys, keycards, passwords, combinations, etc. and protocols for changing access permissions or locks following staff changes.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(c)(6)	The security plan must 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.	The security plan must 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.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(c)(7)	The security plan must contain provisions for ensuring that all individuals with access approval from the HHS Secretary or Administrator understand and comply with the security procedures.	The security plan must contain provisions for ensuring that all individuals with access approval from the HHS Secretary or Administrator understand and comply with the security procedures.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	

Section	Regulation Text	Observation	Status	Comments
11(c)(8)	The security plan must describe procedures for how the Responsible Official will be informed of suspicious activity that may be criminal in nature and related to the entity, its personnel, or its select agents or toxins; and describe procedures for how the entity will notify the appropriate Federal, State, or local law enforcement agencies of such activity.	The security plan must describe procedures for how the Responsible Official will be informed of suspicious activity that may be criminal in nature and related to the entity, its personnel, or its select agents or toxins; and describe procedures for how the entity will notify the appropriate Federal, State, or local law enforcement agencies of such activity.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(c)(9)(i)	The security plan must contain provisions for information security that ensure that all external connections to systems which manage security for the registered space are isolated or have controls that permit only authorized and authenticated users.	The security plan must contain provisions for information security that ensure that all external connections to systems which manage security for the registered space are isolated or have controls that permit only authorized and authenticated users.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(c)(9)(ii)	The security plan must contain provisions for information security that ensure that authorized and authenticated users are only granted access to select agent and toxin related information, files, equipment (e.g., servers or mass storage devices) and applications as necessary to fulfill their roles and responsibilities, and that access is modified when the user's roles and responsibilities change or when their access to select agents and toxins is suspended or revoked.	The security plan must contain provisions for information security that ensure that authorized and authenticated users are only granted access to select agent and toxin related information, files, equipment (e.g., servers or mass storage devices) and applications as necessary to fulfill their roles and responsibilities, and that access is modified when the user's roles and responsibilities change or when their access to select agents and toxins is suspended or revoked.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(c)(9)(iii)	The security plan must contain provisions for information security that ensure that controls are in place that are designed to prevent malicious code (such as, but not limited to, computer virus, worms, spyware) from compromising the confidentiality, integrity, or availability of information systems which manage access to spaces registered under this part or records in §73.17.	The security plan must contain provisions for information security that ensure that controls are in place that are designed to prevent malicious code (such as, but not limited to, computer virus, worms, spyware) from compromising the confidentiality, integrity, or availability of information systems which manage access to spaces registered under this part or records in §73.17.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(c)(9)(iv)	The security plan must contain provisions for information security that establish a robust configuration management practice for information systems to include regular patching and updates made to operating systems and individual applications.	The security plan must contain provisions for information security that establish a robust configuration management practice for information systems to include regular patching and updates made to operating systems and individual applications.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	

Section	Regulation Text	Observation	Status	Comments
11(c)(9)(v)	The security plan must contain provisions for information security that establish procedures that provide backup security measures in the event that access control systems, surveillance devices, and/or systems that manage the requirements of section 17 of this part are rendered inoperable.	The security plan must contain provisions for information security that establish procedures that provide backup security measures in the event that access control systems, surveillance devices, and/or systems that manage the requirements of section 17 of this part are rendered inoperable.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(c)(10)	The security plan must contain provisions and policies for shipping, receiving, and storage of select agents and toxins, including documented procedures for receiving, monitoring, and shipping of all select agents and toxins. These provisions must provide that an entity will properly secure containers on site and have a written contingency plan for unexpected shipments.	The security plan must contain provisions and policies for shipping, receiving, and storage of select agents and toxins, including documented procedures for receiving, monitoring, and shipping of all select agents and toxins. These provisions must provide that an entity will properly secure containers on site and have a written contingency plan for unexpected shipments.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(d)(1)	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Allow access only to individuals with access approval from the HHS Secretary or Administrator.	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Allow access only to individuals with access approval from the HHS Secretary or Administrator.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(d)(2)	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Allow individuals not approved for access from the HHS Secretary or Administrator to conduct routine cleaning, maintenance, repairs, or other activities not related to select agents or toxins only when continuously escorted by an approved individual if the potential for access to select agents or toxins exists.	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Allow individuals not approved for access from the HHS Secretary or Administrator to conduct routine cleaning, maintenance, repairs, or other activities not related to select agents or toxins only when continuously escorted by an approved individual if the potential for access to select agents or toxins exists.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(d)(3)	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: 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).	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: 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).	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	

Section	Regulation Text	Observation	Status	Comments
11(d)(4)	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Inspect all suspicious packages before they are brought into or removed from the area where select agents or toxins are used or stored.	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Inspect all suspicious packages before they are brought into or removed from the area where select agents or toxins are used or stored.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(d)(5)	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Establish a protocol for intra-entity transfers under the supervision of an individual with access approval from the HHS Secretary or Administrator, including chain-of-custody documents and provisions for safeguarding against theft, loss, or release.	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Establish a protocol for intra-entity transfers under the supervision of an individual with access approval from the HHS Secretary or Administrator, including chain-of-custody documents and provisions for safeguarding against theft, loss, or release.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(d)(6)	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Require that individuals with access approval from the HHS Secretary or Administrator refrain from sharing with any other person their unique means of accessing a select agent or toxin (e.g., keycards or passwords).	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Require that individuals with access approval from the HHS Secretary or Administrator refrain from sharing with any other person their unique means of accessing a select agent or toxin (e.g., keycards or passwords).	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	

Section	Regulation Text	Observation	Status	Comments
11(d)(7)	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Require that individuals with access approval from the HHS Secretary or Administrator immediately report any of the following to the Responsible Official: (i) Any loss or compromise of keys, passwords, combination, 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 (vi) Any loss of computer, hard drive or other data storage device containing information that could be used to gain access to select agents or toxins.	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Require that individuals with access approval from the HHS Secretary or Administrator immediately report any of the following to the Responsible Official: (i) Any loss or compromise of keys, passwords, combination, 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 (vi) Any loss of computer, hard drive or other data storage device containing information that could be used to gain access to select agents or toxins.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(d)(7)(i)	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Require that individuals with access approval from the HHS Secretary or Administrator immediately report any of the following to the Responsible Official: (i) Any loss or compromise of keys, passwords, combination, etc.	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Require that individuals with access approval from the HHS Secretary or Administrator immediately report any of the following to the Responsible Official: (i) Any loss or compromise of keys, passwords, combination, etc.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(d)(7)(ii)	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Require that individuals with access approval from the HHS Secretary or Administrator immediately report any of the following to the Responsible Official: (ii) Any suspicious persons or activities.	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Require that individuals with access approval from the HHS Secretary or Administrator immediately report any of the following to the Responsible Official: (ii) Any suspicious persons or activities.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	

Section	Regulation Text	Observation	Status	Comments
11(d)(7)(iii)	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Require that individuals with access approval from the HHS Secretary or Administrator immediately report any of the following to the Responsible Official: (iii) Any loss or theft of select agents or toxins.	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Require that individuals with access approval from the HHS Secretary or Administrator immediately report any of the following to the Responsible Official: (iii) Any loss or theft of select agents or toxins.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(d)(7)(iv)	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Require that individuals with access approval from the HHS Secretary or Administrator immediately report any of the following to the Responsible Official: (iv) Any release of a select agent or toxin.	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Require that individuals with access approval from the HHS Secretary or Administrator immediately report any of the following to the Responsible Official: (iv) Any release of a select agent or toxin.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(d)(7)(v)	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Require that individuals with access approval from the HHS Secretary or Administrator immediately report any of the following to the Responsible Official: (v) Any sign that inventory or use records for select agents or toxins have been altered or otherwise compromised.	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Require that individuals with access approval from the HHS Secretary or Administrator immediately report any of the following to the Responsible Official: (v) Any sign that inventory or use records for select agents or toxins have been altered or otherwise compromised.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(d)(7)(vi)	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Require that individuals with access approval from the HHS Secretary or Administrator immediately report any of the following to the Responsible Official: (vi) Any loss of computer, hard drive or other data storage device containing information that could be used to gain access to select agents or toxins.	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Require that individuals with access approval from the HHS Secretary or Administrator immediately report any of the following to the Responsible Official: (vi) Any loss of computer, hard drive or other data storage device containing information that could be used to gain access to select agents or toxins.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	

Section	Regulation Text	Observation	Status	Comments
11(d)(8)	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Separate areas where select agents and toxins are stored or used from the public areas of the building.	An individual or entity must adhere to the following security requirements or implement measures to achieve an equivalent or greater level of security: Separate areas where select agents and toxins are stored or used from the public areas of the building.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(e)(1)	Entities must conduct complete inventory audits of all affected select agents and toxins in long-term storage when any of the following occur: Upon the physical relocation of a collection or inventory of select agents or toxins for those select agents or toxins in the collection or inventory.	Entities must conduct complete inventory audits of all affected select agents and toxins in long-term storage when any of the following occur: Upon the physical relocation of a collection or inventory of select agents or toxins for those select agents or toxins in the collection or inventory.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(e)(2)	Entities must conduct complete inventory audits of all affected select agents and toxins in long-term storage when any of the following occur: Upon the departure or arrival of a principal investigator for those select agents and toxins under the control of that principal investigator.	Entities must conduct complete inventory audits of all affected select agents and toxins in long-term storage when any of the following occur: Upon the departure or arrival of a principal investigator for those select agents and toxins under the control of that principal investigator.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(e)(3)	Entities must conduct complete inventory audits of all affected select agents and toxins in long-term storage when any of the following occur: In the event of a theft or loss of a select agent or toxin, all select agents and toxins under the control of that principal investigator.	Entities must conduct complete inventory audits of all affected select agents and toxins in long-term storage when any of the following occur: In the event of a theft or loss of a select agent or toxin, all select agents and toxins under the control of that principal investigator.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(f)(1)	In addition to the requirements contained in paragraphs (c) and (d) of this section, the security plan for an individual or entity possessing a Tier 1 select agent or toxin must also describe procedures for conducting a pre-access suitability assessment of persons who will have access to a Tier 1 select agent or toxin.	In addition to the requirements contained in paragraphs (c) and (d) of this section, the security plan for an individual or entity possessing a Tier 1 select agent or toxin must also describe procedures for conducting a pre-access suitability assessment of persons who will have access to a Tier 1 select agent or toxin.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	

Section	Regulation Text	Observation	Status	Comments
11(f)(2)	In addition to the requirements contained in paragraphs (c) and (d) of this section, the security plan for an individual or entity possessing a Tier 1 select agent or toxin must also describe procedures for how an entity's Responsible Official will coordinate their efforts with the entity's safety and security professionals to ensure security of Tier 1 select agents and toxins and share, as appropriate, relevant information.	In addition to the requirements contained in paragraphs (c) and (d) of this section, the security plan for an individual or entity possessing a Tier 1 select agent or toxin must also describe procedures for how an entity's Responsible Official will coordinate their efforts with the entity's safety and security professionals to ensure security of Tier 1 select agents and toxins and share, as appropriate, relevant information.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(f)(3)(i)	In addition to the requirements contained in paragraphs (c) and (d) of this section, the security plan for an individual or entity possessing a Tier 1 select agent or toxin must also describe procedures for the ongoing assessment of the suitability of personnel with access to a Tier 1 select agent or toxin. The procedures must include self- and peer-reporting of incidents or conditions that could affect an individual's ability to safely have access to or work with select agents and toxins, or to safeguard select agents and toxins from theft, loss, or release.	In addition to the requirements contained in paragraphs (c) and (d) of this section, the security plan for an individual or entity possessing a Tier 1 select agent or toxin must also describe procedures for the ongoing assessment of the suitability of personnel with access to a Tier 1 select agent or toxin. The procedures must include self- and peer-reporting of incidents or conditions that could affect an individual's ability to safely have access to or work with select agents and toxins, or to safeguard select agents and toxins from theft, loss, or release.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(f)(3)(ii)	In addition to the requirements contained in paragraphs (c) and (d) of this section, the security plan for an individual or entity possessing a Tier 1 select agent or toxin must also describe procedures for the ongoing assessment of the suitability of personnel with access to a Tier 1 select agent or toxin. The procedures must include the training of employees with access to Tier 1 select agents and toxins on entity policies and procedures for reporting, evaluation, and corrective actions concerning the assessment of personnel suitability.	In addition to the requirements contained in paragraphs (c) and (d) of this section, the security plan for an individual or entity possessing a Tier 1 select agent or toxin must also describe procedures for the ongoing assessment of the suitability of personnel with access to a Tier 1 select agent or toxin. The procedures must include the training of employees with access to Tier 1 select agents and toxins on entity policies and procedures for reporting, evaluation, and corrective actions concerning the assessment of personnel suitability.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	

Section	Regulation Text	Observation	Status	Comments
11(f)(3)(iii)	In addition to the requirements contained in paragraphs (c) and (d) of this section, the security plan for an individual or entity possessing a Tier 1 select agent or toxin must also describe procedures for the ongoing assessment of the suitability of personnel with access to a Tier 1 select agent or toxin. The procedures must include the ongoing suitability monitoring of individuals with access to Tier 1 select agents and toxins.	In addition to the requirements contained in paragraphs (c) and (d) of this section, the security plan for an individual or entity possessing a Tier 1 select agent or toxin must also describe procedures for the ongoing assessment of the suitability of personnel with access to a Tier 1 select agent or toxin. The procedures must include the ongoing suitability monitoring of individuals with access to Tier 1 select agents and toxins.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(f)(4)(i)	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: Procedures that will limit access to a Tier 1 select agent or toxin to only those individuals who are approved by the HHS Secretary or Administrator, following a security risk assessment by the Attorney General, have had an entity-conducted pre-access suitability assessment, and are subject to the entity's procedures for ongoing suitability assessment.	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: Procedures that will limit access to a Tier 1 select agent or toxin to only those individuals who are approved by the HHS Secretary or Administrator, following a security risk assessment by the Attorney General, have had an entity-conducted pre-access suitability assessment, and are subject to the entity's procedures for ongoing suitability assessment.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(f)(4)(ii)	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: Procedures that limit access to laboratory and storage facilities outside of normal business hours to only those specifically approved by the Responsible Official or designee.	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: Procedures that limit access to laboratory and storage facilities outside of normal business hours to only those specifically approved by the Responsible Official or designee.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(f)(4)(iii)	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: Procedures for allowing visitors, their property, and vehicles at the entry and exit points to the registered space, or at other designated points of entry to the building, facility, or compound that are based on the entity's site-specific risk assessment.	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: Procedures for allowing visitors, their property, and vehicles at the entry and exit points to the registered space, or at other designated points of entry to the building, facility, or compound that are based on the entity's site-specific risk assessment.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	

Section	Regulation Text	Observation	Status	Comments
11(f)(4)(iv)	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: A minimum of three security barriers where each security barrier adds to the delay in reaching secured areas where select agents and toxins are used or stored. One of the security barriers must be monitored in such a way as to detect intentional and unintentional circumventing of established access control measures under all conditions (day/night, severe weather, etc.) The final barrier must limit access to the select agent or toxin to personnel approved by the HHS Secretary or Administrator, following a security risk assessment by the Attorney General.	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: A minimum of three security barriers where each security barrier adds to the delay in reaching secured areas where select agents and toxins are used or stored. One of the security barriers must be monitored in such a way as to detect intentional and unintentional circumventing of established access control measures under all conditions (day/night, severe weather, etc.) The final barrier must limit access to the select agent or toxin to personnel approved by the HHS Secretary or Administrator, following a security risk assessment by the Attorney General.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(f)(4)(v)	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: All registered space or areas that reasonably afford access to the registered space must be protected by an intrusion detection system (IDS) unless physically occupied.	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: All registered space or areas that reasonably afford access to the registered space must be protected by an intrusion detection system (IDS) unless physically occupied.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(f)(4)(vi)	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: Personnel monitoring the IDS must be capable of evaluating and interpreting the alarm and alerting the designated security response force or law enforcement.	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: Personnel monitoring the IDS must be capable of evaluating and interpreting the alarm and alerting the designated security response force or law enforcement.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(f)(4)(vii)	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: For powered access control systems, describe procedures to ensure that security is maintained in the event of the failure of access control systems due to power disruption affecting registered space.	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: For powered access control systems, describe procedures to ensure that security is maintained in the event of the failure of access control systems due to power disruption affecting registered space.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	

Section	Regulation Text	Observation	Status	Comments
11(f)(4)(viii)(A)	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: The entity must determine that the response time for security forces or local police will not exceed 15 minutes where the response time is measured from the time of an intrusion alarm, or report of a security incident, to the arrival of the responders at the first security barrier.	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: The entity must determine that the response time for security forces or local police will not exceed 15 minutes where the response time is measured from the time of an intrusion alarm, or report of a security incident, to the arrival of the responders at the first security barrier.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(f)(4)(viii)(B)	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: The entity must provide security barriers that are sufficient to delay unauthorized access until the response force arrives in order to safeguard the select agents and toxins from theft, intentional release, or unauthorized access. The response time is measured from the time of an intrusion alarm, or report of a security incident, to the arrival of the responders at the first security barrier.	Entities with Tier 1 select agents and toxins must prescribe the following security enhancements: The entity must provide security barriers that are sufficient to delay unauthorized access until the response force arrives in order to safeguard the select agents and toxins from theft, intentional release, or unauthorized access. The response time is measured from the time of an intrusion alarm, or report of a security incident, to the arrival of the responders at the first security barrier.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(g)	In developing a security plan, an individual or entity should consider the document entitled, "Security Guidance for Select Agent or Toxin Facilities." This document is available on the National Select Agent Registry at http://www.selectagents.gov/ .	In developing a security plan, an individual or entity should consider the document entitled, "Security Guidance for Select Agent or Toxin Facilities." This document is available on the National Select Agent Registry at http://www.selectagents.gov/ .	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(h)	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. Drills or exercises must be documented to include how the drill or exercise tested and evaluated the plan, any problems that were identified and corrective action(s) taken, and the names of registered entity personnel participants.	The plan must be reviewed annually and revised as necessary.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	

Section	Regulation Text	Observation	Status	Comments
11(h)	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. Drills or exercises must be documented to include how the drill or exercise tested and evaluated the plan, any problems that were identified and corrective action(s) taken, and the names of registered entity personnel participants.	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.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	
11(h)	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. Drills or exercises must be documented to include how the drill or exercise tested and evaluated the plan, any problems that were identified and corrective action(s) taken, and the names of registered entity personnel participants.	Drills or exercises must be documented to include how the drill or exercise tested and evaluated the plan, any problems that were identified and corrective action(s) taken, and the names of registered entity personnel participants.	<input type="radio"/> No <input type="radio"/> Yes <input type="radio"/> N/A	