Security Sensitive Biological Agents Regulatory Scheme

Internal review tool

Sensitive information once completed

Version 5, January 2026

Entity name: Enter the name of the entity

Facility name: Enter the name of the facility

Approvals

Completed by:	Enter name Enter position	Date:	Click or tap to enter a date.
Accepted by:	Enter name Enter position	Date:	Click or tap to enter a date.
Accepted by:	Enter name Enter position	Date:	Click or tap to enter a date.

Review

Date	Name	Position title	Signature
Click or tap to enter a date.	Enter the name of the person	Enter their position title	
Click or tap to enter a date.	Enter the name of the person	Enter their position title	

Table of contents

Part 1 – General information

Introduction

The Internal Review Tool (IRT) is designed to assist entities and facilities when undertaking internal reviews for the purposes of the SSBA Standards. The IRT is not a mandatory document and other methods or documents may be used to undertake reviews.

The SSBA Standards require that entities conduct an internal review at planned intervals of no longer than 6 monthly for Tier 1 and 12 monthly for Tier 2 SSBAs, to determine that operations carried out by the entity comply with both the requirements of the SSBA Regulatory Scheme and the entity's SSBA policies. Records of internal review must be kept and these records should include the findings of the review, any non-compliance or improvement opportunities identified and any actions that result from the findings.

The IRT is designed to assist in determining if the entity and facility meets the requirements of the SSBA Standards, and can be used as a record that an internal review has taken place.

Corresponding SSBA Standards

This version of the IRT has been aligned with the requirements from the *SSBA Standards* – dated March 2013.

Using this document

Requirements under the SSBA Standards

Each Part of the IRT (except Part 1) covers the associated Part of the SSBA Standards[1]. The IRT headings include the Standards clause number that is being covered by the questions. Please note that letters included after a question number (for example Q2.3a) are simply in place to designate that the clause is covered in several questions and do not relate to lettered sub clauses or paragraph numbering within the Standards.

Questions in each section cover the mandatory requirements of the SSBA Standards and the majority have a yes/no answer. A space for comments is included so that the entity can explain how these requirements are being met.

[1] Please note that *Part 1 – Scope and Definitions* of the SSBA Standards is not covered by this document.

It should be noted that while the questions are based on the standards requirements they are not a word-for-word match. For the full details of the requirements, the latest version of the Standards should be consulted.

The IRT also includes sections on reporting to the SSBA Regulatory Scheme, compliance with internal policy and sections to record any non-compliances, corrective actions or improvement opportunities. A section on available resources is included at the end of the document.

Further consideration questions

In addition to the questions that address the mandatory requirements under the SSBA Standards, the IRT includes a number of questions, found at the end of the section, that are based on the suggestions made under the commentary of the SSBA Standards or are recommendations about best practice. These are not mandatory requirements but may be used to enhance the security of the SSBAs in your facility.

Terms and definitions

Below are a number of terms commonly used throughout this document.

Term	Definition
Handling	Includes (a) receiving, holding, using and storing biological agents; and (b) any operation incidental to, or arising out of, any of those operations.
Australian CDC	Australian Centre for Disease Control (CDC)
List of Security-sensitive Biological Agents	The list established under the NHS Act. The list designates which biological agents are regulated.
NHS Act	The *National Health Security Act 2007*.
NHS check	A National Health Security check (background check).
NHS Regulations	The National Health Security Regulations 2018.
Record	A document that states the results achieved or provides evidence of activities performed.

Term	Definition
Reportable event	An event that must be reported to the Australian CDC under section 48(1) of the NHS Act. Reportable events include: • Initial registration • Change of administrative details (including changes to Responsible Officer details) • Starting to handle a new SSBA • Changes to the purpose for handling an SSBA • Incident reports • Transfer In and Transfer Out of SSBAs • Disposal • Suspected SSBAs • Temporary Handling
Sensitive information	Means any of the following: (a) an entity's storage records for the security-sensitive biological agent handled at the facility; (b) an entity's risk assessment plan for the security-sensitive biological agent handled at the facility; (c) an entity's risk management plan for the security-sensitive biological agent handled at the facility; (d) any other information that the entity identifies as being sensitive information under clause 5.3 of the SSBA Standards because it could compromise the security of the security-sensitive biological agent handled at the facility.
SSBA	A security sensitive biological agent.
SSBA Standards	The Security Sensitive Biological Agent (SSBA) Standards determined by the Director General of the Australian Government Centre for Disease Control under the NHS Act.
Standard operating procedure (SOP)	A set of written instructions that documents a routine or repetitive activity to be followed by an entity or facility.

Term	Definition
Suspected SSBA	A biological agent suspected, on the basis of testing in a laboratory, to be a security sensitive biological agent.
Temporary handling	The handling of a known SSBA by an entity that is not registered to handle that particular SSBA. Handling may be for a period of up to seven working days after which an entity must either dispose of or register to handle the SSBA.
Tier 1 SSBAs	Means an agent that is referred to as a Tier 1 agent on the List of Security-sensitive Biological Agents. Tier 1 agents have the highest security concerns.
Tier 2 SSBAs	Means an agent that is referred to as a Tier 2 agent on the List of Security-sensitive Biological Agents. Tier 2 agents have a high security concern.

Part 2 – Risk and incident management

The objective of Part 2 of the SSBA Standards is to ensure that all known biosecurity risks in relation to the SSBAs handled by the entity are identified and managed through risk assessment and risk management plans prior to the commencement of SSBA related work.

2.2 Risk assessment

2.2.1 Timing and scope

2.2.1	Is the scope, nature and timing of the risk assessment proactive rather than reactive?	Yes ☐ No ☐
Comments:		

2.2.2 Hazards/risk identification

2.2.2a	Are the hazards/risks associated with the handling of the SSBAs identified and documented?	Yes ☐ No ☐
Comments:		

2.2.2b	Are the following risks/hazards identified and documented for inclusion in the risk assessment:	
i.	Determination of the potential for/ possible causes of an incident?	Yes ☐ No ☐
ii.	Human behavioural risk?	Yes ☐ No ☐
iii.	Periods of reduced staff availability?	Yes ☐ No ☐
iv.	Identification of potential emergency situations involving SSBAs?	Yes ☐ No ☐
Comments:		

2.2.3 Risk assessment process

2.2.3a	Has the entity undertaken a risk assessment for the SSBAs and the facilities in which they are handled?	Yes ☐ No ☐
Comments:		
2.2.3b	At a minimum, does the risk assessment include:	
i.	Communication and consultation plans with internal and external stakeholders?	Yes ☐ No ☐
ii.	Internal, external and security risk context?	Yes ☐ No ☐
iii.	The risks identified under the hazard/risk identification clause	Yes ☐ No ☐
iv.	Analysis of the risks and the effectiveness of existing controls, including:	Yes ☐ No ☐
a.	If action is needed to prevent incidents?	Yes ☐ No ☐
b.	Effectiveness of physical security controls?	Yes ☐ No ☐
c.	Effectiveness of the procedures for decontamination/inactivation?	Yes ☐ No ☐
d.	Identification of those responsible for devising, implementing and testing control measures?	Yes ☐ No ☐
e.	If further controls are needed to reduce the risk	Yes ☐ No ☐
Comments:		

2.2.3c	If the facility is handling Tier 1 SSBAs, has a vulnerability analysis been undertaken?	Yes ☐ No ☐ N/A (No Tier 1) ☐
Comments:		

2.3 Risk management plan

2.3a	Has a risk management plan been developed, documented and implemented following the risk assessment?	Yes ☐ No ☐
Comments:		
2.3b	At a minimum, does the risk management plan include:	
	i. Treatment for the risks identified in the risk assessment?	Yes ☐ No ☐
	ii. Plans for monitoring and review of the risk management process?	Yes ☐ No ☐
Comments:		
2.3c	Have the risk management plans been effectively communicated to	
	i. All personnel handling SSBAs or sensitive information relating to SSBAs?	Yes ☐ No ☐
	ii. Others as relevant (e.g. security personnel, maintenance contractors)?	Yes ☐ No ☐
Comments:		

2.3d	Have Standard Operating Procedures (SOPs) for the secure handling of SSBAs been:	
	i. Developed?	Yes ☐ No ☐
	ii. Documented?	Yes ☐ No ☐
	iii. Implemented?	Yes ☐ No ☐
Comments:		

2.4 Incident management

2.4a	Has the entity established, documented and maintained procedures to define, report, record and analyse incidents involving SSBAs? *Note: Incidents can include any non-compliance with the NHS Act, NHS Regulations and the SSBA Standards.*	Yes ☐ No ☐
Comments:		

2.4b	Are records of the nature of the incident and any subsequent action taken maintained?	Yes ☐ No ☐
Comments:		

2.4c	Does analysis of the incidents include:	
	i. Determining the cause/s of the incident?	Yes ☐ No ☐
	ii. Evaluating the need for corrective action to ensure incidents do not re-occur?	Yes ☐ No ☐
	iii. Determining and implementing any action needed?	Yes ☐ No ☐
	iv. Recording the results of action taken?	Yes ☐ No ☐

	v. Review of the effectiveness of the action taken?	Yes ☐ No ☐
Comments:		

2.4d	Does the entity have in place processes to encourage learning from incidents involving SSBAs?	Yes ☐ No ☐
Comments:		

2.5 Review

2.5	Are all risk assessment and risk management plans reviewed at least:	
	i. Every 12 months for risks involving Tier 1 SSBAs (or more frequently if required)?	Yes ☐ No ☐ N/A(No Tier 1) ☐
	ii. Every 2 years for risks involving Tier 2 SSBAs (or more frequently if required)?	Yes ☐ No ☐ N/A(No Tier 2) ☐
	iii. Or more frequently as required	Yes ☐ No ☐
Comments:		

Part 2 – Further considerations

The questions below are based on the suggestions made under the commentary of the SSBA Standards or are best practice recommendations. These are not mandatory requirements but may be used to enhance the security of the SSBAs in your facility.

P2a	Have the roles and responsibilities of personnel who perform and verify work affecting risk management been defined and documented?	Yes ☐ No ☐
Comments:		

P2b	Does reactive risk assessment take place following an occurrence of an identified risk or following the occurrence of a new risk not previously considered? Comments:	Yes ☐ No ☐
P2c	Was professional advice sought when developing the risk assessment or risk management plan? Comments:	Yes ☐ No ☐
P2d	Are there procedures to clearly communicate to all personnel what constitutes an incident? Comments:	Yes ☐ No ☐
P2e	Is the review plan included in the risk assessment and risk management document? Comments:	Yes ☐ No ☐
P2f	Does the review plan include space for documentation of outcomes and sign off once the review is completed? Comments:	Yes ☐ No ☐

Part 3 – Personnel

The objective of Part 3 of the SSBA Standards is to have personnel management systems in place to implement and manage the security of SSBAs and related sensitive information.

3.2 Responsible Officers

3.2a	Has the entity documented top management's appointment of a Responsible Officer and a Deputy Responsible Officer? Comments:	Yes ☐ No ☐
3.2b	Do the duties of the Responsible Officer include:	
i.	Overseeing the SSBA management system?	Yes ☐ No ☐
ii.	Reporting to top management on the performance of the entity's SSBA management system and any need for improvement?	Yes ☐ No ☐
iii.	Overseeing internal review, audit and reporting measures?	Yes ☐ No ☐
iv.	Verifying, in conjunction with other personnel, that all known SSBA risks have been addressed?	Yes ☐ No ☐
v.	Advising or participating in the reporting, investigation and follow-up of incidents?	Yes ☐ No ☐
vi.	Where appropriate, referring incidents to top management/ SSBA management committees?	Yes ☐ No ☐
vii.	Ensuring all work relating to SSBAs is conducted in accordance with established policies, SOPs, the NHS Act, NHS regulations and the SSBA Standards?	Yes ☐ No ☐
viii.	Advising top management as to whether staff levels, facilities and equipment are sufficient?	Yes ☐ No ☐

ix.	Maintaining lists of authorised and approved persons?	Yes ☐ No ☐

Comments:

3.2c Do the lists of authorised and approved persons include:

i.	The period for which the person is authorised or approved?	Yes ☐ No ☐
ii.	The review date of the authorisation or approval?	Yes ☐ No ☐
iii.	What the person is authorised or approved for?	Yes ☐ No ☐

Note: A person may be authorised or approved to handle SSBAs, access a facility where SSBAs are handled or access sensitive information relating to SSBAs or any combination of the above.

Comments:

3.2d Are the Responsible Officer and Deputy Responsible Officer authorised persons? Yes ☐ No ☐

Comments:

3.3 Authorised persons

3.3a	Have all persons been made authorised persons if they: • handle SSBAs; • access a facility where SSBAs are handled; or • access sensitive information related to SSBAs? *Note: an entity may choose to authorise a person to do all of the above or may limit the authorisation to any combination of the above.* *A person may not need to be an authorised person if they are to be escorted or supervised in the facility or when handling SSBAs or sensitive information. These persons may instead be made approved persons if they meet the criteria for an approved person under the SSBA Standards. In addition to this, persons who meet certain criteria for handling sensitive information under Part 5 of the SSBA Standards may also not be required to be an authorised or approved person when handling that information.* Comments:	Yes ☐ No ☐
3.3c	Are all authorised person statuses limited to the entity in which the status was conferred? Comments:	Yes ☐ No ☐
3.3d	Are all students who handle SSBAs either authorised or approved persons? Comments:	Yes ☐ No ☐

3.3f	Has the entity revoked (or have a process for revoking) the authorisation of any person who no longer has a need to handle SSBAs, access a facility that handles SSBAs or access sensitive information related to SSBAs?	Yes ☐ No ☐

Comments:

3.3.1 Authorisation of a person

3.3.1	Have all authorised persons:		
	i.	Been trained in the requirements of the NHS Act, NHS Regulations and SSBA Standards as relevant to their authorisation?	Yes ☐ No ☐
	ii.	Provided to the entity a signed and dated record of the training above?	Yes ☐ No ☐
	iii.	Not been excluded from handling SSBAs by the entity nor have been directed not to handle SSBAs by the Director General of the Australian CDC?	Yes ☐ No ☐
	iv.	Undergone an identity check as outlined in the SSBA Standards?	Yes ☐ No ☐
	v.	Been verified as 18 years old or over?	Yes ☐ No ☐
	vi.	Undergone an NHS check if required to do so by the SSBA Standards and have a ‘eligible’ or ‘qualified’ status?	Yes ☐ No ☐

Comments:

3.3.2 Authorisation of a person with an NHS check

3.3.2	If a person has undergone an NHS check and	N/A ☐ (go to Q3.3f)
	i. Received a result of 'eligible' – is the person authorised for up to two years?	Yes ☐ No ☐
	ii. Received a result of 'qualified' – is the person authorised for a period of up to 12 months only?	Yes ☐ No ☐
	iii. Received a result of 'non-eligible' – has the entity not authorised that person?	Yes ☐ No ☐
Comments:		

3.4 Approved persons

3.4a	Does the entity have in place documented processes to ensure that contractors, visitors, suppliers, students and other such persons do not compromise the facility's SSBA security?	Yes ☐ No ☐
Comments:		
3.4b	Do these processes include policies and procedures for the approval of persons who need to:	
	i. Handle SSBAs;	Yes ☐ No ☐
	ii. Access a facility where SSBAs are handled; or	Yes ☐ No ☐
	iii. Access sensitive information related to SSBAs.	Yes ☐ No ☐
	Note: an entity may choose to approve a person to do all of the above or may limit the approval to any combination of the above.	

Comments:		
3.4c	If the facility handles Tier 1 SSBAs, are all approved persons escorted by an authorised person at all times? *Note: Escorted is taken to mean that the approved person should remain within line of sight of the authorised person escorting them while the person is within the secure perimeter or handing sensitive information.* Comments:	N/A ☐ (no Tier 1 – go to Q3.4d) Yes ☐ No ☐
3.4d	If the facility handles Tier 2 SSBAs, are all approved persons supervised by an authorised person at all times? Is the degree of supervision of and the responsibility for an approved person by an authorised person determined by risk assessment? Comments:	N/A ☐ (no Tier 2) Yes ☐ No ☐ Yes ☐ No ☐
3.4e	Has the entity revoked (or have a process for revoking) the approval of any person who no longer has a need to handle SSBAs, access a facility that handles SSBAs or access sensitive information related to SSBAs? Comments:	Yes ☐ No ☐

3.5 Identity check

3.5a	Was an identity check conducted on all persons prior to the person being authorised? Comments:	Yes ☐ No ☐
3.5b	If an NHS check was conducted, was the identity check completed on each person prior to the submission of the persons NHS check application to AusCheck? Comments:	N/A ☐ (no NHS check) Yes ☐ No ☐
3.5c	Did the documentation for all identity checks include: i. Evidence of commencement of identity in Australia? ii. Linkage between the identity and the person? iii. Evidence of operation in the community? iv. Evidence of residential address? *Note: For more information about what can be used in each of these categories – see Table 1 under Clause 3.5 of the SSBA Standards.* Comments:	 Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐
3.5d	Does the entity keep a record of which documents were provided? *Note: this may be a record of the type of document provided; it does not have to be a copy of the document itself.* Comments:	Yes ☐ No ☐

3.6 National Health Security (NHS) checks

3.6a	Does the facility undertake National Health Security checks (either mandatory checks for Tier 1 SSBAs or voluntary checks for Tier 2 SSBAs)? *Note: NHS checks are not required for persons who hold a national security clearance of Negative Vetting Level 1, Negative Vetting Level 2 or Positive Vetting.* *NHS checks are recommended for personnel handling Tier 2 SSBAs but are not mandatory. If they are undertaken, please answer the questions under 3.6.* Comments:	Yes ☐ No ☐ (if No, go to Q3.7a)
3.6b	Has the entity applied to AusCheck for an NHS check of all persons who are authorised to handle Tier 1 SSBAs, access facilities where Tier 1 SSBAs are handled or access sensitive information relating to Tier 1 SSBAs? *Note: some persons may be able to access sensitive information for Tier 1 SSBAs without an NHS Check if they meet certain requirements under Part 5 of the SSBA Standards.* Comments:	Yes ☐ No ☐
3.6c	At the time of application for an NHS check, was a recent photograph, taken by the entity, supplied to AusCheck? Comments:	Yes ☐ No ☐

3.6d	Did the entity take into account the results of the NHS check as part of the assessment for eligibility to become an authorised person? Comments:	Yes ☐ No ☐
3.6e	Has the entity ensured that NHS checks are conducted at intervals of no more than two years to maintain eligibility? *Note: NHS checks may be required more frequently (see clause 3.3 of the SSBA Standards)* Comments:	Yes ☐ No ☐
3.6f	Does the entity have in place policies and procedures to ensure that a person who has undergone an NHS check and who changes their name: i. Informs the entity of the change within 30 days? ii. Provides appropriate documentation to support the change? Comments:	 Yes ☐ No ☐ Yes ☐ No ☐
3.6g	Are any changes reported to the entity under 3.6f subsequently reported to AusCheck within two business days of the entity being notified of the change? Comments:	Yes ☐ No ☐

3.6.1 Transfer of NHS checks between entities

3.6.1a	Does the entity accept NHS check results obtained by another entity?	Yes ☐ No ☐ (if no – go to Q3.6.2a)
Comments:		

3.6.1b	If you answered yes to Q3.6.1a, does the entity:	
	i. Obtain the person's consent to request those results from AusCheck?	Yes ☐ No ☐
	ii. Contact AusCheck to verify the result?	Yes ☐ No ☐
Comments:		

3.6.2 Reporting new convictions

3.6.2a	Does the entity have documented policies and procedures in place to require that:	
	i. A person who has undergone an NHS check must report any new convictions to the entity within two business days of being informed of the conviction?	Yes ☐ No ☐
	ii. The entity reports this information to AusCheck within two business days from being informed of the conviction?	Yes ☐ No ☐
	Note: New convictions that must be reported are only those against the disqualifying offences as listed in Appendix 1 of the SSBA Standards.	
Comments:		

3.6.2b	If a new conviction is reported to the entity, does the entity suspend that person's authorised status pending a new NHS check?	Yes ☐ No ☐
Comments:		

3.7 Provisional authorisation

3.7a	Has the entity used the provisional authorisation clause at clause 3.7 of the SSBA Standards?	Yes ☐ No ☐ (if No, go to Q3.8a)
Comments:		
3.7b	Was the Provisional Authorisation clause used to authorise a person only if:	
	i. The person was to undergo an NHS check?	Yes ☐ No ☐
	ii. The requirements of clause 3.3.1 (a) to (e) of the SSBA Standards were met?	Yes ☐ No ☐
	iii. The relevant facility had no other authorised persons in place?	Yes ☐ No ☐
Comments:		
3.7c	If the entity/facility was not previously registered with AusCheck, were the NHS checks commenced within four weeks of notification by AusCheck that submission of applications could begin?	Yes ☐ No ☐
Comments:		

3.7d	If a person had a provisional authorisation, did it cease upon receipt of their NHS check results?	Yes ☐ No ☐
Comments:		

3.8 Recruitment

3.8a	Is the identity, qualifications and experience of all persons recruited to handle SSBAs assessed as part of the recruitment process?	Yes ☐ No ☐
Comments:		

3.9 Training and competency

3.9a	Has the entity ensured that all personnel who have responsibilities or perform tasks that may have an impact on SSBAs:	
	i. Have the appropriate education, training and experience?	Yes ☐ No ☐
	ii. Are provided with adequate and up-to-date information pertaining to the entity's identified SSBA risks?	Yes ☐ No ☐
Comments:		

3.9b	Has the entity ensured that requirements and procedures for SSBA-related training are established, documented, implemented and maintained?	Yes ☐ No ☐
Comments:		

3.9c	Do the minimum training requirements include:		
	i.	Defining SSBA related training needs?	Yes ☐ No ☐
	ii.	Provision of required SSBA training?	Yes ☐ No ☐
	iii.	Determination of the effectiveness of SSBA training?	Yes ☐ No ☐
	iv.	Provision of SSBA refresher training?	Yes ☐ No ☐
	v.	Restriction on staff to ensure they do not perform tasks for which they are not trained?	Yes ☐ No ☐
	vi.	Records management including the maintenance of adequate records?	Yes ☐ No ☐

Comments:

3.9.1 Training for authorised persons

3.9.1a	For all **authorised** persons, has the SSBA training at a minimum included:		
	i.	An overview of the NHS Act, NHS Regulations and why the SSBA Regulatory Scheme is in place?	Yes ☐ No ☐
	ii.	Reporting requirements?	Yes ☐ No ☐
	iii.	Records management?	Yes ☐ No ☐

Comments:

3.9.1b	For all persons who **handle SSBAs**, does the SSBA training at a minimum include the requirements of the NHS Act, NHS Regulations and all parts of the SSBA Standards?	Yes ☐ No ☐

Comments:

3.9.1c For all persons who **access the facility** where SSBAs are handled, does the SSBA training at a minimum include:

i. Physical security? Yes ☐ No ☐

ii. Risk management? Yes ☐ No ☐

iii. Information security? Yes ☐ No ☐

iv. Personnel security? Yes ☐ No ☐

v. Management system requirements? Yes ☐ No ☐

Comments:

3.9.1d For all persons who **access sensitive information** relating to SSBAs, does the SSBA training at a minimum include:

i. Risk management? Yes ☐ No ☐

ii. Information security? Yes ☐ No ☐

iii. Personnel security? Yes ☐ No ☐

iv. Management system requirements? Yes ☐ No ☐

Comments:

3.9.1e Does all training include:

i. How the SSBA Standards are implemented at each facility? Yes ☐ No ☐

ii. Specific training in the requirements of the entity and facility in relation to SSBAs? Yes ☐ No ☐

Note: requirements of the facility may include the policies and procedures specific to the facility for handling SSBAs and sensitive information, the requirements for escorting/supervising approved persons etc

Comments:	
3.9.1f Does training for personnel handling Tier 1 SSBAs include personal security awareness? Comments:	Yes ☐ No ☐ N/A ☐ (no Tier 1)
3.9.1g Does the entity impose any other training requirements on each category of authorisation? Comments:	Yes ☐ No ☐

3.9.2 Competency levels

3.9i Has the entity defined competency levels and maintain records verifying that personnel have attained and continue to demonstrate those levels of competency? Comments:	Yes ☐ No ☐
3.9j Are competencies of personnel reviewed:	
i. At least annually for facilities handling Tier 1 SSBAs?	Yes ☐ No ☐ N/A ☐ (no Tier 1)
ii. At least every two years for facilities handling Tier 2 SSBAs?	Yes ☐ No ☐ N/A ☐ (no Tier 2)
iii. In response to changes in risk assessment, risk management, SOPs or following an incident?	Yes ☐ No ☐

Comments:

3.10 Behavioural factors

3.10a	Has the entity established and implemented measures to address risks associated with human behaviour, including reliability, of persons who handle SSBAs, access a facility where SSBAs are handled or access sensitive information relating to SSBAs?	Yes ☐ No ☐
	Comments:	
3.10b	Are these measures documented as part of the risk assessment and risk management process and evidence of their application recorded?	Yes ☐ No ☐
	Comments:	

3.11 Exclusion

3.11a	Has the entity established, documented and put into place measures for the removal and exclusion of personnel from the facility (on a temporary, or if appropriate, permanent basis) where deemed necessary or following a direction not to handle SSBAs from the Australian CDC)?	Yes ☐ No ☐
	Comments:	

3.11b	Do exclusion measures include:		
	i.	Prompt removal of access to the facility?	Yes ☐ No ☐
	ii.	Prompt removal of access to any SSBAs held in linked storage units?	Yes ☐ No ☐
	iii.	Prompt removal of access to sensitive information?	Yes ☐ No ☐
	iv.	Suspension or revocation of a person's authorised or approved status?	Yes ☐ No ☐
	v.	Immediate physical removal if deemed necessary?	Yes ☐ No ☐

Comments:

Part 3 – Further considerations

The questions below are based on the suggestions made under the commentary of the SSBA Standards or are best practice recommendations. These are not mandatory requirements but may be used to enhance the security of the SSBAs in your facility.

P3a	When deciding if a person is to be re-authorised following a new NHS check does the entity require the person to undergo refresher training before re-authorisation?	Yes ☐ No ☐ N/A ☐ (no NHS check)

Comments:

P3b	If a person's authorised status is suspended due to a new conviction being reported, does the entity grant the person an approved status until the results of a new NHS check are received?	Yes ☐ No ☐ N/A ☐ (no NHS check)

Comments:

P3c	When determining the degree of supervision for an approved person, does the risk assessment take into account factors such as the set up of the facility, the SSBA involved, the role of the approved person and the results of an NHS check (if undertaken)?	Yes ☐ No ☐
Comments:		
P3d	Do supervision plans include how supervision is handled during an emergency situation (e.g. if security personnel require access to a facility after working hours and an authorised person is not available)?	Yes ☐ No ☐
Comments:		
P3e	Are identity checks undertaken for approved persons?	Yes ☐ No ☐
Comments:		
P3f	Does training for SSBAs include raising awareness of general security issues associated with SSBAs, including the relevance of human behavioural factors?	Yes ☐ No ☐
Comments:		
P3g	Does training for SSBAs include, if appropriate, hazard identification, risk assessment and management and vulnerability analysis?	Yes ☐ No ☐
Comments:		
P3h	Does the entity have in place mechanisms to ensure that relevant and timely information is available regarding SSBAs?	Yes ☐ No ☐
Comments:		

P3i	Does the entity promote awareness of the potential risks (internal and external) associated with unauthorised access to SSBAs?	Yes ☐ No ☐
Comments:		
P3j	Does the entity have a program of briefing authorised persons on risks associated with their role and how to handle and report situations of concern?	Yes ☐ No ☐
Comments:		
P3k	Does the entity use the On-line Training Facility provided by the Australian CDC as a training tool?	Yes ☐ No ☐
Comments:		

Part 4 – Physical security

The objective of Part 4 is to have in place physical security measures, based on requirements identified in the risk assessment and risk management plan, to minimise the risk of unauthorised access to SSBAs.

4.2 Perimeter

4.2a	Does the facility have a clearly defined perimeter that encloses the secure area where SSBAs are handled? Comments:	Yes ☐ No ☐
4.2b	Are the external walls that form part of the secure area of solid construction and physically sound? Comments:	Yes ☐ No ☐
4.2c	Are the external doors: i. Self closing? ii. Suitably protected against unauthorised access with control mechanisms? Comments:	 Yes ☐ No ☐ Yes ☐ No ☐
4.2d	Are doors that form part of the secure perimeter locked when the facility is unattended? Comments:	Yes ☐ No ☐

4.2e	Are the windows of the secure perimeter non-opening and sealed at all times?	Yes ☐ No ☐
Comments:		
4.2f	Is unauthorised recording, photography or filming prohibited within the secure area?	Yes ☐ No ☐
Comments:		

4.2.1 Stand-alone facilities

4.2.1a	Does the facility have any stand-alone facilities? *Note: Mobile laboratories, such as forensic laboratories are not subjected to the requirements for stand-alone facilities.*	Yes ☐ No ☐ (if No, go to Q4.3a)
Comments:		
4.2.1b	Does the stand-alone facility meet the following requirements:	
	i. Has a back to base alarm system?	Yes ☐ No ☐
	ii. Is fixed in place an not easily transportable?	Yes ☐ No ☐
	iii. Have barriers to prevent vehicles from approaching the facility?	Yes ☐ No ☐
	iv. Have good external lighting?	Yes ☐ No ☐
	v. Regular inspections conducted of outer walls to detect tampering?	Yes ☐ No ☐
	vi. Outcomes of regular inspections are documented?	Yes ☐ No ☐
Comments:		

4.3 Physical access controls

4.3a	Is access to secure areas containing SSBAs restricted to authorised and approved persons? Comments:	Yes ☐ No ☐
4.3b	Is at least one form of access control on the secure perimeter? Comments:	Yes ☐ No ☐
4.3c	If the facility is handling Tier 1 SSBAs: • Is there an additional form of access control? Comments:	N/A ☐ (go to Q4.3d) Yes ☐ No ☐
4.3d	Are there measures in place to prevent tail gaiting? Comments:	Yes ☐ No ☐
4.3e	Does the access control ensure that the details of all persons (including identification of the person and date and time of access) are recorded for all persons: i. Entering the secure perimeter? ii. Accessing the secondary access control to the Tier 1 SSBA? iii. For areas holding Tier 1 SSBAs – the time of exit of the person is also recorded? Comments:	 Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐

4.3f	Are access records maintained for a minimum of:	
	i. 5 years for facilities holding Tier 1 SSBAs?	Yes ☐ No ☐ N/A ☐ (no Tier 1)
	ii. 2 years for facilities holding Tier 2 SSBAs?	Yes ☐ No ☐ N/A ☐ (no Tier 2)
Comments:		
4.3g	Are access control systems tested at least every:	
	i. 6 months for facilities holding Tier 1 SSBAs?	Yes ☐ No ☐ N/A ☐ (no Tier 1)
	ii. 12 months for facilities holding Tier 2 SSBAs?	Yes ☐ No ☐ N/A ☐ (no Tier 2)
Comments:		
4.3h	Are any losses of access cards, keys or other items used to access the secure areas reported immediately to the Responsible Officer once the loss is known?	Yes ☐ No ☐
Comments:		
4.3i	Are there measures in place to ensure that the lost items in 4.3h are not used?	Yes ☐ No ☐
Comments:		

4.3j	Are any reports of loss or theft and the actions taken documented?	Yes ☐ No ☐
Comments:		
4.3k	If a person no longer requires access to the secure area, does the Responsible Officer ensure that access is removed?	Yes ☐ No ☐
Comments:		

Part 4 – Further considerations

The questions below are based on the suggestions made under the commentary of the SSBA Standards or are best practice recommendations. These are not mandatory requirements but may be used to enhance the security of the SSBAs in your facility.

P4a	Is there a marked floor plan of the secure area?	Yes ☐ No ☐
	If yes, is the floor plan kept securely?	Yes ☐ No ☐
Comments:		
P4b	Is there a staffed reception area as part of the controls regarding access to the secure area?	Yes ☐ No ☐
Comments:		
P4c	Are any intruder detection systems installed to Commonwealth, State or Territory standards and regularly tested to cover all external doors and accessible windows?	Yes ☐ No ☐
Comments:		

P4d	Are unoccupied areas alarmed:	
	i. At all times?	Yes ☐ No ☐
	ii. After hours only?	Yes ☐ No ☐
	iii. Other? (please note how in comments)	Yes ☐ No ☐
Comments:		
P4e	Is there video monitoring?	Yes ☐ No ☐
Comments:		
P4f	Are exit controls:	
	i. Able to be overridden in case of emergency?	Yes ☐ No ☐
	ii. An alarm generated to indicate unauthorised exit?	Yes ☐ No ☐
Comments:		
P4g	Is any alarm generation subject to an incident report and investigation?	Yes ☐ No ☐
Comments:		
P4h	Does risk assessment determine how access is handled in an emergency?	Yes ☐ No ☐
Comments:		

P4i Are any policies or procedures regarding emergency access:

i. Documented? Yes ☐ No ☐

ii. Communicated to relevant personnel, including contractors such as security guards? Yes ☐ No ☐

Comments:

Part 4A – Storage

The objective of Part 4A is to ensure that SSBAs are stored securely to reduce the risk of unauthorised access.

4A.2 Working cultures

4A.2a	Does the entity have in place documented policies and procedures to track the creation of working cultures from SSBAs held in long term storage?	Yes ☐ No ☐
Comments:		
4A.2b	Does the entity have in place documented policies and procedures to track and control the distribution of working cultures of SSBAs?	Yes ☐ No ☐
Comments:		

4A.3 SSBA inventory

4A.3a	Has the entity established and maintained an accurate and up-to-date inventory of any SSBA held in storage?	Yes ☐ No ☐
Comments:		
4A.3b	Does the inventory identify and document which SSBAs are held and the location of each storage container?	Yes ☐ No ☐
Comments:		
4A.3c	Has the entity ensured that there are measures in place to minimise quantities of SSBAs stored?	Yes ☐ No ☐

Comments:

4A.3.1 Audit of Inventory

4A.3.1	Audits of the inventory:		
	i.	Are conducted at predetermined intervals?	Yes ☐ No ☐
	ii.	The intervals determined through risk assessment?	Yes ☐ No ☐
	iii.	Audits are at a level and frequency that materials can be accounted for?	Yes ☐ No ☐
	iv.	Results of the audit are documented?	Yes ☐ No ☐

Comments:

4A.4 Storage of Tier 1 SSBAs

4A.4	Are Tier 1 SSBAs only stored within the secure perimeter of a registered facility?	Yes ☐ No ☐ N/A ☐ (no Tier 1)

Comments:

4A.5 Storage of Tier 2 SSBAs

4A.5a	Does the entity store Tier 2 SSBAs:		N/A ☐ (no Tier 2)
	i.	Only within the secure perimeter of a registered facility?	Yes ☐ No ☐ (if Yes, go to Q 4A.6)
	ii.	Only in a linked storage unit?	Yes ☐ No ☐

iii.	In both the facility and a linked storage unit?	Yes ☐ No ☐

Comments:

4A.5b	Is the only handling of the SSBA within the linked storage unit either storage or preparation for storage?	Yes ☐ No ☐

Comments:

4A.5c Is the linked storage unit:

i.	Within the same building (preferably the same floor) as the registered facility?	Yes ☐ No ☐
ii.	Included as part of the facility registration?	Yes ☐ No ☐
iii.	Included in the risk assessment and risk management plans?	Yes ☐ No ☐
iv.	Fixed in place or non-transportable?	Yes ☐ No ☐

Comments:

4A.5.1 Access to a linked storage unit

4A.5.1a Is access to the SSBA within the linked storage unit:

i.	Restricted to Authorised or Approved persons?	Yes ☐ No ☐
ii.	Recorded?	Yes ☐ No ☐

Comments:

4A.5.1b	Do access records include:	
	i. Identification of the person?	Yes ☐ No
	ii. Date and time of access?	Yes ☐ No
	iii. A record if any of the SSBA was removed?	Yes ☐ No
	Comments:	

4A.5.1c	Are access records maintained for a minimum of 5 years for a Tier 1 SSBA or 2 years for a Tier 2 SSBA?	Yes ☐ No ☐
	Comments:	

4A.5.1d	Are any losses of access cards, keys or other items used to access the linked storage unit reported immediately to the Responsible Officer once the loss is known?	Yes ☐ No ☐
	Comments:	

4A.5.1e	Are there measures in place to ensure that the lost items in 4A.5.1d are not used?	Yes ☐ No ☐
	Comments:	

4A.5.1f	Are reports of loss or theft of access cards, keys etc. and any actions taken documented?	Yes ☐ No ☐
	Comments:	

4A.5.1g	If a person no longer requires access, does the Responsible Officer ensure that access to the area is removed?	Yes ☐ No ☐
Comments:		

4A.5.2 Transport from and to a linked storage unit

4A.5.2a	Is transport between the linked storage unit and the registered facility undertaken as required under clause 6.4 of the SSBA Standards?	Yes ☐ No ☐
Comments:		
4A.5.2b	Is transport between the linked storage unit and the registered facility recorded? *Note: this type of transport does not need to be reported to the Australian CDC but a record of the transport must be made available on request.*	Yes ☐ No ☐
Comments:		

4A.6 Record keeping

4A.6a	Has the entity ensured that records relating to the storage of SSBAs, including inventory records, are:	
i.	Current?	Yes ☐ No ☐
ii.	Complete?	Yes ☐ No ☐
iii.	Stored securely?	Yes ☐ No ☐
iv.	Adequately backed up?	Yes ☐ No ☐

Comments:

4A.6b	Are the records kept in accordance with clause 5.2 of the SSBA Standards?	Yes ☐ No ☐

Comments:

Part 4A – Further considerations

The questions below are based on the suggestions made under the commentary of the SSBA Standards or are best practice recommendations. These are not mandatory requirements but may be used to enhance the security of the SSBAs in your facility.

P4Aa	Are any additional audits of inventory carried out outside of the predetermined intervals? *Note: additional audits might be undertaken when there are changes such as transfer of inventories to new areas, changes in personnel responsible for inventory or changes in the risk assessment or threat levels.*	Yes ☐ No ☐

Comments:

Part 5 – Information management

The objective of Part 5 is to ensure that information, including sensitive information, relating to the security of SSBAs is current, complete and stored securely.

5.2 Record keeping

5.2a	Does the entity maintain records of all activities related to the SSBA Standards including records of:		
	i.	Receipt of SSBAs?	Yes ☐ No ☐
	ii.	Holding of SSBAs?	Yes ☐ No ☐
	iii.	Transport of SSBAs?	Yes ☐ No ☐
	iv.	Disposal of SSBAs?	Yes ☐ No ☐
	v.	Decontamination and inactivation	Yes ☐ No ☐
	vi.	Policies and procedures	Yes ☐ No ☐
	vii.	Internal and external reviews?	Yes ☐ No ☐
	viii.	Inspections?	Yes ☐ No ☐
	ix.	Incident investigations?	Yes ☐ No ☐
	x.	Risk assessment and risk management plans	Yes ☐ No ☐

Comments:

5.2b	Are records kept for a minimum of:	
	i. 5 years for Tier 1 SSBAs?	Yes ☐ No ☐ N/A ☐ (no Tier 1)
	ii. 2 years for Tier 2 SSBAs? (unless otherwise specified in the SSBA Standards)	Yes ☐ No ☐ N/A ☐ (no Tier 2)
Comments:		

5.2c	Has the entity developed and documented policies regarding records in accordance with the SSBA Standards relation to:	
	i. Access	Yes ☐ No ☐
	ii. Retention	Yes ☐ No ☐
	iii. Destruction (including timeframes)?	Yes ☐ No ☐
Comments:		

5.3 Information security

5.3a	Has the entity identified and documented sensitive information relating to SSBAs? *Note: Documentation may be part of a larger document such as the risk assessment and risk management plan.*	Yes ☐ No ☐
Comments:		

5.3b	Is there a review and approval process to control access to sensitive information? Comments:	Yes ☐ No ☐
5.3c	Is access to sensitive information limited to those who have a need to know and who have been permitted access by the responsible officer? Comments:	Yes ☐ No ☐
5.3d	Is access to sensitive information controlled? *Note: Controls for sensitive information should cover all persons who can access the information (e.g. facility personnel, IT personnel, SSBA Committee members)* Comments:	Yes ☐ No ☐
5.3e	Are access permissions reviewed at least: i. Every 6 months for facilities handling Tier 1 SSBAs? ii. Every 12 months for facilities handling only Tier 2 agents? Are the outcomes of the review documented? Comments:	 Yes ☐ No ☐ N/A ☐ (no Tier 1) Yes ☐ No ☐ N/A ☐ (no Tier 2) Yes ☐ No ☐

5.3f	Is Tier 1 sensitive information:	
	i. Stored in a secure system?	Yes ☐ No ☐ N/A ☐ (no Tier 1)
	ii. Securely backed up at regular intervals?	Yes ☐ No ☐
Comments:		

5.3.1 Provision of sensitive information to other regulatory agencies

5.3.1a	Does the entity/facility have a need to provide sensitive information to other regulatory authorities? *Note: Documents may need to be provided to another regulatory authority as evidence of compliance with another regulatory scheme. A list of who this information may be provided to is available under clause 5.3.1 of the SSBA Standards.*	Yes ☐ No ☐ (if no, go to Q5.4a)
Comments:		
5.3.1b	Is sensitive information only supplied under the following conditions? i. The regulatory authority has a need to know the information for their regulatory purposes. ii. The regulatory authority is able to hold the information at the PROTECTED security level or higher. iii. Measures are in place to limit the amount of sensitive information released.	Yes ☐ No ☐
Comments:		

5.3.1c	Does the entity document what is supplied to the regulatory authority?	Yes ☐ No ☐

Comments:

5.4 Disposal of records

5.4a	Has the entity ensured that there are documented polices and procedures in place, consistent with the requirements of the SSBA Standards, for the disposal of records?	Yes ☐ No ☐

Comments:

Part 5 – Further considerations

The questions below are based on the suggestions made under the commentary of the SSBA Standards or are best practice recommendations. These are not mandatory requirements but may be used to enhance the security of the SSBAs in your facility.

P5a	Has the entity considered information from research, diagnosis and other purposes (that is not identified as sensitive information) in regards to what is released, who may access such information and how it may impact on the security of SSBAs? *Note: Issues such as 'dual use' should be considered when releasing information. Dual use biological research is legitimate research which involves information or technology which can be used for both peaceful and malevolent purposes such as to threaten public health or other aspects of national security.*	Yes ☐ No ☐

Comments:

P5b	Before providing sensitive information to other regulatory authorities, does the entity determine if: • The information can be deidentified instead? • The sensitive information can be removed before provision of documentation? • Can the regulatory officer simply sight the information rather than take copies for their records? Comments:	Yes ☐ No ☐
P5c	Does sensitive information supplied electronically have measures in place to prevent copying? Do any hard copies supplied have clear markings to indicate the document is a copy and the documents security classification? Comments:	Yes ☐ No ☐ Yes ☐ No ☐
P5d	At a minimum, do the procedures addressing information security consider:	
	i. Secure storage of sensitive records including electronic records and electronic signatures?	Yes ☐ No ☐
	ii. Computer security (e.g. firewalls)?	Yes ☐ No ☐
	iii. Strict policies regarding the on-site security of equipment as well as equipment entering or leaving the facility?	Yes ☐ No ☐
	iv. Destruction of unwanted paper files and complete erasure of electronic files?	Yes ☐ No ☐
	v. Security measures and procedures?	Yes ☐ No ☐

vi. Adequate backup strategies for electronic data? Yes ☐ No ☐

Comments:

Part 6 – Transport

The objective of Part 6 is the have policies and procedures in place for the secure movement of SSBAs.

6.2 Transport

6.2a	If the entity is sending SSBAs, does it ensure that the sending facility:		N/A ☐ (entity does not send SSBAs)
	i.	Has documented policies and procedures in place to ensure compliance with Commonwealth, state and territory legislation governing the transport of biological agents?	Yes ☐ No ☐
	ii.	Ensure that the receiving facility will accept the agent?	Yes ☐ No ☐
	iii.	Keep a record of that acceptance?	Yes ☐ No ☐
	iv.	Notifies the receiving facility of the shipment details at the time of shipment?	Yes ☐ No ☐
	v.	If the shipment is lost in transit–immediately informs the Australian CDC and state/territory police once aware of the loss?	Yes ☐ No ☐
	vi.	If the shipment is reported unsuccessful by the receiving facility–immediately informs the Australian CDC and state/territory police once aware of the unsuccessful transfer?	Yes ☐ No ☐
Comments:			

6.2b	If the entity is receiving SSBAs, does it ensure the receiving facility:	N/A ☐ (entity does not receive SSBAs)
	i. Verifies that the transfer was successful; including that: a. the complete shipment was received b. there was no tampering evident on the shipping container?	Yes ☐ No ☐
	ii. Notifies the sending facility of the receipt of the shipment and if the transfer has been successful?	Yes ☐ No ☐
	iii. If a shipment fails to arrive at the expected time–contacts the transport agent and sending facility to seek confirmation of the shipments location and expected time of delivery?	Yes ☐ No ☐
	iv. If the shipment is lost in transit–immediately informs the sending facility, the Australian CDC and State/Territory police once aware of the loss?	Yes ☐ No ☐

Comments:

6.3 Transport security

6.3a	Is a transport agent contracted to transport SSBAs?	Yes ☐ No ☐ (if No go to Q 6.4a)

Comments:

6.3b	Has the entity ensured that the transport agent has a documented security plan and systems in place to track the shipment at all stages of transport?	Yes ☐ No ☐
Comments:		
6.3c	At a minimum does the transport security plan comprise of:	
i.	Specific allocation of security responsibilities to competent and qualified persons with the appropriate authorities?	Yes ☐ No ☐
ii.	Compliance with Commonwealth, State and Territory legislation governing the transport of biological agents?	Yes ☐ No ☐
iii.	Assessment and coverage of security risks, including inter-modal transport, temporary transit storage, handling and distribution?	Yes ☐ No ☐
iv.	Clear statements of measures and resources that are used to reduce security risks?	Yes ☐ No ☐
v.	Up to date procedures for responding to and dealing with security threats, non-compliance with security protocols or security incidents?	Yes ☐ No ☐
vi.	Procedures for the evaluation and testing of security plans and procedures for periodic review and update of the plans?	Yes ☐ No ☐
vii.	Measures to ensure the security of information relating to transport of SSBAs?	Yes ☐ No ☐
viii.	Measures to ensure that the distribution of transport information is as limited as possible?	Yes ☐ No ☐

Note: Due to security or confidentiality requirements, a transport company might not supply their transport security plan to an entity. The entity can supply the transport company with a copy of the requirements of clause 6.3 of the SSBA Standards and request that the company confirms, in writing, that the transport plan meets these requirements.

Comments:

6.4 Transport of SSBAs by authorised persons

6.4a	Is transport that is not undertaken by a transport agent always undertaken by an authorised person?	Yes ☐ No ☐
	Comments:	
6.4b	Are all transport movements by authorised persons:	
	i. Reported to the Responsible Officer?	Yes ☐ No ☐
	ii. Recorded?	Yes ☐ No ☐
	Comments:	
6.4c	If material is being transferred within a building, is the material triple packed unless documented in the risk assessment that double packaging can be used?	Yes ☐ No ☐
	Comments:	
6.4d	If material is being transported outside of the building, is the movement consistent with the requirements of Commonwealth, state and territory legislation governing the transport of biological agents?	Yes ☐ No ☐

Comments:

6.5 Transport of SSBAs from reception areas to a registered facility

6.5a	Does the facility transport SSBAs from a designated reception area to a registered facility?	Yes ☐ No ☐ (if No, go to Part 6 further considerations)
	Comments:	
6.5b	Is transport of the SSBA from the reception area to the registered facility undertaken under the following conditions:	
	i. *Transport* occurs within a single building only?	Yes ☐ No ☐
	ii. Transport occurs only between the reception area and the registered *facility*?	Yes ☐ No ☐
	iii. The person handling the SSBA at the reception area does so only for the purposes of receiving the package and transporting to the registered facility?	Yes ☐ No ☐
	iv. *The* SSBA is delivered to an authorised person at the registered facility?	Yes ☐ No ☐
	v. The *transport* is covered by a documented policy and is included in the risk assessment?	Yes ☐ No ☐
	vi. All *movements* of the SSBA from the reception area to the registered facility are recorded?	Yes ☐ No ☐
	vii. An up to date list is kept of all persons who are permitted to undertake these transports?	Yes ☐ No ☐

Note: While a record of the movements must be kept, the entity is not required to report these movements to the Australian CDC, but must make the records available on request.

Comments:

6.5c The person undertaking the transport:

i.	Is 18 years or older?	Yes ☐ No ☐
ii.	Has undergone an identity check?	Yes ☐ No ☐
iii.	Has not been excluded from handling SSBAs by the entity?	Yes ☐ No ☐
iv.	Has not been directed not to handle SSBAS by the Australian CDC?	Yes ☐ No ☐
v.	Has basic training in the requirements of the SSBA Standards and the internal requirements for this type of transport?	Yes ☐ No ☐

Are records of the training listed above kept? Yes ☐ No ☐

Comments:

Part 6 – Further considerations

The questions below are based on the suggestions made under the commentary of the SSBA Standards or are best practice recommendations. These are not mandatory requirements but may be used to enhance the security of the SSBAs in your facility.

P6a Are the Responsible Officers from both the sending and receiving facilities involved when transport agreements are made? Yes ☐ No ☐

Comments:

P6b	Does the entity have in place guidance about what it considers to be tampering? *For example – does the entity require the use of tamper proof packaging to indicate tampering during transport?* Comments:	Yes ☐ No ☐
P6c	Does the entity use Security Construction and Equipment Committee (SCEC) approved couriers where possible? Comments:	Yes ☐ No ☐

Part 7 – Inactivation and decontamination

The objective of Part 7 is to ensure that all types of contaminated and potentially contaminated materials, including those that may result from an emergency, are identified and documented, and that effective procedures are in place to ensure decontamination of materials or inactivation of the SSBA prior to destruction or further use.

7.2 Procedures

7.2a	Is risk assessment an integral part of the process to identify and develop effective decontamination and inactivation regimes?	Yes ☐ No ☐
	Comments:	
7.2b	Are effective procedures and detailed protocols documented and in place to decontaminate or inactivate the SSBA or waste products potentially contaminated with the SSBA, prior to destruction or further use?	Yes ☐ No ☐
	Comments:	
7.2c	Do the protocols include:	
	i. Validation data on inactivation procedures?	Yes ☐ No ☐
	ii. Quality assurance to ensure inactivation has been correctly performed?	Yes ☐ No ☐
	Comments:	

7.3 Waste management

7.3a	Has the entity ensured that its waste management procedures are such that no SSBA leaves the control of the entity without being inactivated or destroyed, unless it is being transported to another entity or facility for further handling or destruction? Comments:	Yes ☐ No ☐
7.3b	Has a risk assessment been undertaken to determine the procedures that are required to ensure that safe destruction of the waste is carried out? Comments:	Yes ☐ No ☐
7.3c	Is a contracted waste disposal company used for waste disposal? Comments:	Yes ☐ No ☐ (if No, go to Q7.4a)
7.3d	Does the entity have in place mechanisms to ensure that waste taken by an external contractor is: i. Kept secure until it is picked up? ii. The entity is notified when the waste is destroyed? Comments:	 Yes ☐ No ☐ Yes ☐ No ☐

7.4 Record keeping

7.4a	Was risk assessment an integral part of the process to identify records of decontamination/deactivation and validation data that must be kept?	Yes ☐ No ☐
	Comments:	
7.4b	Are records of decontamination/deactivation kept for at least 5 years for Tier 1 SSBAs or 2 years for Tier 2 SSBAs?	Yes ☐ No ☐
	Comments:	

Part 7 – Further considerations

The questions below are based on the suggestions made under the commentary of the SSBA Standards or are best practice recommendations. These are not mandatory requirements but may be used to enhance the security of the SSBAs in your facility.

P7a	Do the validation procedures take into account issues such as:		
	i.	Nature of the material being treated?	Yes ☐ No ☐
	ii.	Contact times and material compatibility issues?	Yes ☐ No ☐
	iii.	Potential health hazards?	Yes ☐ No ☐
	iv.	Need to maintain the required level of active compound including deterioration over time?	Yes ☐ No ☐
	Comments:		

P7b	When planning and conducting decontamination activities did the entity consider:	
	i. Ensuring all disinfectants contain sufficient compound to address the working conditions under which they will be applied and that such concentrations are maintained throughout the process?	Yes ☐ No ☐
	ii. Implementing monitoring measures to ensure the methods have been effective?	Yes ☐ No ☐
	iii. Ensuring adequate methods and resources are available to deal with routine work, spills or other incidents during handling and transport inside and outside the facility?	Yes ☐ No ☐
	iv. Implementing programs to ensure the amount of contaminated waste is minimised?	Yes ☐ No ☐
Comments:		
P7c	When using a waste contractor to dispose of materials, is waste moved from secure areas to collection points as close as possible to the time for pick up?	Yes ☐ No ☐ NA ☐ (No waste contractor used)
Comments:		
P7d	Does the entity have an arrangement with the waste contractor that waste is destroyed as soon as possible after arrival at the treatment facility?	Yes ☐ No ☐ NA ☐ (No waste contractor used)
Comments:		

P7e	If waste is destroyed by the entity, is:	NA ☐ (Not destroyed by entity)
	i. Transport carried out by authorised persons?	Yes ☐ No ☐
	ii. Validated destruction processes carried out by authorised persons?	Yes ☐ No ☐
	iii. The waste destroyed as soon as possible after arrival in the waste destruction area?	Yes ☐ No ☐
Comments:		

P7f	Were the following elements considered for the waste management policy:	
	i. Ensuring a program is in place to minimise waste production?	Yes ☐ No ☐
	ii. Ensuring effective waste audit trails are in place and documented?	Yes ☐ No ☐
	iii. Provision of adequate facilities and procedures for storage of waste?	Yes ☐ No ☐
	iv. Ensuring appropriate packaging material is used to contain waste and maintain its integrity during storage and transport?	Yes ☐ No ☐
Comments:		

Part 8 – SSBA management system requirements

The objective of Part 8 is to establish a systematic approach to the management of the biosecurity of SSBAs that takes into account risk and incident management, personnel management, physical security, information management, transport and inactivation and decontamination in accordance with the requirements of the SSBA Standards, NHS Act and NHS Regulations.

8.2 Policy

8.2a	Has the entity developed, documented, authorised and implemented policies concerning the management of SSBAs? Comments:	Yes ☐ No ☐
8.2b	Does the policy clearly state the overall SSBA management objectives and commitment to improving biosecurity management? Comments:	Yes ☐ No ☐
8.2c	Was the policy in place prior to the handling of SSBAs? Comments:	Yes ☐ No ☐
8.2d	Does the entity continually assess and improve the effectiveness of the SSBA management system through use of:	
	i. Policies?	Yes ☐ No ☐
	ii. Objectives?	Yes ☐ No ☐
	iii. Procedures?	Yes ☐ No ☐
	iv. Self review programs?	Yes ☐ No ☐
	v. Analysis of data?	Yes ☐ No ☐

vi.	Risk assessment and management?	Yes ☐ No ☐
vii.	Corrective and preventative actions?	Yes ☐ No ☐
viii.	Management review?	Yes ☐ No ☐

Comments:

8.2e	Has the entity ensured that relevant information relating to the SSBA Management system and activities is communicated to personnel and other relevant parties? *Note: Other relevant parties may include persons such as cleaners, security staff and maintenance staff. Entities should consider what information is required as part of their duties.*	Yes ☐ No ☐

Comments:

8.3 Roles, responsibilities and authorities

8.3.1 Top management

8.3.1a	Does top management:		
i.	Take ultimate responsibility for the development and implementation of the entity's SSBA management system and policy?	Yes ☐ No ☐
ii.	Ensure the availability of resources to establish, implement, maintain and improve the SSBA management system?	Yes ☐ No ☐
iii.	Appoint and empower a Responsible Officer and Deputy Responsible Officer for the SSBA Regulatory Scheme and puts in place processes to ensure the continuity of the staffing and effectiveness of the positions?	Yes ☐ No ☐

iv.	Ensure that all SSBA related activities conducted in the facility are authorised, defined and reviewed at least annually?	Yes ☐ No ☐
v.	Ensure that criteria and processes are established for work that requires prior approval?	Yes ☐ No ☐
vi.	Ensure that actions are taken promptly in regards to any non-compliance of the management system with the SSBA Standards, NHS Act or NHS Regulations?	Yes ☐ No ☐
vii.	Deal with any identified instances of the entity's non compliance with the SSBA Standards, NHS Act or NHS Regulations?	Yes ☐ No ☐
viii.	Ensure verification of any actions taken to deal with instances of non-compliance and documents such actions?	Yes ☐ No ☐
ix.	Establish controls and put in place documented procedures for monitoring the effectiveness of the controls being applied to reduce or eliminate the hazards identified in risk assessment processes?	Yes ☐ No ☐
x.	Ensure that staff levels, facilities and equipment are sufficient to effectively carry out work involving SSBAs in accordance with technical protocols, approved policies and SOPs?	Yes ☐ No ☐
xi.	Ensure all requirements for reporting to the Australian CDC are met?	Yes ☐ No ☐

Comments:

8.3.2 SSBA Management Committee

8.3.2a Has the entity either:	
i. Established an SSBA Management Committee?	Yes ☐ No ☐
or	
ii. Assigned the tasks required of such a committee to an existing committee?	Yes ☐ No ☐
Comments:	
8.3.2b Does this committee act as a review group for SSBA risks and issues?	Yes ☐ No ☐
Comments:	
8.3.2c Does the committee report to top management?	Yes ☐ No ☐
Comments:	
8.3.2d Does the committee:	
i. Have documented terms of reference?	Yes ☐ No ☐
ii. Include a representative cross section of expertise, appropriate to the nature and scale of activities undertaken?	Yes ☐ No ☐
iii. Include the Responsible Officer and Deputy Responsible Officer?	Yes ☐ No ☐
iv. Meet at defined and appropriate frequency and when otherwise required?	Yes ☐ No ☐
Comments:	

8.3.2e	Do the functions of the committee include:		
	i.	Contributing to the development to the entity's SSBA policies and procedures?	Yes ☐ No ☐
	ii.	Reviewing and approving protocols and risk assessments for work involving SSBAs?	Yes ☐ No ☐
	iii.	Reviewing information relating to significant incidents, non-compliance, data trends, associated local/entity action and associated communication needs?	Yes ☐ No ☐
	iv.	Ensuring biosecurity issues are formally recorded; actions allocated, tracked and closed out effectively?	Yes ☐ No ☐
	v.	Reviewing internal inspection reports?	Yes ☐ No ☐
Comments:			

8.4 Checking and corrective action

8.4.1 Performance management and analysis of data

8.4.1a	Has the entity ensured that data is identified, collected, stored and analysed to:		
	i.	Assess the suitability and effectiveness of the SSBA management system?	Yes ☐ No ☐
	ii.	Evaluate where continual improvement of the system can be made?	Yes ☐ No ☐
Comments:			

8.4.1b	Are all outcomes of the performance management process documented?	Yes ☐ No ☐
Comments:		

8.4.2 Records, documentation and data control

8.4.2a	Has the entity ensured that records, documents and data to provide evidence of compliance with the SSBA Standards are:	
	i. Established?	Yes ☐ No ☐
	ii. Controlled?	Yes ☐ No ☐
	iii. Maintained?	Yes ☐ No ☐
Comments:		

8.4.2b	Have such records, documents and data remained, in alignment with the information management requirements of Part 5 of the SSBA Standards:?	
	i. Legible?	Yes ☐ No ☐
	ii. Readily identifiable?	Yes ☐ No ☐
	iii. Retrievable	Yes ☐ No ☐
Comments:		

8.4.2c	Has the entity documented its record retention policies and ensured that they are implemented?	Yes ☐ No ☐
Comments:		

8.4.3 Internal review

8.4.3a	Has the entity ensured that a program of internal review is conducted? Comments:	Yes ☐ No ☐
8.4.3b	Are the internal reviews conducted at planned intervals of no longer than:	
	i. 6 monthly for Tier 1 SSBAs?	Yes ☐ No ☐ N/A ☐ (no Tier 1)
	ii. Annually for Tier 2 SSBAs?	Yes ☐ No ☐ N/A ☐ (no Tier 2)
	Note: Reviews should determine that operations carried out by the entity comply with the requirements of the SSBA Standards, NHS Act, NHS Regulations and the entity's policies. Comments:	
8.4.3c	Are records maintained:	
	i. Of the findings of the review?	Yes ☐ No ☐
	ii. Of the actions taken to close out any non-compliances?	Yes ☐ No ☐
	iii. Of the actions taken for any improvement opportunities?	Yes ☐ No ☐
	iv. In accordance with Part 5 of the SSBA Standards?	Yes ☐ No ☐
	Comments:	

8.4.4 Control of non-compliance and corrective action

8.4.4a	Has the entity ensured that any areas of non-compliance with the SSBA Standards, NHS Act, NHS Regulations or SSBA management system are identified and managed? Comments:	Yes ☐ No ☐
8.4.4b	Has the entity ensured that action is taken to eliminate the causes of non-compliance to prevent recurrence? *Note: Non-compliances may be identified during regular reviews by the entity, during day to day operations of the entity or through the SSBA Inspection Program.* Comments:	Yes ☐ No ☐
8.4.4c	Are records of the nature of the non-compliance and any subsequent action taken maintained in accordance with Part 5 of the SSBA Standards? Comments:	Yes ☐ No ☐

8.4.5 Preventive action

8.4.5a	Has the entity ensured that action is taken to identify, through risk management or other sources, potential non-compliance to eliminate its causes and to prevent occurrence or recurrence? Comments:	Yes ☐ No ☐

8.4.5b	Is preventive action appropriate to the effects of the potential non-compliance?	Yes ☐ No ☐
Comments:		

Part 8 – Further considerations

The questions below are based on the suggestions made under the commentary of the SSBA Standards or are best practice recommendations. These are not mandatory requirements but may be used to enhance the security of the SSBAs in your facility.

P8a	Has the management system approach been built on the concept of continual improvement through a cycle of planning, implementing, reviewing and improving the processes and action that the entity undertakes to meet goals?	Yes ☐ No ☐
Comments:		
P8b	Does the SSBA management system policy specifically include provisions covering:	
i.	Meeting the reporting requirements under the NHS Act and NHS Regulations?	Yes ☐ No ☐
ii.	Justification of all legitimate uses of the SSBA?	Yes ☐ No ☐
iii.	Documentation and communication of roles, responsibilities and authorities for SSBA management within the facility?	Yes ☐ No ☐
iv.	Effectively informing personnel and other relevant parties of individual obligations?	Yes ☐ No ☐
v.	Requirements for all projects/work involving SSBAs to be assessed for risks and mitigation strategies before work is approved to commence?	Yes ☐ No ☐
vi.	Reviews of the management system following an incident?	Yes ☐ No ☐

Comments:		
P8c	Does the review of the management system include assessment and evaluation of opportunities for improvement and the need for changes to the system, procedures, policies and objectives? Comments:	Yes ☐ No ☐
P8d	Is the policy appropriate to the nature and scale of risks associated with the facility and associated activities? Comments:	Yes ☐ No ☐
P8e	Does the policy commit to: i. Complying with legal requirements for handling SSBAs? ii. Reducing the level of biosecurity risk to an acceptable level? iii. Ensuring that the need for effective SSBA management takes precedence over non 'health and safety' operational requirements? iv. Continually improving SSBA management performance? Comments:	 Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐ Yes ☐ No ☐
P8f	When communicating information regarding SSBA policies to relevant parties, does the entity consider if the person has a need-to-know the information as part of their activities? Comments:	Yes ☐ No ☐

P8g	When assigning roles and responsibilities under the SSBA management system, are potential conflicts of interest taken into account? Comments:	Yes ☐ No ☐
P8h	Is determination of staffing levels, equipment and facilities done in consultation with the Responsible Officer? Comments:	Yes ☐ No ☐
P8g	Does documentation of SSBA related activities include the nature of the activities authorised to be conducted and their definitions? Comments:	Yes ☐ No ☐
P8h	Are all activities routinely associated with the work program specified and supported by formal SOPs? Comments:	Yes ☐ No ☐
P8i	Are any changes to these activities subjected to a formal change management process, including approval by management and communication to and training of staff? Comments:	Yes ☐ No ☐
P8j	Are controls monitored by:	
	i. Regular reviews?	Yes ☐ No ☐
	ii. Using corrective action reporting processes?	Yes ☐ No ☐
	iii. Investigation of accidents and incidents?	Yes ☐ No ☐

	iv.	Improving controls and their implementation?	Yes ☐ No ☐
	v.	Ensuring adequate resources are provided?	Yes ☐ No ☐

Comments:

P8k Do the terms of reference include:

	i.	A short statement of the purpose of the committee?	Yes ☐ No ☐
	ii.	Defined roles and functions of the committee and how objectives are achieved?	Yes ☐ No ☐
	iii.	Who is part of the committee as a member, observer or other?	Yes ☐ No ☐
	iv.	Details regarding quorums – is there one, what is the number and what happens if this is not reached?	Yes ☐ No ☐
	v.	Defined deliverables?	Yes ☐ No ☐
	vi.	Defined timeframes such as meeting frequency, reporting, review and set task timeframes?	Yes ☐ No ☐
	vii.	Details on what is to be reported and to whom?	Yes ☐ No ☐
	viii.	Details on the evaluations undertaken by the committee on the role and function or other terms of reference	Yes ☐ No ☐
	ix.	Details on how the effectiveness of the committee will be evaluated?	Yes ☐ No ☐

Comments:

P8l For the performance management analysis are:

	i.	Data sets generated as a consequence of monitoring, measuring, reviews and other sources considered?	Yes ☐ No ☐

	ii.	Analyses conducted every 2 years or more often if justified by the risks and scope of operations?	Yes ☐ No ☐
	iii.	Results of the analysis considered as part of the management review?	Yes ☐ No ☐
Comments:			
P8m	Are documents identified and controlled on the basis of the nature of the work and the need for record keeping?		Yes ☐ No ☐
Comments:			
P8n	Do controlled documents include:		
	i.	Risk assessments, SOPs and safety manuals?	Yes ☐ No ☐
	ii.	Job hazard analyses and charts of authority?	Yes ☐ No ☐
	iii.	Audit and inspection checklists	Yes ☐ No ☐
	iv.	Laboratory SSBA manuals, authorisations and other security documents?	Yes ☐ No ☐
	v.	Training records?	Yes ☐ No ☐
Comments:			
P8o	Are records kept of internal reviews and actions taken?		Yes ☐ No ☐
Comments:			

P8p	Are reviews undertaken by a team?	Yes ☐ No ☐
Comments:		
P8q	Has a procedure been established to define requirements for:	
i.	Reviewing all non-compliances?	Yes ☐ No ☐
ii.	Determining the causes of non-compliances?	Yes ☐ No ☐
iii.	Evaluating the need for action to ensure that non-compliances do not occur or recur?	Yes ☐ No ☐
iv.	Determining and implementing the actions needed?	Yes ☐ No ☐
v.	Recording results of actions taken?	Yes ☐ No ☐
vi.	Reviewing corrective actions taken?	Yes ☐ No ☐
Comments:		

Part 9 – Handling biological agents suspected of being SSBAs

The objective of Part 9 is to ensure that biological agents suspected, on the basis of laboratory testing, of being an SSBA are handled securely prior to receiving the outcomes of confirmatory testing or destruction.

Does the facility handle biological agents suspected of being SSBAs?	Yes ☐ No ☐ (if No, go to Internal Policies)

9.2 Access and storage

9.2a	Once a reasonable suspicion is formed that the biological agent is an SSBA, is access restricted to persons that have a need to handle? Comments:	Yes ☐ No ☐
9.2b	Does the entity store suspected SSBAs securely to ensure that access is restricted to those who have a need to handle the SSBA? Comments:	Yes ☐ No ☐
9.2c	Does the entity maintain a record of who accessed the suspected SSBA, including the identity of the person and time and date of access? Comments:	Yes ☐ No ☐

9.3 Transport

9.3.1 Transport requirements for a sending facility

9.3.1	If the entity is sending suspected SSBAs, does it ensure that the sending facility:		
	i.	Has documented policies and procedures in place to ensure compliance with Commonwealth, state and territory legislation governing the transport of biological agents?	Yes ☐ No ☐
	ii.	Ensures that the confirmatory testing facility will accept the agent	Yes ☐ No ☐
	iii.	Keeps a record of that acceptance?	Yes ☐ No ☐
	iv.	Notifies the receiving facility of the shipment details at the time of shipment?	Yes ☐ No ☐
	v.	If the shipment is lost in transit – immediately informs the Australian CDC once aware of the loss?	Yes ☐ No ☐
	vi.	If the shipment is reported unsuccessful by the receiving facility – immediately informs the Australian CDC once aware of the unsuccessful transfer?	Yes ☐ No ☐

Comments:

9.3.2 Transport requirements for a receiving facility

9.3.2	If the entity is receiving suspected SSBAs, does it ensure the receiving facility:		
	i.	Verifies that the transfer was successful; including that:	Yes ☐ No ☐
		a. the complete shipment was received?	

	b. there was no tampering evident on the shipping container?	Yes ☐ No ☐
ii.	Notifies the sending facility of the receipt of the shipment and if the transfer has been successful?	Yes ☐ No ☐
iii.	If a shipment fails to arrive at the expected time – contacts the transport agent and sending facility to seek confirmation of the shipment's location and expected time of delivery?	Yes ☐ No ☐

Comments:

9.4 Destruction

9.4a	If destruction has taken place <u>prior</u> to confirmatory testing, has the entity ensured that the processes for destruction are such that no suspected SSBA leaves the entity without being destroyed or inactivated, unless it is being transported for confirmatory testing or destruction?	Yes ☐ No ☐ N/A ☐ (no destruction prior to confirmatory testing)
9.4b	If destruction has taken place <u>following</u> receipt of confirmatory testing results, has the entity ensured that the processes for destruction are such that no confirmed SSBA leaves the entity without being destroyed or inactivated, unless it is being transported in its entirety for the purposes of disposal under Division 4A of the NHS Act? *Note: disposal means either complete destruction/deactivation or transfer of all of the SSBA.*	Yes ☐ No ☐ N/A ☐ (no destruction after to confirmatory testing)

Comments:

9.5 Waste disposal

9.5	Does the entity have validated procedures for the decontamination of waste materials potentially contaminated with suspected SSBA?	Yes ☐ No ☐
Comments:		

9.6 Record keeping

9.6a	Once a reasonable suspicion is formed that the biological agent is an SSBA, are records maintained of all activities relating to the requirements of Part 9 of the SSBA Standards?	Yes ☐ No ☐
Comments:		
9.6b	Unless otherwise specified in the SSBA Standards, are records relating to suspected SSBAs maintained for a minimum of	
	i. 12 months for agents suspected to be Tier 1 SSBAs?	Yes ☐ No ☐ N/A ☐ (no Tier 1)
	ii. 6 months for agents suspected to be Tier 2 SSBAs?	Yes ☐ No ☐ N/A ☐ (no Tier 2)
	Note: records do not need to be kept if confirmatory testing shows that the agent is not an SSBA.	
Comments:		

Part 9 – Further considerations

The questions below are based on the suggestions made under the commentary of the SSBA Standards or are best practice recommendations. These are not mandatory requirements but may be used to enhance the security of the SSBAs in your facility.

P9a	Does the entity have policies in place to contact a receiving facility within two business days of the expected date of arrival of a sample if receipt has not been confirmed?	Yes ☐ No ☐
	Comments:	
P9b	Does the entity have data available to demonstrate that the methodology used for destruction is capable of inactivating the agent under the specific conditions encountered in the facility?	Yes ☐ No ☐
	Comments:	
P9c	Does decontamination take place as soon as possible after the waste is generated?	Yes ☐ No ☐
	Comments:	
P9d	If waste is disposed of outside the facility through a waste disposal company, does the entity:	
	i. Move waste to the disposal point as close as practical to the time of pickup?	Yes ☐ No ☐
	ii. Have arrangements to ensure destruction will take place as soon as possible after the waste arrives at the treatment facility?	Yes ☐ No ☐
	Comments:	

Part 9A – Handling following a positive confirmatory test result

The objective of Part 9A is to ensure that biological agents previously suspected and subsequently confirmed as an SSBA are handled securely prior to disposal.

9A.2 Access and storage

9A.2a	Does the entity ensure that access to the SSBA is restricted to persons that have a need to handle? Comments:	Yes ☐ No ☐
9A.2b	Does the entity store SSBAs securely to ensure physical access is restricted to those who have a need to handle? Comments:	Yes ☐ No ☐
9A.2c	Does the entity maintain a record of who accesses the SSBA, including the identity of the person and time and date of access? Comments:	Yes ☐ No ☐

9A.3 Transport

9A3.1 Transport requirements for a sending facility

9A.3.1	If the entity is sending confirmed SSBAs, does it ensure that the sending facility:	
	i. Has documented policies and procedures in place to ensure compliance with Commonwealth, state and territory legislation governing the transport of biological agents?	Yes ☐ No ☐
	ii. Ensures that the receiving facility will accept the agent	Yes ☐ No ☐

iii.	Keeps a record of that acceptance?	Yes ☐ No ☐
iv.	Notifies the receiving facility of the shipment details at the time of shipment?	Yes ☐ No ☐
v.	If the shipment is lost in transit – immediately informs the Australian CDC and state/territory police once aware of the loss?	Yes ☐ No ☐
vi.	If the shipment is reported unsuccessful by the receiving facility–immediately informs the Australian CDC and state/territory police once aware of the unsuccessful transfer?	Yes ☐ No ☐

Comments:

9A.3.2 Transport for a receiving facility

9A.3.2 If the entity is receiving confirmed SSBAs, does it ensure the receiving facility:

i.	Verifies that the transfer was successful; including that:	Yes ☐ No ☐
a.	the complete shipment was received?	
b.	there was no tampering evident on the shipping container?	Yes ☐ No ☐
ii.	Notifies the sending facility of the receipt of the shipment and if the transfer has been successful?	Yes ☐ No ☐
iii.	If a shipment fails to arrive at the expected time – contacts the transport agent and sending facility to seek confirmation of the shipment's location and expected time of delivery?	Yes ☐ No ☐

Comments:

9A.4 Destruction

9A.4a	Has the entity ensured that the processes for destruction are such that no SSBA leaves the entity without being destroyed or inactivated, unless it is being transported in its entirety for the purposes of disposal? *Note: disposal means either complete destruction/deactivation or transfer of all of the SSBA.*	Yes ☐ No ☐ N/A ☐ (SSBA not destroyed)

Comments:

9A.5 Waste disposal

9A.5a	Does the entity have validated procedures for the decontamination of waste materials potentially contaminated with the SSBA?	Yes ☐ No ☐

Comments:

9A.6 Record keeping

9A.6a	Does the entity maintain a record of all activities relating to the requirements of the SSBA Standards that relate to Part 9A of the SSBA Standards?	Yes ☐ No ☐

Comments:

9A.6b	Are records relating to SSBAs maintained for a minimum of	
	i. 12 months for Tier 1 SSBAs?	Yes ☐ No ☐ N/A ☐ (no Tier 1)
	ii. 6 months for Tier 2 SSBAs?	Yes ☐ No ☐ N/A ☐ (no Tier 2)
Comments:		

Part 9A – Further considerations

The questions below are based on the suggestions made under the commentary of the SSBA Standards or are best practice recommendations. These are not mandatory requirements but may be used to enhance the security of the SSBAs in your facility.

P9Aa	Does the entity send confirmed SSBAs to a reference laboratory for further genetic typing?	Yes ☐ No ☐
Comments:		

Part 10 – Non-registered entity handling an SSBA on a temporary basis

The objective of Part 10 is to ensure that SSBAs are handled temporarily are handled securely prior to disposal.

10.2 Access and storage

10.2a	Does the entity ensure that access to the SSBA is restricted to persons that have a need to handle? Comments:	Yes ☐ No ☐
10.2b	Does the entity store SSBAs securely to ensure physical access is restricted to those who have a need to handle? Comments:	Yes ☐ No ☐
10.2c	Does the entity maintain a record of who accesses the SSBA, including the identity of the person and time and date of access? Comments:	Yes ☐ No ☐

10.3 Transport

10.3.1 Transport requirements for a sending facility

10.3.1	If the entity is sending confirmed SSBAs, does it ensure that the sending facility:	
	i. Has documented policies and procedures in place to ensure compliance with Commonwealth, state and territory legislation governing the transport of biological agents?	Yes ☐ No ☐
	ii. Ensures that the receiving facility will accept the agent	Yes ☐ No ☐

iii.	Keeps a record of that acceptance?	Yes ☐ No ☐
iv.	Notifies the receiving facility of the shipment details at the time of shipment?	Yes ☐ No ☐
v.	If the shipment is lost in transit – immediately informs the Australian CDC and state/territory police once aware of the loss?	Yes ☐ No ☐
vi.	If the shipment is reported unsuccessful by the receiving facility–immediately informs the Australian CDC and state/territory police once aware of the unsuccessful transfer?	Yes ☐ No ☐

Comments:

10.3.2 Transport for a receiving facility

10.3.2 If the entity is receiving confirmed SSBAs, does it ensure the receiving facility:

i.	Verifies that the transfer was successful; including that:	Yes ☐ No ☐
a.	the complete shipment was received?	
b.	there was no tampering evident on the shipping container?	Yes ☐ No ☐
ii.	Notifies the sending facility of the receipt of the shipment and if the transfer has been successful?	Yes ☐ No ☐
iii.	If a shipment fails to arrive at the expected time – contacts the transport agent and sending facility to seek confirmation of the shipment's location and expected time of delivery?	Yes ☐ No ☐

Comments:

10.4 Destruction

10.4a	Has the entity ensured that the processes for destruction are such that no SSBA leaves the entity without being destroyed or inactivated, unless it is being transported in its entirety for the purposes of disposal? *Note: disposal means either complete destruction/deactivation or transfer of all of the SSBA.*	Yes ☐ No ☐ N/A ☐ (SSBA not destroyed)

Comments:

10.5 Waste disposal

10.5a	Does the entity have validated procedures for the decontamination of waste materials potentially contaminated with the SSBA?	Yes ☐ No ☐

Comments:

10.6 Record keeping

10.6a	Does the entity maintain a record of all activities relating to the requirements of the SSBA Standards that relate to Part 10 of the SSBA Standards?	Yes ☐ No ☐

Comments:

10.6b	Are records relating to SSBAs handled under Part 10 of the SSBA Standards maintained for a minimum of	
	i. 12 months for Tier 1 SSBAs?	Yes ☐ No ☐ N/A ☐ (no Tier 1)
	ii. 6 months for Tier 2 SSBAs?	Yes ☐ No ☐ N/A ☐ (no Tier 2)
Comments:		

Part 10 – Further considerations

The questions below are based on the suggestions made under the commentary of the SSBA Standards or are best practice recommendations. These are not mandatory requirements but may be used to enhance the security of the SSBAs in your facility.

P10a	Does the entity send confirmed SSBAs to a reference laboratory for further genetic typing?	Yes ☐ No ☐
Comments:		

Part 11 – Registered entity handling an SSBA on a temporary basis

The objective of Part 11 is to ensure that SSBAs are handled temporarily by a facility of a registered entity are handled securely prior to disposal.

11.2 Access and storage

11.2a	Does the registered entity ensure that access to the SSBA is restricted to persons that have a need to handle? Comments:	Yes ☐ No ☐
11.2b	Does the registered entity store SSBAs securely to ensure physical access is restricted to those who have a need to handle? Comments:	Yes ☐ No ☐
11.2c	Does the registered entity maintain a record of who accesses the SSBA, including the identity of the person and time and date of access? Comments:	Yes ☐ No ☐

11.3 Transport

11.3.1 Transport requirements for a sending facility

11.3.1	If the registered entity is sending confirmed SSBAs, does it ensure that the sending facility:	
	i. Has documented policies and procedures in place to ensure compliance with Commonwealth, state and territory legislation governing the transport of biological agents?	Yes ☐ No ☐

ii.	Ensures that the receiving facility will accept the agent	Yes ☐ No ☐
iii.	Keeps a record of that acceptance?	Yes ☐ No ☐
iv.	Notifies the receiving facility of the shipment details at the time of shipment?	Yes ☐ No ☐
v.	If the shipment is lost in transit – immediately informs the Australian CDC and state/territory police once aware of the loss?	Yes ☐ No ☐
vi.	If the shipment is reported unsuccessful by the receiving facility–immediately informs the Australian CDC and state/territory police once aware of the unsuccessful transfer?	Yes ☐ No ☐

Comments:

11.3.2 Transport for a receiving facility

11.3.2 If the registered entity is receiving confirmed SSBAs, does it ensure the receiving facility:

i.	Verifies that the transfer was successful; including that:	Yes ☐ No ☐
	a. the complete shipment was received?	
	b. there was no tampering evident on the shipping container?	Yes ☐ No ☐
ii.	Notifies the sending facility of the receipt of the shipment and if the transfer has been successful?	Yes ☐ No ☐
iii.	If a shipment fails to arrive at the expected time – contacts the transport agent and sending facility to seek confirmation of the shipment's location and expected time of delivery?	Yes ☐ No ☐

Comments:

11.4 Destruction

11.4a	Has the registered entity ensured that the processes for destruction are such that no SSBA leaves the entity without being destroyed or inactivated, unless it is being transported in its entirety for the purposes of disposal? *Note: disposal means either complete destruction/deactivation or transfer of all of the SSBA.*	Yes ☐ No ☐ N/A ☐ (SSBA not destroyed)

Comments:

11.5 Waste disposal

11.5a	Does the registered entity have validated procedures for the decontamination of waste materials potentially contaminated with the SSBA?	Yes ☐ No ☐

Comments:

11.6 Record keeping

11.6a	Does the registered entity maintain a record of all activities relating to the requirements of the SSBA Standards that relate to Part 10 of the SSBA Standards?	Yes ☐ No ☐

Comments:

11.6b	Are records relating to SSBAs handled under Part 11 of the SSBA Standards maintained for a minimum of	
	i. 12 months for Tier 1 SSBAs?	Yes ☐ No ☐ N/A ☐ (no Tier 1)

	ii. 6 months for Tier 2 SSBAs?	Yes ☐ No ☐ N/A ☐ (no Tier 2)
Comments:		

Part 11 – Further considerations

The questions below are based on the suggestions made under the commentary of the SSBA Standards or are best practice recommendations. These are not mandatory requirements but may be used to enhance the security of the SSBAs in your facility.

P11a	Does the entity send confirmed SSBAs to a reference laboratory for further genetic typing?	Yes ☐ No ☐
Comments:		

Reporting

The following questions are not based on the requirements of the SSBA Standards but are best practice recommendations. They are not mandatory but are recommended to ensure that all requirements for reporting to the Australian CDC are met.

Ra	Does the entity have documented policies and procedures to ensure that the mandatory time frames for reporting to the Australian CDC are met? *Note: The timeframes for reporting to the Australian CDC are set out in the NHS Act, NHS Regulations and Standards. For all reportable events, this timeframe is 2 business days.* Comments:	Yes ☐ No ☐
Rb	How does the entity submit reports to the Australian CDC? • Hard copy submission via Registered Post? • Electronic submission via the online Data Collection System (DCS)? Comments:	Yes ☐ No ☐ Yes ☐ No ☐
Rc	If the entity uses the DCS to submit reports who administers the passwords for this system? Comments:	
Rd	Does the entity have documented policies about who can sign and submit mandatory reports to the Australian CDC? Comments:	Yes ☐ No ☐

Re	What policies and procedures are in place regarding storage of reportable event reports? i. Where are they stored? ii. Hard copy or *electronic* storage? iii. Who can *access*? Comments:
Rf	Is there training available for completion and submission of reports? Yes ☐ No ☐ Comments:

Internal policies

IPa	Does the facility conform to the internal policies regarding SSBAs set by the entity? *Note: Non- compliances should be recorded in Table 2 below* Comments:	Yes ☐ No ☐
IPb	Where are these policies kept and how can they be accessed by personnel? Comments:	

Outcomes from review

Areas of non-compliance

ORa	Are there any areas of non-compliance with the SSBA Regulatory Scheme? *Record details in Table 1 below.* Comments:	Yes ☐ No ☐
ORb	Are there any areas of non-compliance with the internal policies set by the entity in regards to SSBAs? *Record details in Table 2 below.* Comments:	Yes ☐ No ☐

Actions to address non-compliance

Table 1 – Non-compliance with the SSBA Standards

SSBA Standards clause number	Information about the non-compliance	Actions to rectify	Timeframe for action	Responsibility for action

Comments:

Table 2 – Non-compliance with internal policies

Policy	Information about the non-compliance	Actions to rectify	Timeframe for action	Responsibility for action

Comments:

Further improvements

Are there any areas of potential improvement?	Yes ☐ No ☐
What are they?	
Comments:	

Recommended policies, procedures and processes

Personnel policies, procedures or processes for:

- authorising people to handle and access SSBAs and sensitive information relating to SSBAs;
- recruitment, including establishing identity, history, qualifications, experience and character references of job applicants;
- approving persons who are not authorised persons;
- escorting/supervising approved persons;
- ensuring personnel have an appropriate level of education, training and experience;
- ensuring staff are provided with up-to-date information pertaining to the entity's SSBA risks;
- establishing minimum training requirements for personnel including competency levels for this training;
- ensuring staff meet the competency levels for training;
- providing security awareness training to staff with access to SSBA or sensitive information relating to SSBAs;
- ensuring staff have the required technical competency to handle SSBAs;
- addressing risks associated with human behaviour; and
- excluding personnel, either temporarily or permanently, from the facility.

Physical access policies, procedures or processes for:

- ensuring all recording, photography and filming is authorised;
- access during an emergency;
- managing, reviewing and testing access to secure areas containing SSBA;
- recording, storing and reviewing details of all approved and authorised persons entering areas where SSBAs are handled;
- recording, storing and reviewing exit details from Tier 1 area;

- monitoring, managing and investigating access alarms;
- issuing and managing keys/proximity cards/PINS for access to secure areas; and
- testing access control systems.

Storage of SSBAs policies, procedures or processes for:

- location, security and use of linked storage units for Tier 2 SSBAs;
- minimising the quantities of SSBA held by the facility
- recording transport between the linked storage unit and registered facility; and
- establishing, maintaining and auditing an SSBA inventory

Information management policies, procedures or processes for:

- access, retention and destruction of records relating to all activities relating to the SSBA Standards;
- identifying which material relating to the security of SSBAs is deemed sensitive;
- approving and reviewing access to sensitive information relating to SSBAs;
- storing sensitive information appropriately;
- ensuring computer security;
- on-site security of IT equipment, including IT equipment entering and leaving the building; and
- investigating, managing and reporting breaches of information security.

Transport policies, procedures or processes for:

- ensuring the transport agent has a documented transport security plan and complies with the requirement set out in the section 6.3 of the SSBA Standards;
- verifying that the receiving facility will accept the SSBA;
- supplying the shipping details to the receiving facility;
- notifying the receiving facility at the time of shipment;
- involving the Responsible Officer in the transport process;
- recording incoming shipments of SSBAs;
- notifying the sending facility of the receipt of the shipment;
- liaising with the transport agent to ensure that if there are delays they are informed of these;
- notification when a shipment fails to arrive at the expected time;
- verifying the complete shipment of the SSBA;
- verifying there is no evidence of tampering;

- transporting SSBAs using authorised persons between entities and between facilities in one entity; and
- recording the transport of SSBA by authorised persons.

Inactivation and decontamination policies, procedures or processes for:

- ensuring decontamination and/or inactivation of SSBAs and all contaminated items before their destruction or use as an inactive SSBA;
- ensuring appropriate methodologies are selected;
- ensuring appropriate validation data and verification procedures used to guarantee inactivation has occurred correctly; and
- ensuring no SSBA leaves the facility without being inactivated or destroyed unless for the purpose of transport to another facility or entity.

SSBA management system policies, procedures or processes for:

- the development, authorisation and implementation of the SSBA management system;
- continually assessing and improving the effectiveness of the SSBA management system;
- ensuring that relevant information relating to the SSBA management system is communicated to and from the employees and other relevant parties;
- reviewing the SSBA management system for improvement opportunities;
- meeting the reporting requirements under the NHS Act and the NHS Regulations in respect of any SSBA held;
- justification for all legitimate uses of SSBA held;
- documentation and communication of roles, responsibilities and authorities for SSBA management;
- requirements for all work involving SSBA to be assessed for risks and for mitigation strategies to be prepared before any work is approved to commence;
- complying with legal requirements in relation to handling SSBAs and their transport;
- reducing the level of biosecurity risk;
- continually improving SSBA management performance;
- identifying, collecting, storing and analysing data to assess the suitability and effectiveness of the SSBA management system;
- ensuring that records, documents and data are established, controlled and maintained to provide evidence of compliance with the requirement of the SSBA Standards;
- ensuring SSBA record retention;

- establishment and management of an internal audit program;
- identifying and managing areas of non-compliance with the SSBA Standards, the NHS Act, the NHS Regulations or the SSBA management system;
- acting upon, recording and eliminating the causes of non-compliance;
- reviewing non-compliance records;
- defining, reporting, recording and analysing incidents involving SSBAs; and
- maintaining records of the nature of the incident and any subsequent action taken.

Suspected SSBAs policies, procedures or processes for:

- what constitutes a reasonable suspicion based on laboratory testing;
- restriction of access to those who have a need to handle;
- recording access, transport and destruction;
- verifying that the receiving facility will accept the SSBA;
- supplying the shipping details to the receiving facility;
- notifying the receiving facility at the time of shipment;
- recording incoming shipments of suspected SSBAs;
- notifying the sending facility of the receipt of the shipment;
- liaising with the sending facility in regards to any delays;
- notification when a shipment fails to arrive at the expected time;
- verifying the complete shipment;
- verifying there is no evidence of tampering; and
- reporting to the Australian CDC receipt, transport and disposal of suspected SSBAs.

Resources

The SSBA Regulatory Scheme has produced a series of documents to assist in compliance with the scheme. Please check our website for the latest version of these documents.

Other guidelines

The Australian Federal Police have prepared the following two guidelines to assist entities handling SSBAs:

- Toxin levels in environmental and clinical samples
- Indicators of Suspicious Behaviour in Laboratories Handling SSBA

A copy of these guidelines is available by request – please email ssba@cdc.gov.au.