

# *Security Sensitive Biological Agent (SSBA) Standards*

*Standards for the handling, storage, disposal and  
transport of security sensitive biological agents and  
suspected security sensitive biological agents*

*Consultation Draft*

---

## **Security Sensitive Biological Agent (SSBA) Standards**

ISBN: TBC

Online ISBN: TBC

Publications approval number: TBC

Copyright Statements:

### **Paper-based publications**

© Commonwealth of Australia

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed malesuada scelerisque est. Vestibulum non porttitor nunc, et blandit mauris. In hac habitasse platea dictumst. Curabitur sagittis augue sit amet ipsum tristique, a maximus enim feugiat. Curabitur hendrerit venenatis metus, in pulvinar turpis ultricies at. Donec mattis aliquam nisi, quis fermentum nisi tincidunt a. Ut justo lorem, euismod in posuere quis, porta at eros. Donec accumsan molestie eros. Integer at neque ac dolor consequat hendrerit in sed metus. Etiam turpis nisi, tempor ut consectetur ac, pharetra sed eros. Praesent mattis purus at luctus dapibus. Praesent ultrices, risus non mattis pharetra, nibh elit dapibus dui, sed rutrum purus nulla id elit. Vivamus gravida tellus eu dolor faucibus elementum. Etiam ultrices nulla id magna tristique porta. Duis a congue elit, id tristique turpis. Vestibulum sollicitudin, lorem at viverra

### **Internet sites**

© Commonwealth of Australia

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed malesuada scelerisque est. Vestibulum non porttitor nunc, et blandit mauris. In hac habitasse platea dictumst. Curabitur sagittis augue sit amet ipsum tristique, a maximus enim feugiat. Curabitur hendrerit venenatis metus, in pulvinar turpis ultricies at. Donec mattis aliquam nisi, quis fermentum nisi tincidunt a. Ut justo lorem, euismod in posuere quis, porta at eros. Donec accumsan molestie eros. Integer at neque ac dolor consequat hendrerit in sed metus. Etiam turpis nisi, tempor ut consectetur ac, pharetra sed eros. Praesent mattis purus at luctus dapibus. Praesent ultrices, risus non mattis pharetra, nibh elit dapibus dui, sed rutrum purus nulla id elit. Vivamus gravida tellus eu dolor faucibus elementum. Etiam ultrices nulla id magna tristique porta. Duis a congue elit, id tristique turpis. Vestibulum sollicitudin, lorem at viverra

## FOREWORD

The Security Sensitive Biological Agent (SSBA) Standards (SSBA Standards) are requirements for non-exempt entities to ensure the security of biological agents of security concern in Australia. These Standards set out the physical, personnel, transport, information management, inactivation and decontamination security requirements for non-exempt entities when handling SSBA and biological agents suspected of being SSBA<sup>1</sup>.

The SSBA Standards are made under Part 3 of the *National Health Security Act 2007* (NHS Act), which provides the legislative framework for establishing controls for the security of certain biological agents that could be used as weapons.

---

<sup>1</sup> The List of Security Sensitive Biological Agents, which details which biological agents are considered to be security sensitive biological agents, can be found at [www.cdc.gov.au/ssba](http://www.cdc.gov.au/ssba).

## CONTENTS

|                                                                                 |           |
|---------------------------------------------------------------------------------|-----------|
| INTRODUCTION .....                                                              | 6         |
| Scope .....                                                                     |           |
| Normative references .....                                                      | 8         |
| Terms and definitions .....                                                     | 9         |
| <b>Part 1 SSBA management system .....</b>                                      | <b>15</b> |
| 1.1 Objective.....                                                              | 16        |
| 1.2 Policy.....                                                                 | 17        |
| 1.3 Roles, responsibilities, and authorities.....                               | 17        |
| 1.4 Checking and corrective action.....                                         | 20        |
| <b>Part 2 Risk and incident management.....</b>                                 | <b>23</b> |
| 2.1 Objective.....                                                              | 24        |
| 2.2 Hazard and risk identification, assessment, and management.....             | 24        |
| 2.3 Review.....                                                                 | 29        |
| <b>Part 3 Personnel .....</b>                                                   | <b>31</b> |
| 3.1 Objective.....                                                              | 32        |
| 3.2 Responsible Officers.....                                                   | 32        |
| 3.3 Authorised persons.....                                                     | 33        |
| 3.4 Approved persons .....                                                      | 34        |
| 3.5 Provisional authorisation for new entities.....                             | 35        |
| 3.6 National Health Security (NHS) checks .....                                 | 36        |
| 3.7 Recruitment .....                                                           | 38        |
| 3.8 Training and competency .....                                               | 39        |
| 3.9 Behavioural factors .....                                                   | 41        |
| 3.10 Exclusion .....                                                            | 42        |
| <b>Part 4 Physical security and Storage.....</b>                                | <b>43</b> |
| 4.1 Objective.....                                                              | 44        |
| 4.2 Perimeter.....                                                              | 44        |
| 4.3 Physical access controls.....                                               | 45        |
| 4.4 Storage.....                                                                | 47        |
| 4.5 Working cultures and Toxin Extracts .....                                   | 47        |
| 4.6 SSBA inventory .....                                                        | 47        |
| 4.7 Storage of Tier 1 SSBA.....                                                 | 48        |
| 4.8 Storage of Tier 2 SSBA.....                                                 | 48        |
| 4.9 Record keeping .....                                                        | 50        |
| <b>Part 5 Information management.....</b>                                       | <b>51</b> |
| 5.1 Objective.....                                                              | 52        |
| 5.2 Record keeping .....                                                        | 52        |
| 5.3 Information security .....                                                  | 53        |
| 5.4 Disposal of records.....                                                    | 55        |
| <b>Part 6 Transport.....</b>                                                    | <b>57</b> |
| 6.1 Objective.....                                                              | 58        |
| 6.2 Transport.....                                                              | 58        |
| 6.3 Transport security.....                                                     | 59        |
| 6.4 Transport of SSBA by authorised persons.....                                | 61        |
| 6.5 Transport of SSBA from reception areas to a registered facility .....       | 61        |
| <b>Part 7 Inactivation and decontamination.....</b>                             | <b>63</b> |
| 7.1 Objective.....                                                              | 64        |
| 7.2 Procedures .....                                                            | 64        |
| 7.3 Waste management.....                                                       | 65        |
| 7.4 Record keeping .....                                                        | 66        |
| <b>Part 8 Handling biological agents suspected of being SSBA.....</b>           | <b>67</b> |
| 8.1 Objective.....                                                              | 68        |
| 8.2 Access and Storage.....                                                     | 68        |
| 8.3 Transport .....                                                             | 69        |
| 8.4 Destruction .....                                                           | 70        |
| 8.5 Waste Disposal.....                                                         | 70        |
| 8.6 Record Keeping.....                                                         | 71        |
| <b>Part 9 Handling SSBA following a positive confirmatory test result .....</b> | <b>72</b> |
| 9.1 Objective.....                                                              | 73        |
| 9.2 Access and Storage.....                                                     | 73        |
| 9.3 Transport .....                                                             | 74        |
| 9.4 Destruction .....                                                           | 75        |
| 9.5 Waste Disposal.....                                                         | 75        |
| 9.6 Record Keeping.....                                                         | 75        |
| <b>Part 10 Non-registered entity handling an SSBA on a temporary basis.....</b> | <b>77</b> |

|                     |                                                                                                       |           |
|---------------------|-------------------------------------------------------------------------------------------------------|-----------|
| 10.1                | Objective .....                                                                                       | 78        |
| 10.2                | Access and Storage .....                                                                              | 78        |
| 10.3                | Transport.....                                                                                        | 79        |
| 10.4                | Destruction .....                                                                                     | 80        |
| 10.5                | Waste Disposal .....                                                                                  | 80        |
| 10.6                | Record Keeping .....                                                                                  | 80        |
| <b>Part 11</b>      | <b>Registered entity handling an SSBA that they are not registered for, on a temporary basis.....</b> | <b>82</b> |
| 11.1                | Objective .....                                                                                       | 83        |
| 11.2                | Access and Storage .....                                                                              | 83        |
| 11.3                | Transport.....                                                                                        | 84        |
| 11.4                | Destruction .....                                                                                     | 85        |
| 11.5                | Waste Disposal .....                                                                                  | 85        |
| 11.6                | Record Keeping .....                                                                                  | 86        |
| <b>Appendix 1</b>   | <b>Health Security Relevant Offences .....</b>                                                        | <b>87</b> |
| <b>Bibliography</b> | <b>.....</b>                                                                                          | <b>90</b> |

# INTRODUCTION

The *National Health Security Act 2007* (NHS Act) provides the legislative framework for the regulation of security sensitive biological agents (SSBAs) in Australia. Part 3 of the NHS Act provides for the establishment of:

- The List of Security Sensitive Biological Agents
- SSBA Standards (these Standards)
- A National Register of SSBAs
- Exemptions from the regulatory scheme
- Purposes for handling SSBAs that are considered legitimate
- Reporting requirements
- An inspection scheme

SSBAs are defined as biological agents that are included in the List of SSBAs, established by the Minister for Health, Disability and Ageing under the NHS Act. The list is published on the Australian Centre for Disease Control's (CDC) website. This list consists of two tiers: Tier 1 agents are those that pose the highest biosecurity risk and are subject to the highest level of security and reporting, while Tier 2 agents pose a high biosecurity risk and are subject to proportionately high security and reporting.

The SSBA Standards are determined under section 35 of the NHS Act. They set out the requirements that must be met by the entity to ensure physical security around handling, storage, disposal and transport of SSBAs and biological agents suspected of being SSBAs, as well as personnel and information security. The SSBA Standards set out specific requirements for managing SSBA related biosecurity risks and issues, and establish a systematic approach to managing the biosecurity of SSBAs.

The Standards comprise:

- Requirements, which are presented in shaded boxes. They are mandatory for compliance purposes and generally use absolute language such as the word "must"
- Commentary, which generally use suggestive language such as the word "should" and comprise either recommended approaches to achieving the requirements, recommended extensions to them or further information about the requirement. They should be used to develop equivalent best practice and are presented as "Commentary" in *italic* text

The SSBA Standards are set out in a number of Parts:

- Parts 1–7 of these Standards set out the requirements for entities registered with the Australian CDC that are handling SSBAs. These parts apply to registered entities only
- Part 8 sets out the requirements for entities handling a suspected SSBA. This part applies to any entity handling a suspected SSBA that they are not registered for
- Part 9 sets out the requirements for entities that are handling a (formerly suspected) SSBA following a positive confirmatory test result, prior to disposal or registration. This part applies to any entity handling a (formerly

suspected) SSBA that they are not registered for that has received a positive confirmatory testing result

- Part 10 sets out the requirements for non-registered entities handling a known SSBA under the temporary handling provisions (for up to seven working days) of the NHS Act
- Part 11 sets out the requirements for known SSBA's which are being handled temporarily by a registered entity, which is not registered to handle that SSBA, to ensure the SSBA is handled securely prior to disposal

Because SSBA's are biological materials such as infectious agents or toxins, the requirements of AS/NZS 2243.3:2022 Safety in laboratories - Microbiological safety and containment, together with the other parts of AS/NZS 2243<sup>2</sup>, need to be considered by entities when developing plans as required by these Standards. The Commonwealth, States and Territories have occupational health and safety legislation that should be complied with when following these Standards.

Electronic versions of the NHS Act, NHS Regulations and these Standards are available on the Australian CDC's website.

---

<sup>2</sup> The Standards Australia web site ([www.standards.org.au/](http://www.standards.org.au/)) should be consulted for the most up to date versions.

## Scope

The NHS Act is complemented by the *National Health Security Regulations 2018* (NHS Regulations) and the Security Sensitive Biological Agent (SSBA) Standards (these Standards). All three documents must be consulted to gain a full picture of requirements for the management of SSBA and suspected SSBA. Compliance with the NHS Act, NHS Regulations and these Standards is mandatory.

The objective of these Standards is to set out the requirements that must be met by the entity to ensure physical security around handling, storage, disposal and transport of SSBA and biological agents suspected of being SSBA, as well as personnel and information security.

In addition, entities handling or transporting SSBA must comply with all relevant legislation, regulations and standards governing biological materials. Where an SSBA is subject to biosecurity controls, organisations must ensure that any required import permits are obtained in advance from the Department of Agriculture, Fisheries and Forestry (DAFF) for specific applicable conditions for importation. If an SSBA is considered to pose enough of a human biosecurity risk (as per the Biosecurity Act 2015), work involving the material must be conducted within an Approved Arrangement. Approved Arrangements are voluntary agreements that allow facilities to manage biosecurity risks at their own sites in line with DAFF requirements<sup>3</sup>.

Any dealings with genetically modified organisms are prohibited unless authorised by the Office of the Gene Technology Regulator (OGTR). For transport of SSBA, in addition to the mandatory requirements of these Standards, entities should be aware of Commonwealth, State and Territory legislation governing the transport of biological materials such as the *Australian Code for the Transport of Dangerous Goods by Road and Rail* and the *Civil Aviation Safety Regulations 1998*.<sup>4</sup>

The emphasis of these Standards is on biosecurity and not biosafety. The latter should be addressed by complying with the Occupational Health and Safety Acts of the Commonwealth, States and Territories, by following AS/NZS 2243.3:2022 Safety in laboratories – Microbiological safety and containment, by complying with relevant National Pathology Accreditation Advisory Council (NPAAC) Standards and National Association of Testing Authorities (NATA) requirements, and adhering to the recommendations of the World Health Organization's (WHO) Laboratory Biosafety Manual, 4<sup>th</sup> Edition.

These Standards, as well as referenced complementary legislation, regulations and standards, are reviewed at regular intervals and entities should ensure that they have the current version available. The current version of the SSBA Standards can be downloaded from the Australian CDC's website or requested from [ssba@cdc.gov.au](mailto:ssba@cdc.gov.au).

## Normative references

*Australian Code for the Transport of Dangerous Goods by Road and Rail (ADG Code)*<sup>5</sup>

*AS/NZS 2243.3:2022 Safety in laboratories – Microbiological safety and containment*

---

<sup>3</sup> [www.agriculture.gov.au/biosecurity-trade/import/arrival/arrangements](http://www.agriculture.gov.au/biosecurity-trade/import/arrival/arrangements)

<sup>4</sup> All documents referenced throughout these Standards are current at the time of publication. Entities should ensure that they are using the most recent version of any document.

<sup>5</sup> Available for free download from [www.ntc.gov.au](http://www.ntc.gov.au)

*Civil Aviation Safety Regulations 1998*<sup>6</sup>

*National Health Security Act 2007*

*National Health Security Regulations 2018*

*WHO Laboratory Biosafety Manual, 4th Edition, 2020*

## Terms and definitions

**Adverse or Adverse criminal record**—for the purposes of a result from a NHS check under the Department of Home Affairs AusCheck scheme ([www.auscheck.gov.au](http://www.auscheck.gov.au)), means that a person has been found to have a health-security-relevant offence that has a sentence of imprisonment.

**Adverse security assessment**—has the same meaning as in Part IV of the *Australian Security Intelligence Organisation Act 1979*.

**Approved person**—means a person, such as contractors, visitors, suppliers, students, and other such persons, approved to:

- Handle SSBA
- Access the facility where SSBA are handled
- Access sensitive information related to SSBA

under escort or supervision of an authorised person (see clause 3.4).

**Audit**—as defined by ISO 35001:2019, means a systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which criteria are fulfilled. Note that independent does not necessarily mean external to the organisation. In many cases, particularly in smaller organisations, independence can be demonstrated by freedom from responsibility for the activity being audited. For further guidance on audit evidence and audit criteria, see ISO 19011:2018.

**Authorised person**—means a person authorised (refer to Part 3) to:

- Handle SSBA
- Access the facility where SSBA are handled
- Access sensitive information related to SSBA (unless the person meets the requirements in line with Part 5, Clause 5.3.1 of these Standards)

**Biological agents**—include:

- Bacteria and viruses
- Toxins derived from biological sources, including animals, plants and microbes. [NHS Act]

**Biological materials**—means any material comprised of, containing, or that may contain biological agents and/or their harmful products, such as toxins and allergens. [ISO 35001:2019]

**Biosafety**—means the practices that reduce the risk of unintentional exposure or release of biological materials. [ISO 35001:2019]

---

<sup>6</sup> The Civil Aviation Safety Regulations 1998, NHS Act and NHS Regulations are available for free download from [www.comlaw.gov.au](http://www.comlaw.gov.au)

**Biosecurity**—means the practices and controls that reduce the risk of loss, theft, misuse, diversion of, or intentional unauthorised release of biological materials. [ISO 35001:2019]. In the context of these Standards, biosecurity is restricted to SSBA.

**Competence**—means having the appropriate education, training, skills and experience needed to perform roles and responsibilities. [Adapted from ISO 9000:2015]

**Confirmatory testing**—means a test undertaken to confirm that an agent is an SSBA.

**Containment**—the combination of physical design parameters and operational practices that protect personnel, the immediate work environment and the community from exposure to biological agents. [WHO Laboratory Biosafety Manual, 4<sup>th</sup> Edition, 2020]

**Continual improvement**—means a process of enhancing the SSBA management system on a regular, periodic and sustained basis to achieve improvements in overall SSBA management performance consistent with the organisation's SSBA management policy. [Adapted from ISO 45001:2018]

**Convicted**—for the purposes of the SSBA Standards, means that a person has a conviction of a health security relevant offence.

**Conviction**—(of a person for an offence) has the meaning given by subsection 85ZM (1) of the *Crimes Act 1914*, but does not include:

- A spent conviction (within the meaning given by subsection 85ZM (2) of that Act) if Division 3 of Part VIIC of that Act applies to the person
- A conviction for an offence of which, under a law relating to pardons or quashed convictions, the person is taken never to have been convicted

Additionally, note that:

- Under the definition of conviction in subsection 85ZM (1) of the *Crimes Act 1914*, a person is also taken to have been convicted of an offence if the person has been convicted of the offence but no conviction has been recorded, and if a court has taken the offence into account in sentencing the person for another offence (see paragraphs 85ZM (1) (b) and (c) of the *Crimes Act 1914*)
- Under Part VIIC of the *Crimes Act 1914*, if a person receives a free and absolute pardon for an offence against a law of the Commonwealth or a Territory because the person was wrongly convicted of the offence, the person is taken for all purposes never to have been convicted (see section 85ZR)
- In certain circumstances, Division 3 of Part VIIC of the *Crimes Act 1914* ceases to apply to a person in relation to a spent conviction if Division 4 (Convictions of further offences) applies
- Under the *Crimes Act 1914*, a person need not disclose convictions that have been quashed (see section 85ZT) or are spent (see section 85ZV)
- Convictions for health security relevant offences do not become spent if they fall within the scope of the National Health Security Check Scheme exemptions listed in Schedule 4 of the Crimes Regulations 1990

**Corrective action**—means an action to eliminate the cause of a detected non-compliance or other undesirable situation, and to prevent recurrence. [Adapted from ISO 35001:2019]

**Decontamination**—means a procedure that eliminates or reduces biological agents to a safe level with respect to transmission of infection or other adverse effects. [Adapted from ISO 35001:2019]

**Deputy Responsible Officer**—a position appointed by top management who is able to assume the responsibilities and duties of the responsible officer as defined in Part 3.2 of these Standards.

**Disposal (or to dispose of)**—for the purposes of the SSBA Regulatory Scheme, means the complete transfer or destruction of all holdings of the biological agent. [Adapted from NHS Act]

**Eligible**—for the purposes of a result from an NHS check under the Department of Home Affairs AusCheck scheme ([www.auscheck.gov.au](http://www.auscheck.gov.au)), means that a person has:

- No health-security-relevant offence
- Less than 3 separate health security-relevant offences in the 10 years before the check, and none of them has a sentence of imprisonment

**Entity**—means any of the following:

- An individual
- A body corporate
- An agency or instrumentality of the Commonwealth, a State, or a Territory. [NHS Act]

**Exempt entity**—has the meaning given by s 40 of the *National Health Security Act 2007*. [NHS Act]

**Facility**—includes:

- A building, or part of a building
- A laboratory (including a mobile laboratory) [NHS Act]

**Handling**—includes:

- Receiving, holding, using, and storing biological agents
- Any operation incidental to, or arising out of, any of those operations [NHS Act]

**Harm**—means the adverse effect on the health of people, animals, or plants, on the environment or on the Australian economy. [Adapted from ISO 35001:2019]

**Hazard**—means a source, situation or act with a potential for causing harm. [Adapted from ISO 35001:2019]

**Imprisonment**—includes a suspended sentence, periodic detention and home-based detention but does not include:

- Detention of a person until the rising of the court
- A sentence of community service

**Inactivation**—means removal of the activity of biological agents by destroying or inhibiting reproductive or enzyme activity. [WHO Laboratory Biosafety Manual, 4<sup>th</sup> Edition]

**Incident**—An occurrence that has the potential to, or results in, the exposure of laboratory personnel to biological agents and/or their release into the environment that may or may not lead to actual harm. [WHO Laboratory Biosafety Manual, 4<sup>th</sup> Edition]

**Initial tester**—means an entity that has tested a biological agent to determine the identity of the biological agent and has formed a reasonable suspicion (but is not certain) that the biological agent is an SSBA. [Adapted from the NHS Act]

**Inspector**—means a person appointed as an inspector under s 63 of the NHS Act. [NHS Act]

**Inventory**—means a record of stored SSBA.

**List of Security Sensitive Biological Agents**—means the list established under the NHS Act. The list designates which biological agents are regulated under Part 3 of the NHS Act. Refer to [www.health.gov.au/ssba](http://www.health.gov.au/ssba).

**NHS Act**—means the *National Health Security Act 2007*.

**National criminal history check**—for the purposes of an NHS check, is an assessment of a person's criminal history information.

**NHS check**—means a National Health Security check, conducted via the Department of Home Affairs AusCheck scheme ([www.auscheck.gov.au](http://www.auscheck.gov.au)). For the purposes of the SSBA Standards, these checks consist of a national criminal history check against the list of health security relevant offences set out in Appendix 1 of the SSBA Standards, and a national security assessment.

**NHS Regulations**—means the *National Health Security Regulations 2018*.

**National Register**—means the National Register of Security Sensitive Biological Agents. [Adapted from the NHS Act]

**National security assessment**—conducted by the Australian Security Intelligence Organisation (ASIO), determines whether an individual has any known links to politically motivated violence, terrorism or other high-risk activities or groups, including espionage, sabotage, promotion of communal violence, attacks on Australia's defence system or acts of foreign interference. [adapted from *Australian Security Intelligence Organisation Act 1979*].

**Non-compliance**—for the purposes of these Standards, means a failure or refusal to comply with the requirements of the NHS Act, the NHS Regulations or the SSBA Standards. Non-compliance may be a discrete event in time or an ongoing event.

**Not eligible**—for the purposes of these Standards, means that a person has been found to have an adverse security assessment result from a NHS check under the Department of Home Affairs AusCheck scheme ([www.auscheck.gov.au](http://www.auscheck.gov.au)) (see **Adverse or Adverse criminal record**).

**Preventive action**—means an action that is intended to eliminate the cause of a potential non-compliance or other undesirable potential situation. [Adapted from ISO 9000:2015]

**Prohibited drug**—means any of the following (as defined in section 300.2 of the *Criminal Code Act 1995* (Criminal Code))

- a controlled drug
- a controlled plant
- a controlled precursor

**Qualified offence**—means an offence against a law of the Commonwealth, or of a State or Territory, of a kind mentioned in Appendix 1 of these Standards.

**Qualified or qualified criminal record**—for the purposes of a result from a NHS check under the Department of Home Affairs AusCheck scheme

([www.auscheck.gov.au](http://www.auscheck.gov.au)), means that a person has 3 or more separate health security-relevant offences in the 10 years before the check, and none of them has a sentence of imprisonment.

**Record**—means a document stating results achieved or providing evidence of activities performed. [Adapted from ISO 9000:2015]

**Reportable event**—means an event referred to in s 48(1) of the NHS Act.

**Responsible Officer**—A position appointed by top management to oversee the SSBA management system as defined in Part 3.2 of these Standards.

**Risk**—A combination of the likelihood of an incident occurring and the severity of the harm (consequences) if that incident were to occur. [Adapted from WHO Laboratory Biosafety Manual, 4<sup>th</sup> Edition, 2020]

**Risk assessment**—means a systematic process of gathering information and evaluating the likelihood and consequences of exposure to, or release of, workplace hazards and determining the appropriate risk control measures to reduce the risk. [Adapted from WHO Laboratory Biosafety Manual, 4<sup>th</sup> Edition, 2020]

**Sample of a biological agent**—includes:

- A subculture of the agent
- A preparation made of the agent [the NHS Act]

**Sensitive information**—means any of the following:

- An entity's storage records for the security-sensitive biological agent handled at the facility
- An entity's risk assessment and risk management plan for the security-sensitive biological agent handled at the facility
- 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. [Adapted from the NHS Regulations]

**SSBA**—means a security sensitive biological agent. The List of Security Sensitive Biological Agents defines which biological agents are SSBAs. [the NHS Act]

**SSBA Standards/These Standards**—means the Security Sensitive Biological Agent (SSBA) Standards determined by the Minister under the NHS Act.

**Stand-alone facility**—where all four walls of the secure perimeter are accessible from the outside and is not surrounded or connected to any other building (such as a demountable unit).

**Standard operating procedure (SOP)**—means a set of written instructions that documents a routine or repetitive activity to be followed by an entity or facility.

**Suspected SSBA**—means a biological agent suspected, on the basis of testing in a laboratory, to be a security sensitive biological agent. [Adapted from the NHS Act].

**Temporary handling**—means the handling of a known SSBA by a non-registered entity, or a known SSBA that the entity is not registered for, for a period of up to seven working days. After this seven-day period, an entity must either dispose of or register to handle the SSBA.

**The Australian CDC**—means the Australian Centre for Disease Control.

**Tier 1 SSBAs**—means an agent that is referred to as a Tier 1 agent on the List of Security-sensitive Biological Agents. These agents pose the highest level of

biosecurity risk and must be tightly regulated. The current list is published on the Australian CDC's website.

**Tier 2 SSBA**s—means an agent that is referred to as a Tier 2 agent on the List of Security Sensitive Biological Agents. These agents pose a high biosecurity risk and must be subjected to proportionally high regulation. The current list is published on the Australian CDC's website.

**Top management**—means a person or group of people who direct and control the entity at the highest practical level and are able to allocate resources and make top level decisions regarding the entity/facility.

**Transport**—for the purposes of the SSBA Standards includes the processes (for example, information and security requirements at the facility of origin and receipt) involved with the physical movement of SSBA from one place to another place.

**Transport agent**—for the purposes of the SSBA Standards is an entity that has relevant training and recognition to ship or transport Class 6 dangerous goods (refer to the *Australian Code for the Transport of Dangerous Goods by Road and Rail*).

**Validation**—means confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled. [Adapted from ISO 9000:2015]

**Verification**—means confirmation, through the provision of objective evidence, that specified requirements have been fulfilled. [Adapted from ISO 9000:2015]

**Vulnerability analysis**—means the determination of how each credible threat can be realised against critical assets (including SSBA). This involves determining:

- Potential means by which a successful “attack” against an asset could be carried out
- The effectiveness of each of the layers of security in managing this “attack” against the assets, people, information, or infrastructure

[Adapted from SA HB 167:2025]

# Part 1 SSBA management system

# 1

## 1.1 Objective

- (1) To ensure that entities establish a systematic approach to the management of the biosecurity of SSBA. To achieve this, entities must consider risk and incident management, personnel management, physical security, information management, transport, inactivation and decontamination, in accordance with the requirements of the NHS Act, the NHS Regulations and these Standards.

*The management system approach implies that identifying, understanding and managing a system of interrelated processes for a given objective improves the entity's effectiveness and efficiency for managing SSBA.*

*The SSBA management system should meet more rigorous requirements for Tier 1 SSBA, as articulated in these Standards. The entity should strive to continue to develop and refine its SSBA management system to ensure that further opportunities for improvement are identified and implemented. This may be achieved through goal setting and targets placed upon those working within the facility, and monitoring progress to ensure the goals are achieved.*

*Application of a management system approach leads to the following actions:*

- *Defining the system by identifying or developing the processes that affect a given objective*
- *Structuring the system to achieve the objective in the most effective manner*
- *Understanding the interdependence among the processes of the system*
- *Continually improving the system through measurement and evaluation*
- *Establishing and providing adequate resources prior to action*

*An effective management system approach should be built on the concept of continual improvement through a cycle of planning, implementing, reviewing and improving the processes and actions that an entity undertakes to meet goals. This is known as the PDCA (Plan-Do-Check-Act) cycle:*

**Plan:** *Planning, including identification of the hazards and risks, and establishing goals*

**Do:** *Implementing, including training and operational issues*

**Check:** *Checking, including monitoring and corrective actions*

**Act:** *Reviewing, including process innovation and acting to make needed changes to the SSBA management system.*

*The approach outlined above has been successfully adopted by the International Organization for Standardization (ISO) in a range of areas relevant to biorisk management, including ISO 35001:2019. It can be integrated with established quality, environmental and occupational health and safety systems within an entity. These Standards are compatible with other systems and risk management standards, such as those listed in the bibliography of these Standards.*

*In order to improve SSBA management the entity should focus on identifying and addressing the causes of non-compliance and incidents. Systematic identification and correction of system deficiencies leads to improved performance and control of SSBA.*

## 1.2 Policy

- (1) The entity must develop, document, authorise, and implement policy concerning the management of SSBA. This policy must clearly state the overall objectives and commitment to improving SSBA biosecurity management. This policy must be in place prior to the handling of SSBA. The policy must specifically include provisions covering:
  - (a) meeting the reporting requirements under the NHS Act and the NHS Regulations in respect of any SSBA or suspected SSBA held by the entity
  - (b) justification for all legitimate uses of any SSBA held by the entity
  - (c) documentation and communication of roles, responsibilities, and authorities for SSBA management within the entity
  - (d) effectively informing all personnel and other relevant parties of individual obligations regarding SSBA management
  - (e) a requirement for all projects/work involving SSBA to be assessed for risks and for mitigation strategies to be prepared before any work is approved to commence
  - (f) review of the management system at least every two years or following an incident
- (2) The entity must continually assess and improve the effectiveness of the SSBA management system using policies, objectives, procedures, self-review programs, data analysis, risk assessment and management, corrective and preventive actions, and management review.
- (3) The policy must be appropriate to the nature and scale of risk associated with the facility and associated activities, and commit to:
  - (a) complying with legal requirements in relation to handling SSBA and their transport
  - (b) reducing the level of biosecurity risk to an acceptable level (refer to Part 2 of these Standards) and, in the context of SSBA related activities, ensuring that the need for effective SSBA management takes precedence over all non “health and safety” operational requirements
  - (c) continually improving SSBA management performance
- (4) The entity must ensure that relevant information relating to its SSBA management system and activities is communicated to personnel and other relevant parties.

*When communicating information about SSBA policies to other relevant parties, the entity should consider who may need to know such information as part of their activities. Other relevant parties may include, for example, government agencies, emergency services, security personnel, cleaners, maintenance staff and other support groups.*

## 1.3 Roles, responsibilities, and authorities

### 1.3.1 Top management

- (1) The entity must ensure that top management:

- (a) takes ultimate responsibility for the development and implementation of the entity's SSBA management system and policy
- (b) ensures the availability of resources to establish, implement, maintain and improve the SSBA management system
- (c) appoints and empowers a Responsible Officer and a Deputy Responsible Officer for the SSBA Regulatory Scheme, and puts in place processes to ensure continuity of the staffing and effectiveness of these positions (refer to clause 3.2)
- (d) ensures that all SSBA-related activities to be conducted by the entity are authorised, defined, documented and reviewed at least annually
- (e) ensures that criteria and processes are established for work that requires prior approval
- (f) ensures that actions are taken promptly to eliminate any identified non-compliance of the management system with these SSBA Standards, the NHS Act and the NHS Regulations, and to deal with any identified instances of the entity's non-compliance with these three legislative instruments. Top management must ensure verification of the actions taken and the documentation of such verification
- (g) establishes controls and puts in place documented procedures for monitoring the effectiveness of the controls being applied to reduce or eliminate the hazards identified in risk assessment processes
- (h) ensures that staff levels, facilities and equipment are sufficient to effectively carry out work involving SSBA in accordance with technical protocols, approved policies and SOPs
- (i) ensures that all requirements for reporting to the Australian CDC are met
- (j) In assigning roles and responsibilities, conflicts of interest (real or perceived) must be considered.

*While overall responsibility for management of SSBA rests with top management, tasks may be delegated through the entity provided they are passed to competent individuals with adequate resources to perform the activities effectively. In smaller entities, one individual may hold more than one role described in these Standards. It is important that roles and responsibilities are defined, there is clear communication within the entity in terms of the actions that need to be taken and persons with responsibilities for actions have the required authority.*

*The SSBA Standards identify roles that need to be covered by the entity and use titles only to illustrate these roles. These titles may not be the same as the titles used in specific entities.*

*Resources include human resources and specialised skills, entity infrastructure, technology and financial resources. Determination of staffing levels, facilities and equipment should be determined in consultation with the Responsible Officer of the facility.*

*Documentation of SSBA-related activities should include the nature of the activities authorised to be conducted in the facility and their definitions (for example, diagnostics, research, small scale/large scale). All activities routinely associated with the work program should be specified and supported by formal SOPs approved in accordance with the requirements for controlled documents as defined by these Standards. Any changes to these activities should be subjected to a formal change*

*management process that involves approval by management with subsequent communication and training of relevant staff.*

*The controls can be monitored by regular reviews, by utilising corrective action reporting processes where problems have been identified, by investigation of incidents, by improving controls and their implementation, and by ensuring that adequate resources are provided to maintain the effectiveness of the controls.*

### 1.3.2 SSBA Management Committee

- (1) The entity must establish an SSBA Management Committee, or assign the tasks required of such a committee to an existing committee, to act as a review group for SSBA risks and issues. The Committee must report to top management and must:
  - (a) maintain documented terms of reference
  - (b) include a representative cross-section of expertise, appropriate to the nature and scale of the SSBA activities undertaken
  - (c) include both the Responsible Officer and the Deputy Responsible Officer
  - (d) meet at a defined and appropriate frequency, and when otherwise required
- (2) The functions of the committee must include:
  - (a) contributing to the development of the entity's SSBA policies and procedures
  - (b) reviewing and approving protocols and risk assessments for work involving SSBA's
  - (c) reviewing information relating to significant incidents, non-compliance, data trends, associated local/entity actions and associated communication needs
  - (d) ensuring biosecurity issues are formally recorded, actions allocated, tracked and closed out effectively, and that internal inspection reports are reviewed

*The SSBA Management Committee may be a stand-alone committee or part of another existing committee. The list of functions under clause 1.3.2 includes the minimum areas which are to be addressed and is neither exhaustive nor comprehensive. When determining membership of the committee, the entity will need to balance the need for relevant expertise versus the need to restrict the number of persons with knowledge about SSBA's.*

*The terms of reference for the committee should provide clear direction to committee members on the parameters and expected objectives of their task.*

*Terms of reference may include:*

*Purpose – a brief statement of the purpose of the committee*

*Role and Function – sets out the roles and functions of the committee and how the objectives are to be achieved.*

*Composition – sets out who is part of the committee as a member, observer or other.*

*Quorum – if a quorum is in place this should set out what that number is and what will occur if quorum is not reached.*

*Deliverables – sets out what the committee will deliver.*

*Timeframes – this should set out what the committee timeframes are, such as meeting frequency, reporting timeframes, review timeframes and timeframes for any set tasks.*

*Reporting – sets out what needs to be reported and to whom.*

*Evaluation – sets out when the committee is to undertake any evaluations of its roles and functions or other terms of reference and how the committee effectiveness will be evaluated.*

*It may not be necessary for both the Responsible Officer and Deputy Responsibility Officer to attend all meetings, but entities should ensure that at least one officer is able to attend each meeting.*

## 1.4 Checking and corrective action

### 1.4.1 Performance management and analysis of data

- (1) The entity must ensure that data is identified, collected, stored and analysed to assess the suitability and effectiveness of the SSBA management system and to evaluate where continual improvement of the system can be made.
- (2) Outcomes of this process must be documented.

*The analysis should include consideration of data generated through monitoring, measurement, reviews, and other sources. Examples of data that would be collected include records of entry and exit from the facility, records of SSBA storage and usage, records of validation data and decontamination of SSBA's (including validation that autoclaves and disinfectants are functioning within operating parameters), testing of access control systems to validate that they are within operating parameters, any records of shipment or receipt of SSBA's, and records of reporting to the Australian CDC. Analyses should be conducted at least every two years and more often if justified by the risks and the scope of operations. The results of the analysis should be considered as part of management review.*

### 1.4.2 Records, documentation and data control

- (1) The entity must ensure that records, documents and data are established, controlled and maintained to provide evidence of compliance with the requirements of these SSBA Standards, and that they remain legible, readily identifiable and retrievable in alignment with the information management requirements in Part 5 of these Standards.
- (2) The entity must document and implement its SSBA record retention policies.

*Where appropriate, documents should be identified and controlled based on the nature of the work and the need for record keeping.*

*Controlled documents may include:*

- Risk assessments, SOPs and safety manuals
- Job hazard analyses and charts of authority
- Audit and inspection checklists

- *Laboratory SSBA manuals, authorisations and other security documents*
- *Training records*

### 1.4.3 Internal review

- (1) The entity must ensure that an internal program of review is conducted.
- (2) These reviews must be conducted at planned intervals (no longer than 6 monthly for Tier 1 and annually for Tier 2 SSBA) to determine that operations carried out by the Entity comply with the requirements of these Standards, the NHS Act, NHS Regulations and the entity's SSBA policies.
- (3) Records must be maintained of findings of reviews, including action taken to close out any non-compliances or improvement opportunities and in accordance with Part 5 of these Standards.

*Reviews may range from frequent checks on specific areas to ensure standards are being maintained (for example, storage of SSBA, disinfectant levels/concentrations for inactivation of SSBA and entry/exit records), to more extensive but less frequent reviews of laboratories or other operations.*

*Review of documentation relating to the SSBA Regulatory Scheme should be periodically undertaken and include consideration of whether records have been altered or tampered with, especially if any other instances of suspicious behaviour have occurred. Entities may consider training for staff in the review of management systems.*

*Reviews may be conducted at any time including following a direction from top management or at the request of the Australian CDC. An Internal Review Template is available on the Australian CDC's website.*

### 1.4.4 Control of non-compliance and corrective action

- (1) The entity must ensure that any areas of non-compliance with these Standards, the NHS Act, the NHS Regulations or the SSBA management system, as identified by the entity or through the SSBA Regulatory Scheme Inspection Program are documented, addressed and managed. At a minimum this must include:
  - (a) reviewing all non-compliances
  - (b) determining the causes of non-compliance
  - (c) evaluating the need for, and implementing relevant action to ensure that non-compliance does not reoccur
  - (d) determining and implementing action needed
  - (e) recording results of action taken
  - (f) reviewing corrective actions taken
- (2) Records of the nature of the non-compliance and any subsequent action taken must be maintained in accordance with Part 5 of these Standards.

*Non-compliance, if not addressed may lead to a reportable event and/or further compliance action being taken by the SSBA Regulatory Scheme as defined by the NHS Act and NHS Regulations.*

*Refer to clause 2.2.3 for incident management.*

### 1.4.5 Preventive action

- (1) The entity must ensure action is taken to identify, through risk assessment or other sources, potential non-compliance to eliminate its causes and prevent occurrence or recurrence. Preventive action must be appropriate to the effects of the potential non-compliance and at a minimum include:
  - (a) determining the potential for non-compliance and its causes
  - (b) evaluating the need for, and implementing relevant action to prevent occurrence of non-compliance
  - (c) recording the results of actions taken
  - (d) reviewing preventive action taken

## Part 2 Risk and incident management

# 2

## 2.1 Objective

- (1) Entities must ensure that all known biosecurity risks in relation to the SSBA handled by the entity are identified and managed through risk assessment and risk management plans prior to commencement of SSBA related work.
- (2) Entities must ensure that the scope, nature and timing of the risk assessment is proactive rather than reactive and is kept up to date.

*Tier 1 SSBA's pose the highest biosecurity risk and are subject to the highest level of security and reporting, while Tier 2 SSBA's pose a high biosecurity risk and are subject to proportionately high security and reporting. The risks identified for Tier 1 versus Tier 2 SSBA's may therefore be different and the risk management plan should reflect these differences.*

*Entities should consider consulting the following documents regarding the risk assessment processes and the development of plans for managing risks:*

- *AS/NZS ISO 31000:2018 Risk management – Principles and guidelines*
- *SA HB 167:2025 Managing security related risks*
- *ISO 35001:2019 Biorisk management for laboratories and other related organisations*
- *WHO Laboratory Biosafety Manual, 4th Edition, 2020*

*The risk assessment and risk management plan processes are critical for managing the security requirements in the rest of these Standards. A Security Risk Template created to assist with risk assessment and risk management is available on the Australian CDC's website.*

*The risk assessment and risk management plan may be contained in one document.*

*Reactive risk assessment should take place following the occurrence of an identified risk or following the occurrence of a new risk previously not considered. See also clause 2.2.3.*

## 2.2 Hazard and risk identification, assessment, and management

### 2.2.1 Risk assessment process

- (1) The entity must undertake a thorough risk assessment process for each SSBA it handles. This process must be documented.
- (2) In undertaking the risk assessment, the entity must identify and assess the hazards and risks associated with handling each SSBA, and include (at a minimum):
  - (a) determination of the potential for and possible causes of an incident, including those listed as reportable events (as per s 48(1) of the NHS act)
  - (b) human behavioural risks (see also clause 3.9)

- (c) the location and strength of the SSBA secure perimeter, including physical access controls (see clause 4.2 and 4.3)
  - (d) periods of reduced staff availability (for example, during weekends and holiday periods)
  - (e) identify potential emergency situations involving SSBAs to:
    - i. prepare for their occurrence and to limit possible illness or other damage that may be associated with them
    - ii. ensure preparedness to enable an appropriate response to emergency situations both during and outside normal working hours, including the control of emergency access as appropriate and emergency exit routes to avoid evacuating personnel through areas of higher risk
    - iii. identify risks surrounding the safe removal, transport, treatment and accommodation of contaminated people or objects
- (3) Examples of potential hazards and risks to be included in the risk assessment are:
- (a) theft of SSBAs
  - (b) inadequate personnel screening
  - (c) loss of records required to remain secure (for example, inventories)
  - (d) infection or intoxication of personnel or visitors with an SSBA
  - (e) disgruntled personnel causing a non-compliance or theft of an SSBA or sensitive information associated with an SSBA
  - (f) inadequate access control and/or physical security allowing unauthorised access to SSBAs or secure records
  - (g) inability of the entity to properly account for the storage or handling of an SSBA
  - (h) loss of an SSBA during transport
  - (i) inadequate controls for sensitive information security, including cyber security capability
  - (j) an emergency or unforeseen event where there may be disruption to normal operating conditions
- (4) The risk assessment must also include the following at a minimum:
- (a) the internal and external security risk context, including communication and consultation plans with internal and external stakeholders
  - (b) analysis of the identified risks and the effectiveness of existing controls, including:
    - i. if action is needed to prevent occurrence of incidents
    - ii. effectiveness of physical security controls (see Part 4 of these Standards)
    - iii. effectiveness of the processes for decontamination/inactivation of contaminated and potentially contaminated items (see Part 7 of these Standards)
    - iv. identification of those responsible for devising, implementing and testing control measures
    - v. if further controls to reduce risk are required (see Risk management under clause 2.2.2)

- (c) It must address the need for adequate redundancy, replacement or other measures in the event of an emergency or unforeseen event where there may be disruption to normal operating conditions. This includes but is not limited to:
- i. alternative means of decontamination in the case of an autoclave failure
  - ii. maintenance of physical security systems in a power outage
  - iii. a complete secure shutdown of operations in extreme circumstances
- (5) For Tier 1 SSBAAs, a vulnerability analysis.

*Hazards and risks to be identified should include what can happen, when and where it can happen, and how and why it can happen. Australian Standard AS3745:2010 – Planning for emergencies in facilities may be useful as a reference guide.*

*The steps in the risk assessment process are illustrated in the flow diagram at Figure 1 (below).*

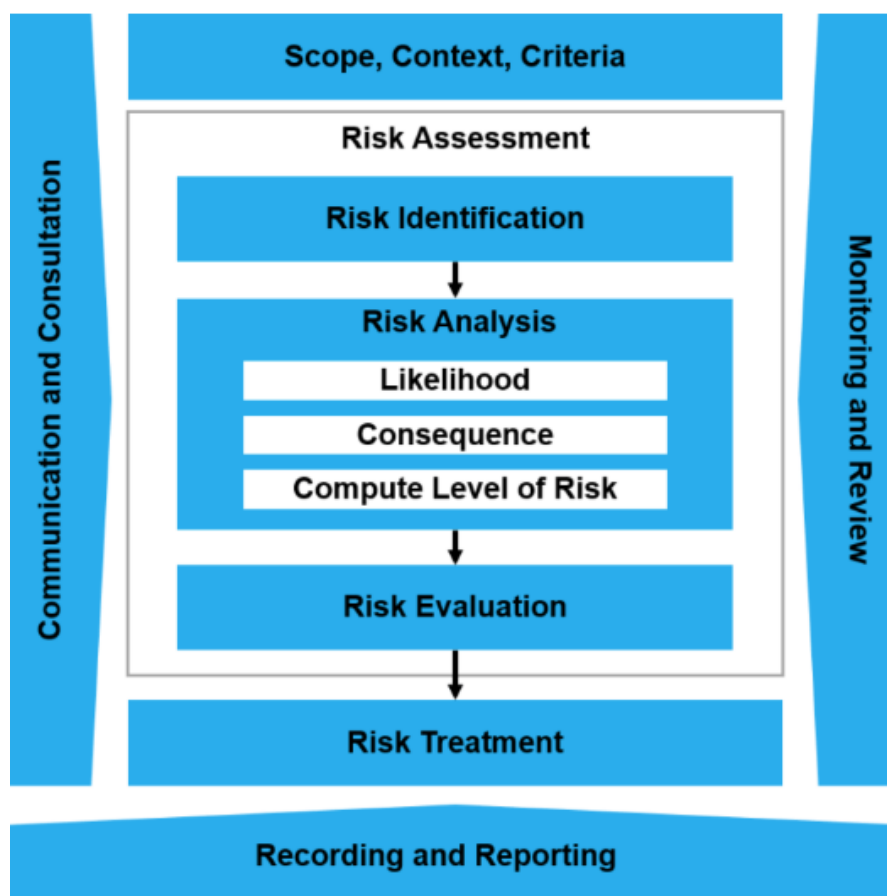


**Figure 1 - Illustration of the Risk Assessment process**

*The identified risks should be analysed by determining the likelihood and consequences of the risk occurring and identifying existing controls and their effectiveness. From this the level of risk can be determined and the risk management process undertaken, including the implementation of further controls if necessary. Professional advice may assist in risk assessment and the development of risk management plans, and the entity should balance the need for this advice against the need to keep the details of SSBA information restricted to those who have a need to know.*

*Communication and consultation plans should identify:*

- *Internal stakeholders - those who have a direct impact or are directly affected by the scheme - for example facility staff and management, contractors, clients, the SSBA Regulatory Scheme*
- *External stakeholders - those who have an interest in or peripheral role in the scheme - for example other laboratories in the organisation*

*Stakeholders are defined as those who may affect or be affected by the regulatory scheme.*

*Communication and consultation plans should include information about:*

- *The objectives of the communication, what information needs to be consulted on and with whom*
- *Timeframes*
- *The communication methods (e.g. formal documents, emails, newsletters, verbal communications etc.)*
- *Evaluations of the effectiveness of the communication*

*The external context for the purposes of the risk assessment includes the consideration of the external environment in which the entity operates, such as the general regulatory environment, and understanding the relationship between the environment, external stakeholders and the entity.*

*Defining the internal context includes documenting the key aspects of the business and may include defining the governance structure of the entity, resourcing issues and significant changes (for example new facilities) and the assumptions and constraints that the entity works under (in relation to SSBAs).*

*The security risk context relates to defining what influences the security environment within the entity. This may include the security culture present in the entity, type of SSBAs held, SSBA legislation (i.e. the NHS Act, NHS Regulations and SSBA Standards) and the type and location of the facilities handling the SSBAs.*

*The vulnerability analysis should be performed using guidelines found in HB 167:2025 Managing security related risks. A vulnerability is defined as any weakness that can be exploited to make an asset susceptible to change (HB 167:2025). A vulnerability analysis is the determination of how each credible threat can be realised against a critical asset.*

*Critical assets (in this case the SSBA and the sensitive information relating to the SSBA) are usually protected by several layers of security. Multiple layers of controls are aimed at preventing access if one layer fails. The layers might be physical security controls, access controls, staff selection and vetting, standard operating procedures, secure record controls, auditing and incident investigation and other layers of controls.*

*The vulnerability analysis looks at weaknesses in each of the layers of security and works out how they can be exploited, to identify gaps that need to be addressed. The vulnerability analysis does not look at what the consequences of the attack are, as this is conducted in the risk assessment. Vulnerability analyses should look at the most credible worst-case scenario, not the absolute worst-case scenario.*

## 2.2.2 Risk management plan

- (1) The entity must ensure a risk management plan is developed, documented and implemented, following the risk assessment. At a minimum, the risk management plan must include:
  - (a) treatment of the risks identified in clause 2.2.1
  - (b) plans for monitoring and review of the risk management process
- (2) The risk management plan must be effectively communicated to all personnel handling SSBA's or sensitive information relating to SSBA's and to others as relevant.
- (3) As part of the risk management plan, standard operating procedures (SOPs) for secure handling of SSBA's must be developed, documented and implemented.

*In treating risks, options for controlling the risks need to be identified, assessed and implemented. From this, treatment and implementation plans are prepared. Any residual risk is analysed and assessed with these treatment options in place, and a decision is made on whether the risks are reduced to a level where it is reasonable to proceed and monitor the risk, where additional controls need to be developed, or whether it is not secure to proceed. Controls that eliminate the risk are the most effective, followed by controls of an engineering or physical nature that cannot be modified by personnel. Management controls, which always depend on personnel compliance to work effectively, are the least effective controls to manage risk.*

*The areas of the risk management plan communicated to personnel and others should be those relevant to the activities undertaken and on a needs to know basis, for example risk management plans relating to decontamination should be related to all personnel handling SSBA's but would not need to be communicated to persons who are only handling sensitive information (such as information technology staff).*

*SOPs for the secure handling of SSBA's can be part of existing SOPs. SOPs may be developed at either the entity or facility level, as appropriate.*

*The risk assessment and risk management plans may be contained in one document.*

## 2.2.3 Incident management

- (1) The entity must establish, document and maintain procedures to define, report, record and analyse incidents involving SSBA's, including any non-compliance with the NHS Act, NHS Regulations and these Standards. Records of the nature of the incident and any subsequent action taken must be maintained as per Part 5 of these Standards.
- (2) This procedure must include:
  - (a) determining the cause(s) of incidents
  - (b) evaluating the need for corrective action to ensure that incidents do not reoccur
  - (c) determining and implementing the action needed
  - (d) recording results of action taken
  - (e) reviewing the effectiveness of the corrective action taken
- (3) The entity must put in place processes to encourage learning from incidents involving SSBA's.

*Procedures should be put in place to ensure that what constitutes an incident is clearly defined and communicated to all relevant personnel. This may include events of exposure and accidental release. An incident where no harm is caused may also be referred to as a “near miss”, “near hit”, “close call” or “dangerous occurrence”. Emergency situations are a particular type of incident.*

*Several types of incidents are defined by the NHS Act and the NHS Regulations as reportable events and must be reported to the Australian CDC and to jurisdictional law enforcement (if required by the NHS Act, the NHS Regulations or these Standards) as per the timeframes set out in the NHS Regulations (usually within 2 business days), and to any other appropriate authorities. The incidents that are required to be reported include:*

- *Unauthorised access or an attempt to access an SSBA or sensitive information relating to an SSBA*
- *Theft or attempted theft of an SSBA*
- *Accidental release of an SSBA*
- *Loss of SSBA's either from the facility or during transfer (e.g. the package does not arrive at the destination)*
- *A person is affected by an SSBA because of the entity's SSBA handlings*

*There is a broad scope of circumstances under which other incidents such as “near misses” can occur. Incidents that are not explicitly defined as reportable in the legislative framework, should still undergo a risk assessment and be notified to the Australian CDC via a voluntary incident report using the ‘other’ category. Examples of such incidents recommended for voluntary reporting may include, but are not limited to:*

- *Power outages*
- *Equipment failures or water leaks within the facility*
- *Natural disasters*
- *Violent or explosive equipment failure in or around the SSBA secure perimeter*
- *Events or situations that indirectly impact or affect the SSBA secure perimeter*

*Whether a defined reportable incident or an incident that is voluntarily reported, each should be addressed by corrective action and any investigative findings should be used to educate staff so they do not reoccur.*

## 2.3 Review

- (1) The entity must ensure that the risk assessment and risk management plans are reviewed at least every twelve months for risks involving Tier 1 SSBA's and every two years for risks involving Tier 2 SSBA's, or more frequently as required. Outcomes of the review must be documented.
- (2) Entities must undertake a review more frequently (i.e. more than every year or two years), in the following circumstances:
  - (a) following an incident
  - (b) when there are changes in SSBA's handled

- (c) when there are changes in procedures
- (d) when national threat levels change
- (e) at the request of the Australian CDC

*It is recommended that the review plan is included in the risk assessment and risk management document, with space for documentation of outcomes and sign off once the review is completed.*

*The risk assessment and management plans can be monitored through regular reviews, by utilising corrective action reporting processes where problems have been identified, by investigation of incidents, by improving controls and their implementation, and by ensuring that adequate resources are provided to maintain the effectiveness of the controls.*

*A complete review is not necessary when new personnel commence, but they should be made fully aware of the contents of the risk assessment and risk management plan and this should be recorded.*

## Part 3 Personnel

# 3

## 3.1 Objective

- (1) Entities must ensure they have personnel management systems in place to implement and manage the security of SSBA's and related sensitive information.

## 3.2 Responsible Officers

- (1) The entity must document top management's appointment of a Responsible Officer, who will oversee the SSBA management system and a Deputy Responsible Officer, who is able to assume the responsibilities and duties of the Responsible Officer. As part of this appointment, the duties of the Responsible Officer must include:
  - (a) reporting to top management on the performance of the entity's SSBA management system and any need for improvement
  - (b) overseeing internal review, audit and reporting measures to provide assurance that the requirements of these Standards are being met and maintained
  - (c) verifying, in conjunction with other relevant personnel, that all known SSBA risks have been addressed
  - (d) advising or participating in the reporting, investigation and follow-up of incidents, and, where appropriate, referring these to top management/ SSBA management committees (as defined under clause 1.3.2)
  - (e) ensuring that all work relating to SSBA's is conducted in accordance with established policies, the risk management plan, SOPs, the NHS Act, the NHS Regulations and these Standards
  - (f) advising top management as to whether staff levels, facilities and equipment are sufficient to effectively carry out work involving SSBA's in accordance with technical protocols, approved policies and SOPs
  - (g) any other responsibilities allocated under these Standards
- (2) The Responsible Officer and Deputy Responsible Officer must be authorised persons under clause 3.3.1 of these Standards, and have the necessary qualifications, training and technical understanding to meet their obligations under these Standards.

*The appointment of a Deputy Responsible Officer is in order to ensure continuity in this important oversight and leadership role.*

*Entities that have multiple facilities may appoint one Responsible Officer and one Deputy Responsible Officer for each facility or have a Responsible Officer and Deputy Responsible Officer who are responsible for multiple facilities.*

*Documentation regarding the appointment of Responsible Officers and Deputy Responsible Officers should include acknowledgment from Top Management that if the Responsible Officer or Deputy Responsible Officer develops the training materials required to meet clause 3.3.1, and have demonstrated a comprehensive knowledge of the materials, then these persons are deemed to have met this requirement themselves.*

## 3.3 Authorised persons

- (1) The entity must establish, document and implement processes to ensure that relevant personnel do not compromise the entity's SSBA security. The entity must authorise all unescorted or unsupervised persons in order for a person to:
  - (a) handle SSBA's
  - (b) access the facility where SSBA's are handled
  - (c) access sensitive information related to SSBA's (unless the person meets the requirements in line with clause 5.3.1 of these Standards)
- (2) The entity may authorise a person to do all of the above or limit the authorisation to any combination of the above.
- (3) A person's status as an authorised person is limited to the entity to which it is given and cannot be transferred between entities, as training procedures will be specific to that entity.
  - (a) for personnel who work in more than one entity or who move between entities, the results of NHS checks can be verified through AusCheck for the purposes meeting the requirements of clause 3.3 (see also clause 3.6)
  - (b) students must become either authorised persons or approved persons (see also clause 3.4), depending on the requirements of the facility before handling SSBA's
- (4) The entity must maintain a list of authorised persons. The list must include:
  - (a) the period for which the person is authorised
  - (b) the review date of the authorisation
  - (c) what they are authorised for
- (5) An entity must promptly revoke a person's authorisation if that person no longer has a need to handle SSBA's, access a facility where SSBA's are handled or access sensitive information relating to SSBA's (see also clause 3.10).

*An entity may choose to restrict a person's authorisation. For example, an information technology (IT) person may be authorised to access sensitive information about an SSBA but may not be authorised to access the facility where the SSBA is handled or the SSBA itself.*

### 3.3.1 Authorisation of a person

- (1) The entity must only authorise a person who:
  - (a) has completed training in the requirements listed under clause 3.9.1 as relevant to their authorisation (see also clause 3.3 for authorisation categories), and has provided a signed and dated record of the training to the entity
  - (b) has not been excluded from handling SSBA's by the entity nor directed not to handle SSBA's by the CDC
  - (c) is 18 years or over
  - (d) holds a current 'eligible' or 'qualified' NHS check result (see clause 3.6)

- (2) The entity must consider the results of the NHS check as part of the assessment of a person's eligibility to become an authorised person under clause 3.3.
  - (a) where the entity has used their judgement (to authorise or not authorise) a person with a 'qualified' rating, the reasoning for the decision must be clearly documented
- (3) If a person to be authorised has undergone an NHS check (clause 3.6) then the following requirements apply:
  - (a) if the person received an NHS check result of 'eligible', the entity may authorise that person for a period of up to two years. Following this period, the person must undergo a new NHS check before they can be re-authorised/maintain authorisation
  - (b) if the person received an NHS check result of 'qualified', the entity must not authorise the person for more than twelve months. Following this period, the person must undergo a new NHS check before they can be re-authorised/maintain authorisation
  - (c) if the person received an NHS check result of 'adverse', the entity must not authorise the person

*Even if a person receives an NHS check result of 'eligible' or 'qualified' it does not automatically mean that the person will become authorised if the entity decides they do not meet the criteria set for authorisation by the Standards and by any additional criteria set by the entity.*

*The entity may choose not to re-authorise a person until they have completed refresher training on the requirements of the NHS Act, NHS Regulations and the SSBA Standards.*

### 3.4 Approved persons

- (1) The entity must establish, document and implement processes to ensure that contractors, visitors, suppliers, students, non-employees and other such persons do not compromise the entity's SSBA security. These processes must include policies and procedures for the approval of persons who, unless a person is authorised, are required to:
  - (a) handle SSBA's
  - (b) access the facility where SSBA's are handled
  - (c) access sensitive information related to SSBA's
- (2) The entity may approve a person to do all of the above or limit the approval to one or any combination of the above.
- (3) For facilities handling Tier 1 SSBA's, approved persons must be escorted by an authorised person and remain in line of sight of their escort at all times.
- (4) For facilities handling Tier 2 SSBA's, approved persons must be supervised by an authorised person at all times. The degree of supervision and responsibility for an approved person by an authorised person must be determined and documented via the risk assessment.
- (5) The entity must maintain a list of approved persons. The list must include:
  - (a) the period for which the person is approved
  - (b) the review date of the approval
  - (c) what they are approved for

- (6) The entity must revoke a person's approval if that person no longer has a need to handle SSBA's, access a facility where SSBA's are handled or access sensitive information relating to SSBA's (see also clause 3.10).

*Escorted means that an approved person remains in line of sight of the authorised person escorting them while the approved person is within the secure area or handling sensitive information.*

*Supervision means that an authorised person is responsible for the approved person while they are within the facility or when accessing sensitive information.*

*When determining the degree of supervision for an approved person, the entity should consider factors such as the setup of the facility, the SSBA involved, the role of the approved person and the results of an NHS check (if undertaken).*

*For example, following the risk assessment it may be determined that where an approved person has access to locked storage facilities containing Tier 2 SSBA's, the authorised person (supervisor) should be in the facility at all times but does not need to have direct line of sight of the approved person. However, another approved person who requires access to the facility but does not have access to locked Tier 2 storage facilities, may be approved to enter the facility at times when the authorised person (supervisor) is not present in the facility, but is available nearby*

*An entity may limit a person's approval status. For example, a person may be approved to access a facility in which an SSBA is handled for the purposes of deliveries, but would not be permitted access to the SSBA or to sensitive information relating to the SSBA's, even when under escort or supervision by the authorised person.*

*Processes for approved persons should include how supervision may be handled in an emergency situation, for example if security personnel may need to enter a facility outside of working hours where an authorised person is not available.*

## 3.5 Provisional authorisation for new entities

- (1) The entity may provisionally authorise a person to become a Responsible Officer, Deputy Responsible Officer, handle SSBA's, access a facility where SSBA's are handled or to access sensitive information relating to SSBA's if:
- (a) the person is to commence an NHS check
  - (b) the requirements of paragraphs (a) to (d) of clause 3.3.1(1) have been met
  - (c) the relevant facility has no authorised persons (as under clause 3.3)
- (2) For an entity/facility that has not previously registered with AusCheck, an NHS check must commence within four weeks of notification by AusCheck that the entity/facility may begin submission of applications for NHS checks.
- (3) The entity/facility must cease a person's provisional authorisation upon receipt of the results of the NHS check.

*Provisional authorisations are temporary arrangements for newly registered entities to enable persons to handle SSBA's, access a facility where SSBA's are handled or access sensitive information relating to SSBA's, prior to receipt of the results of the NHS checks. Entities/facilities will not be able to apply for an NHS check until they have been informed by AusCheck that access has been provided to the required systems to allow the applications to be submitted. AusCheck will begin the process of provision of access to the application system following contact by the Australian CDC during the entity/facility registration process.*

*Persons who commence handling SSBA's, who access the facility where SSBA's are handled or access sensitive information relating to SSBA's in facilities that already have authorised persons in place may become approved persons (see clause 3.4) until the results of an NHS check have been received.*

## 3.6 National Health Security (NHS) checks

- (1) The entity must apply to AusCheck for an NHS check for all persons that it is considering authorising to:
  - (a) handle SSBA's
  - (b) access a facility where SSBA's are handled
  - (c) access sensitive information relating to SSBA's
- (2) An NHS check undertaken under this clause is valid for the entity that requested the check.
- (3) The entity must maintain policies and procedures to ensure that a person who has undergone an NHS check and who changes their name informs the entity of the change of name within 30 days of the change and provides appropriate documentation to support the change. This change of name must be reported to AusCheck within two business days of the entity being notified of the change.

*NHS checks are conducted via the Department of Home Affairs AusCheck scheme. they consist of a national criminal history check against the list of health security relevant offences set out in Appendix 1 of the SSBA Standards, and a national security assessment.*

*NHS checks cannot be performed on personnel who reside overseas, and therefore entities cannot authorise those persons to access sensitive information related to SSBA's. However, some persons may access sensitive information relating to SSBA's without undergoing an NHS check or holding a national security clearance (under clause 3.6.3) if they meet the requirements in line with Part 5 of these Standards.*

*NHS checks will be conducted based on the information supplied to AusCheck and will require the consent of the person to be checked. AusCheck will notify the relevant entity of the outcome of an NHS check. In the case of a potential qualified or adverse finding, AusCheck will also contact the individual and provide them with an opportunity to comment or provide additional information before a final decision is made. In these circumstances, AusCheck will also notify the individual of the final decision. Personal information, including criminal history information, will not be forwarded to the entity with one exception. If an individual receives a 'qualified' finding as a result of the criminal record check, an extract of the health security relevant offences is required, under the AusCheck Regulations, to be sent to the entity in order to assist the entity to make a decision about whether or not a person may become an authorised person.*

*Photographs supplied to AusCheck as part of the application process should be photographs taken by the entity for the purposes of security access cards or other such official photographs. Photographs cannot be supplied by the person undergoing the check.*

*Appropriate documentation for evidence of a name change may include marriage certificates, deed poll documents or a statutory declaration.*

*For more information on the requirements for submitting NHS checks under this scheme, visit [www.auscheck.gov.au](http://www.auscheck.gov.au).*

*If a person works in multiple facilities within an entity, an NHS check does not need to be undertaken for each facility as the results of the check are valid for any facility registered under the entity.*

*A guideline on conducting NHS checks is available on the Australian CDC's website.*

### 3.6.1 Transfer of NHS checks between entities

- (1) If a person who holds a current NHS check commences employment with an entity other than the entity that applied for the NHS check, the entity with which the person commences employment may accept the result of the NHS check for the purposes of clause 3.3.2.
- (2) If an entity decides to accept the result of a current NHS check undertaken by another entity, then the entity must contact AusCheck to verify the result of the check. The entity may only contact AusCheck after the person has given his or her consent to information regarding the result of the check being provided to the entity by AusCheck.

*If a person who works for more than one entity or who changes the entity they work for consents to an entity seeking information from AusCheck about the result of that person's NHS check at another entity, AusCheck will confirm if the person received a rating of eligible, not eligible or qualified but will not forward any personal information, including any information about criminal history, to the requesting entity. The exception to this is if the person received a qualified rating and in this case an extract of health security relevant offences will be provided to the entity to assist the entity to make a decision about if the person may become an authorised person.*

### 3.6.2 Reporting new convictions

- (1) The entity must have documented policies and procedures in place to require that:
  - (a) An authorised person who has undergone an NHS check must report any new convictions that is a kind of offence listed in Appendix 1 of these Standards to the entity and to Auscheck within two business days of being informed of the conviction
  - (b) the entity must inform AusCheck and the Australian CDC of the information reported under clause 3.6.3(a) above within two business days from being informed of the conviction
- (2) As soon as the entity is aware of a new conviction as reported above, the entity must suspend the person's authorised status pending the outcome of a new NHS check.

*Evidence of the conviction should be presented at the time of reporting to the entity to assist in informing AusCheck of the conviction. This evidence may include such things as charge sheets, court records or other such documents.*

*As part of a new NHS check following the reporting of a new conviction, AusCheck may approach the courts to confirm the details of the conviction. If a person's authorised status is suspended, the person may become an approved person to continue handling SSBA's, access the facility where SSBA's are handled or access sensitive information relating to SSBA's until the results of the new NHS check are received. The degree of supervision of the approved person in these circumstances should be determined by risk assessment and justifiable by the entity.*

### 3.6.3 National security clearance NHS check exemptions

- (1) The entity can authorise persons who currently hold a National security clearance (or equivalent) of Negative Vetting Level 1, Negative Vetting Level 2 or Positive Vetting to:
  - (a) handle Tier 1 SSBA's
  - (b) access a facility where Tier 1 SSBA's are handled
  - (c) access sensitive information relating to Tier 1 SSBA's
- (2) Entities must only authorise National security clearance holders as listed above if their clearance status has been verified by the Australian Government Security Vetting Agency (AGSVA), Department of Defence, and the persons do not have a criminal record against the list of health security relevant offences as set out in Appendix 1 of these Standards. The entity must document this confirmation.
- (3) National security clearance holders as listed above can be considered to have received a result of 'eligible' as per clause 3.3.1, and a review of the currency of their clearance must be conducted in line with the requirements of that clause and documented by the entity.
- (4) The entity must have in place policies and procedures to ensure that a person with a relevant national security clearance as listed above who changes their name, informs the entity of the change of name within 30 days of the change and provides appropriate documentation to support the change. The entity must notify the Department of Defence of this name change within two business days of the entity being notified of the change.

*Due to the nature of national security clearances, persons who hold a current national security clearance of Negative Vetting Level 1, Negative Vetting Level 2 or Positive Vetting are taken to have satisfied the requirements for clause 3.3.2 and do not have to undergo an NHS check.*

*National security clearances are managed by the AGSVA within the Department of Defence. For further information, visit the AGSVA website at [www.defence.gov.au/agsva](http://www.defence.gov.au/agsva).*

## 3.7 Recruitment

- (1) The entity must ensure that the identity, qualifications and experience of all persons recruited for the purpose of handling SSBA's are assessed and deemed suitable as part of the recruitment process.

*It is an offence under the Migration Act 1958 for a person to knowingly or recklessly allow an illegal worker to work or to refer an illegal worker for work with another business, and it is the responsibility of the employer to ensure that they comply with their obligations in this area. Further information on the requirements of employers in regard to checking a person's work entitlements and visa conditions can be obtained from the [Department of Home Affairs](http://www.dhs.gov). The following sources may be used (where authorised by law) to check the staff being recruited.*

*Integrity:*

- Curriculum vitae to ensure that there are no unexplained gaps or anomalies

- *Character references for a minimum of five years, including persons to whom the applicant reported directly*

*Credentials:*

- *Verify the applicant's declared academic and professional memberships*
- *Reference checks, up to five years previous employment history*

*Other checking as identified by the risk assessment should be undertaken. Where authorised by law and appropriate, checks may include a person's financial probity or membership of groups hostile to biological research.*

*AS 4811:2022 Workforce screening should be consulted for guidance on staff recruitment. Some checks will require consent from the applicant.*

## 3.8 Training and competency

- (1) The entity must ensure that all personnel who have responsibilities or perform tasks that may impact on SSBAs, have appropriate education, training and experience, and are provided with adequate and up-to-date information pertaining to the entity's identified SSBA risks.
- (2) The entity must ensure that requirements and procedures for SSBA related training of personnel are established, documented, implemented and maintained. At a minimum, training and competency requirements must include:
  - (a) defining SSBA related training needs
  - (b) provision of required SSBA training
  - (c) determination of the effectiveness of SSBA training
  - (d) provision of SSBA refresher training
- (3) Restrictions on staff to ensure they do not perform tasks for which they are not trained.
- (4) The entity must put in place mechanisms to ensure that relevant and timely information is available regarding SSBAs as they affect personnel, and promote an awareness of the potential external and internal risks associated with unauthorised access to these agents.

*Training should include raising personnel awareness of security issues associated with SSBAs, including the relevance of human factors in SSBA management. Training in hazard identification, risk assessment, risk management and vulnerability analysis should be provided where appropriate.*

*Learning outcomes from management of incidents should be included in personnel training.*

*If the Responsible Officers and Deputy Responsible Officers are responsible for developing the training materials for clauses 3.9 and its subclauses, then Top Management should include in the appointment documentation for these officers that these persons are deemed to have met the training requirements themselves.*

*Technical competency is taken to mean that the personnel have worked at the Physical Containment Level (AS/NZS 2243.3:2022) for the relevant risk group of the SSBA and have demonstrated competency in the procedures required at that level.*

### 3.8.2 Training for authorised persons

- (1) For the purposes of authorising persons under clause 3.3 training must, at a minimum, include:
  - (a) for all authorised persons:
    - i. an overview of the NHS Act and Regulations, the SSBA Standards and why the SSBA Regulatory Scheme is in place
    - ii. reporting requirements, including what constitutes reportable events as defined under the NHS Act and Regulations, as well as incidents as specifically defined by the entity
    - iii. records management
  - (b) For persons who will handle SSBA's, the requirements of the:
    - i. NHS Act
    - ii. NHS Regulations
    - iii. all parts of the SSBA Standards
  - (c) For persons who will access the facility where SSBA's are handled, the following parts of the SSBA Standards:
    - i. Part 1 – SSBA Management System
    - ii. Part 2 – Risk and Incident Management
    - iii. Part 3 – Personnel
    - iv. Part 4 – Physical Security
    - v. Part 5 – Information Management
  - (d) For persons who will access sensitive information relating to SSBA's, the following parts of the SSBA Standards:
    - i. Part 1 – SSBA Management System
    - ii. Part 2 – Risk and Incident Management
    - iii. Part 3 – Personnel
    - iv. Part 5 – Information Management
- (2) The above training must include how the SSBA Standards are implemented in each facility and must include specific training in the requirements of the entity and facility in relation to SSBA's, such as policies and procedures for handling SSBA's and sensitive information, requirements for supervision or escorting approved persons etc.
- (3) Training for personnel handling Tier 1 SSBA's must include personal security awareness.
- (4) Entities may choose to impose further training requirements on each category of authorisation.

*Training for the SSBA Regulatory Scheme does not mean that all persons need to know all the details of the NHS Act, NHS Regulations and the SSBA Standards. Training can be tailored to the specific role the person has in the entity, for example, IT personnel will need to be trained in the requirements listed for accessing sensitive information but would not need to be trained in the requirements regarding transport of SSBA's.*

*The SSBA Regulatory Scheme provides training information to assist personnel to understand the legislative requirements. This training does not include entity and*

facility specific information, such as policies and procedures, and does not include a determination of competency levels. Training by the entity is important to ensure understanding of how the requirements of the SSBA Regulatory Scheme and the entity's own policies and procedures apply to the facility and to the handling of SSBA's. Information about this training material can be obtained by contacting the SSBA Regulatory Scheme at [ssba@cdc.gov.au](mailto:ssba@cdc.gov.au).

Personal security awareness refers to staff security during off-duty hours away from the facility. During these times, staff members may be vulnerable because of their function or position.

Note that assessment of personal security should be part of the risk assessment and risk management plan.

A program of briefing authorised persons on potential risks associated with their role and provision of advice on how to handle and report situations of concern should be put in place. Advice could be sought from the Commonwealth, State and Territory police on the content of this program.

Training for personnel handling Tier 2 SSBA's may also include personal security awareness.

### 3.8.3 Competency Levels

- (1) The entity must define required competency levels, including the appropriate technical competencies to handle SSBA's for those authorised to do so. The entity must maintain records verifying that personnel have attained and continue to demonstrate the defined levels of competency.
- (2) For facilities handling Tier 1 SSBA's, competencies of authorised and approved personnel must be reviewed at least annually. For facilities handling Tier 2 SSBA's, competencies of authorised and approved personnel must be reviewed at least every 2 years. Competencies must also be reviewed in response to changes in risk assessment, risk management, SOPs or following an incident or changes to the NHS Act, NHS Regulations or SSBA Standards.

Technical competency is taken to mean that the personnel have worked at the Physical Containment Level (AS/NZS 2243.3:2022) for the relevant risk group of the SSBA and have demonstrated competency in the procedures required at that level.

## 3.9 Behavioural factors

- (1) The entity must establish and implement measures to address risks associated with human behaviour, including reliability, of persons who handle SSBA's, access a facility where SSBA's are handled or access sensitive information relating to SSBA's.
- (2) These measures must be documented as part of risk assessment and management processes, and evidence of their application recorded.

Managing behavioural issues is one of the most difficult areas but it is also one of the most important. One of the risks with handling SSBA's is the possibility of a "trusted insider" accessing the SSBA's for a non-legitimate purpose.

The entity should ensure that factors associated with behaviours and the need for individual support and communication are managed responsibly, both to protect workers from direct hazards and to ensure they can function optimally within the

facility. Many incidents are caused by inappropriate behaviour or human error, and a preventive and proactive approach to managing risk associated with the individual should be pursued, including the specific inclusion of such issues in risk management. The use of experts in assessing this area should be considered.

Measures should be put in place to address:

- Human reliability and behavioural safety and security, including adherence to procedures
- Communications, consultation and feedback
- Conflict management and resolution
- Empowerment, including authority to stop work if potentially non-secure conditions are identified
- Avoidance of “blame culture”, including willingness to report incidents and non-secure conditions/behaviours, and protection of personnel who do so
- Respect for individual privacy and dignity

Safe Work Australia’s Model Code of Practice: Managing psychosocial hazards at work ([www.safeworkaustralia.gov.au](http://www.safeworkaustralia.gov.au)), may be consulted for further guidance on personnel reliability policies and management.

The nature and extent of the personnel reliability assessment measures required should be determined as part of the risk assessment process. In some instances, few checks may be required other than collection of employment references, whereas in others, more in-depth screening may be deemed necessary. The nature and extent of the personnel reliability assessment measures required should be determined as part of the risk assessment process

A guideline on Indicators of Suspicious Behaviour in Laboratories Handling SSBA is available on request from the Australian CDC (email: [ssba@cdc.gov.au](mailto:ssba@cdc.gov.au)).

## 3.10 Exclusion

- (1) The entity must establish, document and implement 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 SSBA from the Australian CDC.
- (2) The measures must include:
  - (a) prompt removal of access to the facility (for example, removal/deactivation of passes and change of keys, access codes and other security devices)
  - (b) prompt removal of access to any SSBA held in linked storage units (see Part 4)
  - (c) prompt removal of access to sensitive information relating to SSBA
  - (d) suspension or revocation of a person’s authorised or approved status
  - (e) immediate physical removal of personnel if deemed necessary

The exclusion could be because of non-compliance or assessed risks associated with the NHS Act, the NHS Regulations or these Standards.

Wording should be included in employment contracts to enable exclusion of personnel.

# Part 4 Physical security and Storage

# 4

## 4.1 Objective

- (1) Entities must ensure they have physical security measures in place, based on requirements identified in the risk assessment and risk management plan, to minimise the risk of unauthorised access to SSBA's.

*SSBA's are variable and might be found in different formats such as cultures, powders, specimens/samples and potentially contaminated materials.*

*Consultation with local State or Territory Police Counter-terrorism and Infrastructure Protection branches is recommended.*

*Care should be taken to coordinate physical security measures with those of biosafety to minimise conflicting requirements.*

## 4.2 Perimeter

- (1) Each facility must have a clearly defined secure perimeter that fully encloses the area where SSBA's are handled.
  - (a) external walls that form part of the secure perimeter must be of solid construction and physically sound
  - (b) external doors of the secure perimeter must be self-closing and suitably protected against unauthorised access with control mechanisms
  - (c) windows must be non-opening and sealed at all times
- (2) In addition to access controls as described in clause 4.3, doors that form part of the secure perimeter must be locked when the facility is unattended.
- (3) Unauthorised recording, photography or filming must be prohibited within the secure area. Policies on this prohibition must be documented.

*The location and strength of the secure perimeter should depend on the security requirements of the SSBA's contained within and the results of risk assessment as per clause 2.2.1. To ensure that the exact location of the secure perimeter is understood, the entity should use a marked floor plan to assist in defining it. This floor plan should be kept with other sensitive information.*

*When defining the secure perimeter for a facility, the entity should consider that all personnel with access to the secure perimeter must be either an authorised or approved person and is subject to the requirements of the NHS Act and Regulations. Where possible, it is recommended that the secure area be limited in size to assist with access control. A staffed reception area or other means (for example, bars or locks) to control physical access to the secure area should be in place.*

*Intruder detection systems should be installed to Commonwealth, State or Territory standards and regularly tested to cover all external doors and accessible windows. Unoccupied areas should always be alarmed. The extent of the requirement of these intruder detection systems should be determined by the entity and be justified via the risk assessment requirements under clause 2.2.1*

*The use of multiple barriers gives additional protection, in that the failure of a single barrier does not mean that security is immediately compromised.*

*There are a wide range of standards and requirements that relate to physical security. Guidance can be sought from State or Territory Police Counter-terrorism*

and Infrastructure Protection branches, the Protective Security Policy Framework or professional security consultants.

*Video monitoring of access points should be considered for Tier 1 SSBA, subject to risk assessment and risk management plans. Appropriate video monitoring of access points and within the secure area should be maintained both for security and safety reasons with the monitoring requirements determined on the basis of the risk assessment. Constant monitoring of the video screens is not needed unless indicated by the risk assessment. It provides a record for later review, in case of an intrusion or incident.*

*For the physical security requirements for linked storage units, see clause 4.8.1.*

## 4.2.1 Stand-alone facilities

- (1) Stand-alone facilities are subject to additional risks, especially relating to access and security. A facility that is a stand-alone facility as defined by these Standards must also meet the following requirements. The facility must:
  - (a) be installed with a back-to-base alarm system
  - (b) be fixed in place and not able to be transportable
  - (c) have barriers to prevent vehicles from approaching the facility
  - (d) have good external lighting
  - (e) be regularly inspected to ensure that the outer walls have not been tampered with. Outcomes of these inspections must be documented
- (2) Mobile laboratories, such as police forensic mobile laboratories are not subject to the requirements of this clause.

## 4.3 Physical access controls

- (1) Access to secure perimeters containing SSBA must be restricted to authorised persons and approved persons. At least one form of access control must be at the secure area perimeter.
- (2) An additional form of access control must be used to further control unauthorised access to Tier 1 SSBA.
- (3) Effective measures, determined by risk assessment, must be put in place to prevent 'tailgating'.
- (4) Access control must ensure that details, including identification of the person and the date and time of access, are recorded for all persons:
  - (a) entering the secure perimeter
  - (b) accessing the secondary access control to a Tier 1 SSBA
  - (c) for facilities handling Tier 1 SSBA, the time of exit from the secure perimeter (specific to the person) must also be recorded
- (5) Access control records must be kept in line with Part 5 of these Standards.
- (6) Testing of access control systems must be implemented by the entity and in line with the methods outlined in the risk assessment. Entities must perform the testing:
  - (a) At least every 6 months for Tier 1 SSBA

(b) At least annually for Tier 2 SSBA's

- (7) The loss of any access cards, keys or other items used to access the secure areas must be reported immediately to the Responsible Officer once the loss is known and measures taken to ensure that they are not used. Reports of loss or theft of access controls (swipe cards, keys etc.) and the actions taken must be documented.
- (8) If a person no longer requires access to the secure area, the entity must ensure that access to the area is removed (for example, by deactivation of card access or returning of keys).

*“Tailgating” refers to one or more additional persons accessing a facility by entering on the access code of the original person, such as when two or more people enter through a controlled door using only one access card. This could be controlled by using physical barriers such as a turnstile or by using a monitoring system that will detect the entry of more than one person on a card authorisation and generate an alarm. Exit control and recording should be by a pass back control reader on the secure side of the access door.*

*For safety reasons, the exit control should be able to be overridden for emergencies and an alarm generated to indicate an unauthorised exit. Any triggering of the alarm should be subject to an incident report and investigation. Risk assessment will determine how access is handled in emergencies (see clause 2.2.1). These documented policies should be communicated to all relevant personnel, including contractors such as security guards.*

*Examples of additional forms of access control include biometric readers or keypads with individual PINs.*

*The additional access control to further control access to Tier 1 SSBA's does not have to be at the secure perimeter but may be within the secure perimeter itself. The second access control may be at the last physical barrier to the SSBA. For example, if the SSBA is stored in vials kept on a shelf of a freezer, then secondary access controls might be on the freezer door.*

## 4.4 Storage

- (1) Entities must ensure that SSBA's are stored securely to reduce the risk of unauthorised access.

*Secure storage may include storing SSBA's in a dedicated locked freezer, a dedicated locked liquid nitrogen storage tank or locked containers within these devices.*

## 4.5 Working cultures and toxin extracts

- (1) The entity must document and implement policies and procedures to:
  - (a) track the creation of working cultures derived from SSBA's held in long term storage
  - (b) track and control the distribution of working cultures and toxin extracts of SSBA's
- (2) The entity must record details about:
  - (a) who has access to working cultures and toxin extracts
  - (b) who has accessed cultures and toxin extracts in storage for the creation of working cultures and toxin extracts, including:
    - i. why working cultures and toxin extracts were accessed
    - ii. where they are being handled
- (3) The exact amounts of SSBA taken or used is not required to be recorded

*Access control requirements for working (active) SSBA's will be determined as part of the risk assessment.*

*The entity is not required to record exact amounts of SSBA taken or used, but rather details about who has accessed cultures and toxin extracts in storage for creation of working cultures and toxin extracts, who has access to working cultures and toxin extracts and where they are being handled.*

*Similar to inventory controls, the entity should be able to provide information on where the cultures and toxin extracts are and approximately how much is in existence (for example, by logging the number of plates or vials that are created or destroyed). As such, the process that the entity may put in place to control, track and record working cultures and toxin extracts could be similar to that which is used to manage the facility's inventory. Entities should align the amounts of SSBA held with the purpose for handling to assist in the reduction of risk of unauthorised access to the agent.*

## 4.6 SSBA inventory

- (1) The entity must establish and maintain an accurate and current inventory of any SSBA's held in storage.
- (2) The inventory must identify and document which SSBA's are held by the entity and the location of each of the storage containers of the SSBA's.

- (3) The entity must ensure that measures are put in place to minimise the quantities of SSBA stored.

*Inventory records are not intended to capture working cultures where the sample size may change on a day-to-day basis. In documenting the location of SSBA storage containers, entities should document more specific SSBA location information such as the rack, shelf or box number.*

*The nature of the inventory and associated controls should be based upon risk assessment and should include an assessment of the nature of the material held, including if the SSBA is Tier 1 or Tier 2, and the risk of harm should it be misplaced, lost, stolen or if there is unauthorised access.*

*There is less risk when the range and amount of SSBA are kept to a minimum. When work on a particular SSBA is no longer required, the SSBA should be disposed of, either by transfer or destruction.*

## 4.6.1 Audit of inventory

- (1) The entity must ensure that audits of the SSBA inventory are conducted at predetermined intervals as determined through risk assessment outlined in clause 2.2.1.
- (2) Audits must be frequent and thorough enough to ensure all materials are fully accounted for. Additional audits are required in the following circumstance:
  - (a) following an incident directly involving SSBA inventory
  - (b) when there are changes in SSBA handled, including transfer to new storage areas, changes in responsible persons for inventory, or changes in the risk assessment or threat level
  - (c) at the request of the Australian CDC
- (3) The results of audits must be documented.

*The level, detail and frequency of inventory audits will be unique to each entity and vary based on the specific requirements of facilities and SSBA handled. Timing and procedures established*

*for the audit should align with the reasoning and justification outlined in the risk assessment as required in Part 2 of these Standards.*

## 4.7 Storage of Tier 1 SSBA

- (1) The entity must only store Tier 1 SSBA within the secure perimeter (as defined under clause 4.2) of a registered facility.

## 4.8 Storage of Tier 2 SSBA

- (1) The entity may store Tier 2 SSBA in a storage unit that is located within the secure perimeter of the facility (as defined under clause 4.2), or within a storage unit that is linked to the facility (see clause 4.8.1).

- (2) The entity must ensure that the Tier 2 SSBA's are only handled in the linked storage unit for the purpose of storage or preparation for storage.
- (3) If a storage unit is linked to the facility, then it must be:
  - (a) located within the same building as the facility, preferably on the same floor
  - (b) included as part of the registration of the facility
  - (c) included in the risk assessment and risk management plans for the facility
  - (d) fixed in place or non-transportable

#### 4.8.1 Access to a linked storage unit

- (1) Access to the SSBA within the storage unit must be restricted to Authorised or Approved persons and all access must be recorded. Access records must include the identification of the person, the date and time of access, and if any of the SSBA was removed.
  - (a) the point at which access is recorded must be at the final access control barrier to the SSBA
- (2) Records of access must be kept in line with Part 5 of these Standards.
- (3) The loss of any access cards, keys or other items used to access the storage unit must be reported immediately to the Responsible Officer once the loss is known and measures taken to ensure that they are not used. Reports of loss or theft of access cards, keys etc. and the actions taken must be documented.
- (4) If a person no longer requires access, the Responsible Officer must ensure that access is removed (for example by deactivation of card access or returning of keys).
- (5) Storage units that are easily transportable, such as locked boxes or wheeled cabinets, must be secured to a larger structure to prevent easy removal.

*If an SSBA is stored in vials kept on a shelf in a freezer and the access controls are on the freezer door, then all access to the freezer should be recorded, regardless of if the person was accessing the SSBA or not. As the freezer door is the last point of access control, all persons accessing the freezer would need to be authorised or approved. However, if the SSBA is stored within the freezer in a locked box that cannot be easily removed and the keys only held by authorised/approved persons, then access would be recorded when personnel open the locked box. In this second scenario it is not necessary to authorise or approve all persons accessing the freezer or to record all access to the freezer itself.*

#### 4.8.2 Transport from and to a linked storage unit

- (1) Transport of SSBA's between the linked storage unit and the registered facility is subject to the transport requirements of clause 6.4 of these Standards.

- (2) The entity must record all transport of SSBA's between the linked storage unit and the registered facility but does not need to report these movements to the Australian CDC.

## 4.9 Record keeping

- (1) The entity must ensure that records relating to the storage, inventory, and transport of SSBA's, are current, complete, and stored securely with adequate backup. These records must be kept in accordance with Part 5 of these Standards.

# Part 5 Information management

# 5

## 5.1 Objective

- (1) Entities must ensure that information, including sensitive information, relating to the security of SSBA is current, complete, and stored securely.
- (2) Entities must be aware of their responsibilities under the NHS Act, including the requirements to make records available for the purposes of inspections.

*Information generated by a facility can be as valuable or dangerous as stored SSBA. Adequate measures to prevent the unauthorised release of such information are critical to biosecurity.*

## 5.2 Record keeping

- (1) The entity must maintain records of all activities related to these Standards, including:
  - (a) receipt
  - (b) holding
  - (c) transport
  - (d) disposal
  - (e) decontamination and inactivation
  - (f) policies and procedures, including authorisation and training
  - (g) internal and external reviews, including audits
  - (h) inspections
  - (i) incident investigations
  - (j) risk assessment and risk management plans
- (2) Records for SSBA must be kept for a minimum of 5 years unless otherwise specified in these Standards.
  - (a) records for staff must be kept for as long as staff remain in the entity
- (3) The entity must develop and document policies for accessing, retaining and destroying records, including timeframes, consistent with these Standards.

*Disposal records are records of the complete transfer or destruction of the SSBA and should not be confused with records of decontamination/inactivation and validation. Handling of these records is defined under clause 7.4.*

*Entities should be aware of other legislation related to the storage of records. For example, If the entity is a Commonwealth agency, records it holds or has control over will be subject to the provisions of both the Commonwealth Freedom of Information Act 1982 (FOI Act) and the Archives Act 1983 (Archives Act). It will also be subject to the provisions of the Information Privacy Principles (IPPs) contained in the Commonwealth Privacy Act 1988 (Privacy Act).*

*If the entity is an agency of a State or Territory, it will not be subject to the provisions of the FOI Act or the Archives Act, but it may be subject to similar legislation in the relevant jurisdiction.*

*If the entity is a private sector body (which can include an individual person, a body corporate, a partnership, an unincorporated association or a trust) it will be an*

*'organisation' for the purposes of the Privacy Act if its annual turnover is \$3 million or greater and it will, accordingly, be required to comply with the Australian Privacy Principles (APPs) contained in the Privacy Act.*

## 5.3 Information security

### 5.3.1 Sensitive information

- (1) The entity must identify and document what is considered by the NHS Regulations as sensitive information relating to the security of SSBA's.
- (2) A review and approval process must be used to control access to such information and be limited to those who need to know and have been permitted such access by the entity.
- (3) Access permissions must be reviewed at least every 6 months for entities handling Tier 1 SSBA's and at least annually for entities handling Tier 2 SSBA's. Outcomes from the review must be documented.
- (4) Sensitive information relating to Tier 1 SSBA's must be stored in a secure system and securely backed up at regular intervals.
- (5) At a minimum, procedures addressing sensitive information security must address:
  - (a) secure storage of all sensitive records, including electronic records and electronic signatures
  - (b) strict policies regarding the on-site security of equipment such as PCs, laptop computers, storage media, cameras, mobile phones, as well as the security of equipment entering and leaving the facility
  - (c) destruction of unwanted paper files and complete erasure of unwanted electronic files
  - (d) adequate backup strategies for sensitive electronic data, including keeping backup copies in secure environments, either within the entity or externally

*Sensitive information is defined under the NHS Regulations as:*

- *The entity's storage records for the SSBA's handled at the facility*
- *The entity's risk assessment and risk management plans for the SSBA's handled at the facility*
- *Any other information that the entity identifies as being sensitive information because it could compromise the security of the SSBA's handled at the facility*

*When determining additional sensitive information under the NHS Regulations, the entity should consider if the release of the information may assist someone to gain unauthorised access to the SSBA, to the facility or to further sensitive information. Records that may be considered sensitive information could include:*

- *Marked floor plans of the secure perimeter*
- *Lists of authorised and approved persons (as this can identify who has access)*

- Lists of access codes or key numbers
- Information relating to submission of NHS checks
- Incident reports that may indicate vulnerability in the security of an SSBA

*While records of research and diagnosis and other legitimate uses may not need to be considered sensitive information, entities should consider whether information is to be released, who will have access to the information and how it may impact on the security of the SSBA.*

*Review of permissions should include checking that the persons authorised to access the sensitive information still have a need to know and a need to access. It is not necessary to review each occasion that sensitive information is accessed, unless warranted by the risk assessment.*

*ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection should be consulted to assist the entity in developing its guidelines.*

*See clause 1.4.2 of these Standards for more information regarding records, documentation, and data control.*

## 5.3.2 Cyber Security

- (1) The entity must implement strategies to mitigate cyber security incidents on systems that hold sensitive information.
- (2) The entity must, via risk assessment, be able to identify and demonstrate a minimum level of cyber security capability to ensure:
  - (a) all access to systems which manage information security of sensitive information are isolated or have controls that permit only authorised persons
  - (b) authorised persons are only granted access to sensitive information, files, equipment (for example servers or mass storage devices) and applications as necessary to fulfill their roles and responsibilities
  - (c) controls are in place that are designed to prevent malicious code (such as computer viruses, worms and spyware) from compromising the confidentiality, integrity, or availability of sensitive information
  - (d) a management practice for information systems to include regular patching and updates of software and applications

*While no set of mitigation strategies are guaranteed to protect against all cyberthreats, the Australian Signals Directorate (ASD) has developed [Strategies to mitigate cybersecurity incidents](#), to help organisations protect themselves against various cyberthreats and to protect their internet-connected information technology networks.*

*Entities should familiarise themselves with ASD's guidance and develop, review and update their processes and procedures based on current ASD guidance.*

## 5.3.3 Provision of sensitive information to other regulatory authorities

- (1) The entity may provide information deemed as sensitive information under the *National Health Security Regulations 2018* (see clause 5.3.1) and any other information deemed as sensitive by the entity, to persons from

regulatory authorities, who are not authorised or approved persons, if required to do so for the purposes of complying with or providing evidence of compliance with another regulatory scheme.

(2) Regulatory authorities include:

- (a) the Office of the Gene Technology Regulator
- (b) the Department of Agriculture, Fisheries and Forestry
- (c) federal, state or territory law enforcement
- (d) any other authority approved in writing by the Australian CDC

(3) Sensitive information may only be provided under the following conditions:

- (a) the regulatory authority has a need to know of the information for their regulatory purposes
- (b) the regulatory authority is able to hold the information at the PROTECTED security level (or equivalent) or higher
- (c) measures are put in place to limit the amount of sensitive information released to only information that the authority has a need to know

(4) The entity must document what information is provided to the regulatory authority.

*An entity may be required to provide evidence of compliance with other regulatory schemes and the Regulatory Officer may request to keep copies of documents provided for this purpose.*

*When using this clause, the entity should determine if, as an alternative, the information can be de-identified or have the sensitive information removed, or if the Regulatory Officer can sight the information at the entity rather than take copies for their records.*

*The PROTECTED security classification under the Australian Government Protective Security Policy Framework involves:*

- *Persons accessing information holding a Baseline Vetting security clearance*
- *Storing information in a PROTECTED classified file*
- *Storing information in a Class C container or, at a minimum, a lockable container*
- *Destroying information using a Class B shredder*

## 5.4 Disposal of records

(1) The entity must ensure that there are documented policies and procedures in place for the appropriate disposal of records and sensitive information, consistent with the requirements of clause 1.4.2, and Parts 2 and 5 of these Standards.

*Disposing of sensitive information or records does not always mean it is destroyed. Appropriate disposal can mean that records and sensitive information are destroyed, transferred (to a new owner or custodian) or altered.*

*Destruction methods may vary depending on the type of information and its sensitivity. Examples of destruction for physical records can include physical destruction via shredding, pulping, burning, pulverisation or disintegration. Examples of destruction for digital information can include overwriting, purging, erasing or degaussing.*

*For more information on the appropriate disposal of records and sensitive information, visit the National Archives of Australia website at [www.naa.gov.au](http://www.naa.gov.au).*

## Part 6 Transport

6

## 6.1 Objective

- (1) Entities must ensure they have policies and procedures in place for the secure movement of SSBA's.

*Policies and procedures should cover all relevant forms of transportation of the SSBA, including walking an SSBA to another facility. The transportation of SSBA's is considered a high-risk activity. Policies and procedures should mitigate all risk for all forms of transportation of SSBA's to a very low level, including addressing how the security and containment risk for SSBA's will be appropriately managed whilst they are being transported between facilities.*

*These Standards apply to the transport of SSBA's within Australia. DAFF manage the importation of goods into Australia, including SSBA's. Imports of SSBA's will require an import permit from DAFF.*

*Certain SSBA's, such as imports of ricin, require a permit from the Australian Safeguards and Non-Proliferation Office under the provisions of the Customs (Prohibited Imports) Regulations 1956 and the Chemical Weapons (Prohibition) Act 1994. Exports of SSBA's may require a permit from the Department of Defence (Defence Export Controls) if the SSBA is contained on the Defence and Strategic Goods List under the Customs (Prohibited Exports) Regulations 1958).*

## 6.2 Transport

### 6.2.1 Transport requirements for a sending facility

- (1) The entity responsible for the sending facility must ensure that the facility:

  - (a) has documented policies and procedures in place to ensure compliance with Commonwealth, State and Territory legislation governing the transport of biological and toxin agents
  - (b) ensures that the receiving facility will accept the shipment prior to dispatch of the agent. A record must be kept of this acceptance
  - (c) notifies the receiving facility of the shipment details (such as the waybill, consignment note or tracking number, together with details of the transport agent and the expected time of delivery) at the time of shipment
  - (d) immediately informs the Australian CDC and State/Territory police if the shipment is lost, stolen (once the entity is aware of the loss or theft) or if the shipment is reported as an unsuccessful transfer (see clause 6.2.2) by the receiving facility (once the entity is aware of the unsuccessful transfer)

*It is recommended that Responsible Officers from each facility are included when transport agreements are being made. The sending facility should contact the receiving facility within a maximum of two business days after the expected delivery time to ensure the shipment has been received if it has not already received confirmation from the receiving facility.*

*The transport of SSBA's by air is covered by the Civil Aviation Safety Regulations 1998 and by road and rail by the Australian Dangerous Goods Code for Road and Rail, as incorporated by each State and Territory in relevant legislation.*

*Air transport consistent with the International Air Transport Association (IATA) Dangerous Goods Regulations is permitted by the Civil Aviation Safety Regulations. SSBA's usually fall into Category A infectious substances and require packing in accordance with Packing Instruction 620. Personnel that pack the SSBA for shipment are required by the Civil Aviation Safety Regulations to have current training in shipping dangerous goods.*

*Under the Civil Aviation Safety Regulations 1998 and Australian Dangerous Goods Code for Road and Rail, SSBA's are transported as Class 6 dangerous goods. Toxins are outlined in Division 6.1 and infectious substances are outlined in Division 6.2.*

## 6.2.2 Transport requirements for a receiving facility

- (1) The entity responsible for the receiving facility must ensure that the facility:
  - (a) verifies that the transfer has been successful. Verification of successful transfer includes that:
    - i. the complete shipment (quantity and type), as covered in the shipment details, has been received
    - ii. there is no evidence of tampering of the shipping package or container
  - (b) notifies the sending facility of the receipt of the shipment and if the transport has been successful (as defined under clause 6.2.1)
  - (c) contacts the transport agent (if used) and sending facility as a matter of urgency, if a shipment fails to arrive at the expected time to seek confirmation of the location of the shipment and its expected time of delivery
  - (d) immediately informs the sending facility, the Australian CDC and State/Territory police if the shipment is lost, stolen (once the entity is aware of the loss or theft) or identifies the transfer has been unsuccessful (see clause 6.2.1)

*It is recommended that Responsible Officers from each facility are included when transport agreements are being made.*

*If the receiving facility has any concerns about the shipment, they should contact the sending facility to verify the details and if there are any discrepancies then the receiving and sending facility should notify the Australian CDC, as required under the NHS Regulations and these Standards.*

*Tampering refers to the deliberate altering or damaging of the package. It does not refer to accidental damage sustained to the outer packaging during transport where the inner packaging is unaltered or undamaged.*

## 6.3 Transport security

- (1) Where a transport agent has been contracted to transport SSBA's, the entity responsible for the sending facility (or receiving facility if importing from outside Australia from a non-registered entity) must ensure that the transport agent has a documented transport security plan and systems in place to track the shipment at all stages of transport.

- (a) the entity is ultimately responsible for SSBA transport and must be able to justify their decision to hire a transport agent
  - (b) the entity must not permit a transport agent to transport SSBA's unless they demonstrate effective capability and compliance with Commonwealth, state and territory rules for transporting dangerous goods
- (2) At a minimum, the transport security plan must comprise of the following elements:
- (a) specific allocation of security responsibilities to competent and qualified persons with appropriate authority to carry out their responsibilities
  - (b) compliance with the requirements of Commonwealth, State and Territory legislation governing the transport of biological agents (for example – the Australian Dangerous Goods Code for Road and Rail and the Civil Aviation Safety Regulations for air transport)
  - (c) assessment and coverage of security risks, including vulnerabilities, across all operations, including inter-modal transport, temporary transit storage, handling, and distribution as appropriate
  - (d) clear statements of measures and resources that are to be used to reduce security risks. These measures must include:
    - i. policies (including response to higher threat conditions and new employee/employment verification)
    - ii. training
    - iii. operating practices (for example choice/use of routes where known, access to dangerous goods in temporary storage, and proximity to vulnerable infrastructure)
  - (e) up-to-date procedures for responding to and dealing with security threats, non-compliance with security protocols, or security incidents
  - (f) procedures for the evaluation and testing of security plans and procedures for periodic review and update of the plans
  - (g) measures to ensure the security of information relating to the transport of the SSBA's, including the transport security plan
  - (h) measures to ensure that the distribution of the transport information is as limited as possible. These measures must not preclude provision of documentation required by the relevant transport regulations
- (3) If a transport agent is not able to release a copy of their security plan to the entity (for example, if the plan is considered to be commercially confidential information), then the entity must supply the transport agent with a copy of the Standards requirements and ensure that the transport agent supplies, in writing, an assurance that these requirements have been met in the transport security plan.

*In Australia, the Commonwealth is responsible for regulating the transport of dangerous goods by air through the Civil Aviation Safety Authority (CASA) and by sea through the Australian Maritime Safety Authority (AMSA). The National Transport Commission administers the Australian Code for the Transport of Dangerous Goods by Road & Rail, and the states and territories have responsibility for road and rail transport of dangerous goods.*

*Each state and territory implements the Australian Dangerous Goods Code by road and rail and provide associated updates to their dangerous goods transport regulations separately. Each state and territory's dangerous goods transport act and*

regulations are available on the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts website at [www.infrastructure.gov.au](http://www.infrastructure.gov.au).

It is recommended that, where possible, the transport agent is a Security Construction and Equipment Committee (SCEC) endorsed courier. For more information, visit [www.scec.gov.au/scec-couriers](http://www.scec.gov.au/scec-couriers).

## 6.4 Transport of SSBA by authorised persons

- (1) Transport undertaken without the assistance of a transport agent must be undertaken by an authorised person and the movements reported to the Responsible Officer, who must maintain a record of such movements.
- (2) For material that is being transferred within a building, material must be triple packed unless it is documented in a risk assessment that double packaging is suitable and may be used.
- (3) If the material is to leave the building, the movement must be consistent with the requirements of Commonwealth, State and Territory legislation governing the transport of biological agents.

*Transportation by authorised persons may be between an entity and the facilities of another entity, between facilities of the same entity or between a facility and a linked storage unit (clause 4.8.1). This transport includes surface transportation, including walking.*

*A risk assessment does not need to be undertaken for each individual transport but can be part of the overall risk assessment for the handling of SSBA. The transport risk assessment should cover when double or triple packaging must be used.*

*If transporting SSBA waste for destruction, refer to clause 7.3 of these Standards. Record keeping requirements are set out in clause 5.2 of these Standards.*

*Entities are recommended to consult documents such as 'AS 4834-2007 – Packaging for surface transport of biological material that may cause disease in humans, animals and plants' and the 'National Pathology Accreditation Advisory Council (NPAAC) Requirements for the packaging and transport of pathology specimens and associated material' for determining minimum packaging requirements.*

## 6.5 Transport of SSBA from reception areas to a registered facility

- (1) Where a facility receives a package containing an SSBA that is delivered to a reception area (such as a mail receipt area or reception desk) prior to movement to a registered facility, the SSBA may be transported from the reception area to the facility by non-authorised persons under the following conditions:
  - (a) transport may only be between the reception area and the registered facility
  - (b) the person handling the SSBA must do so only for the purposes of receiving the package and transporting it to the registered facility, and must not open or re-package it

- (c) the SSBA must be delivered to an authorised person for the registered facility
  - (d) the entity must ensure that this transport is governed by a documented policy and procedure and included in the risk assessment
  - (e) the entity must record all movement of the SSBA between the reception area and the facility but does not need to report these movements to the Australian CDC
  - (f) the entity must keep an up-to-date list of persons who are permitted to undertake these transports
- (2) The person undertaking the transport must:
- (a) be 18 years or over
  - (b) have not been excluded from handling the SSBA by the entity nor directed not to handle SSBA's by the Australian CDC
  - (c) have basic training in the requirements of the SSBA Standards and the internal requirements for this type of transport. Records of this training must be kept
    - i. the basic training must include an overview of the of the NHS Act, NHS Regulations and SSBA Standards, the reporting requirements of the SSBA Regulatory Scheme and records management training

*A risk assessment does not need to be undertaken for each individual transport but can be part of the overall risk assessment for the handling of SSBA's.*

# Part 7 Inactivation and decontamination

# 7

## 7.1 Objective

- (1) Entities must ensure that all types of contaminated and potentially contaminated materials, including those that may result from an emergency, are identified and documented.
- (2) Effective procedures must be put in place to ensure the decontamination of materials or inactivation of the SSBA prior to its destruction or further use.

*The entity should identify all different types of materials that could be contaminated, or potentially contaminated by the SSBA, into classes so that their decontamination and destruction can be clearly defined. It is not necessary to individually identify items for each cycle of decontamination.*

## 7.2 Procedures

- (1) The Entity must identify and develop effective decontamination and inactivation regimes as per clause 2.2.1 of these Standards.
- (2) The Entity must develop and document effective processes to decontaminate or inactivate SSBA, or waste products potentially contaminated with SSBA, prior to destruction or further use.
- (3) Inactivation and decontamination methods must be supported with validation data and a quality assurance framework must be put in place to ensure inactivation or decontamination has been correctly performed.
- (4) Waste products potentially contaminated with SSBA prior to confirmed inactivation must be treated as SSBA, and must comply with the access, handling and transport requirements of these Standards.

*Sources of contamination that should be identified include all potential waste streams. Reusable items such as glassware should be decontaminated before being sent for washing and recycling. Laboratory gowns should be decontaminated before being sent for washing and other personal protective equipment handled in accordance with the relevant standards. Procedures should ensure that no unauthorised access to an SSBA is possible.*

*The entity should select inactivation methods supported by validation data demonstrating effectiveness under facility specific conditions. Validation procedures should consider issues such as:*

- *The nature of the material being treated (for example, volume, presence of protein/other potentially inhibitory substances)*
- *Contact times and material compatibility issues (for example, interaction with stainless steel or rubber seals)*
- *Potential health hazards associated with the disinfectant*
- *The need to maintain the required level of active compound, including deterioration over time.*

*In planning and conducting decontamination activities the entity should consider:*

- *Ensuring all disinfectants used contain sufficient active compound to address the working conditions under which they will be applied, and that such concentrations are maintained throughout the process, including conducting specific validation activities where necessary*

- *Implementing monitoring measures to ensure the methods have been effective (for example, cycle recording and use of chemical or biological indicators in autoclaves)*
- *Ensuring adequate methods and resources are available to deal with routine work and any spillages or other incidents during handling and transport of materials inside and outside the facility*
- *Implementing programs to ensure the amount of contaminated waste is minimised*

## 7.3 Waste management

- (1) The entity must ensure that its waste management processes 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.
- (2) Risk assessment must determine the procedures required to ensure the secure destruction of waste is carried out, as per clause 2.2.1 of these Standards.
- (3) If waste disposal is undertaken through a contracted waste disposal company, the entity must put in place mechanisms to ensure that waste is kept secure until picked up (for example within locked bins) and that the entity receives notification when the waste is destroyed.

*Waste can be decontaminated at another part of the entity if it is permissible by the entity's policies and procedures and if it is securely transported. Entities are recommended to consult documents such as AS 4834-2007 – Packaging for surface transport of biological material that may cause disease in humans, animals and plants and the National Pathology Accreditation Advisory Council (NPAAC) Requirements for the packaging and transport of pathology specimens and associated material for determining minimum packaging requirements.*

*Waste should be moved from secure areas to collection points as close as practical to the time of pickup. Entities should have arrangements with any waste contractors used to ensure that destruction will take place as soon as possible after the waste arrives at the treatment facility.*

*Where a waste contractor is not used, transport should be by an authorised person, validated processes performed by an authorised person, and appropriate records maintained (see clause 5.2). Destruction should take place as soon as possible after the waste arrives.*

*Policies and procedures should include other standard or regulatory requirements, such as AS/NZS 2243.3:2022 Safety in laboratories – Microbiological safety and containment.*

*The following elements should be considered for a waste management policy:*

- *Ensure a program is in place to minimise waste production*
- *Ensure effective waste audit trails are in place and documented*
- *Provide adequate facilities and procedures for the storage of waste (including short-term storage)*
- *Ensure appropriate packaging material is used to contain the waste and to maintain its integrity during storage and transport.*

## 7.4 Record keeping

- (1) The entity must keep records of decontamination/inactivation and validation data for all SSBA's in accordance with clause 5.2 of these Standards.

*Records of decontamination/inactivation and validation required in Part 7 are different to records of disposal which refer to the complete transfer or destruction of the SSBA. Handling of disposal records is defined under clause 5.2.*

# Part 8 Handling biological agents suspected of being SSBAAs

# 8

## 8.1 Objective

- (1) Entities must ensure that biological agents suspected, based on testing in a laboratory, of being an SSBA are handled securely prior to the outcome of confirmatory testing or destruction.
- (2) Entities must meet the handling and reporting requirements under the NHS Act and the NHS Regulations in respect of any SSBA or suspected SSBA held by the entity.

*Division 4A of the NHS Act sets out the requirements for handling biological agents that are suspected to be SSBA. Division 4A requires confirmatory testing or destruction of those agents and compliance with SSBA Standards for handling those agents. This Part sets standards for handling those agents that are suspected to be SSBA.*

*The requirement for compliance with this Part begins when the initial tester forms a reasonable suspicion, based on testing in the laboratory, that the biological agent is an SSBA. Note that field tests do not apply in this scenario, as the test must be conducted in a laboratory to confirm suspicion.*

*Reasonable suspicion does not apply simply because an SSBA cannot be ruled out, but rather, on the balance of probability, the agent is likely to be an SSBA.*

*The requirement for compliance with this Part ends when the initial tester receives the results of the confirmatory test or upon the complete destruction of the agent if confirmatory testing is not undertaken.*

*If the sample is confirmed as an SSBA, then the entity must comply with the requirements of the NHS Act and NHS Regulations in relation to confirmed SSBA as per Part 9 of these Standards. If the entity intends to handle the SSBA on an ongoing basis, compliance will include registration and meeting the requirements of Parts 1-7 of the SSBA Standards.*

## 8.2 Access and Storage

- (1) The entity must ensure that physical access to the suspected SSBA is restricted to persons that have a need to handle the agent.
- (2) The entity must store suspected SSBA securely to ensure that physical access is restricted to persons that have a need to handle the agent.
- (3) The entity must maintain a record of who accesses the suspected SSBA, including the identity of the person and the date and time of access.

*Controls to restrict access, and the point at which access to the storage unit is recorded, should be at the last physical barrier to the suspected SSBA. Storage may include a locked freezer, a locked cupboard, a locked liquid nitrogen storage tank or locked containers within these devices for which the access is controlled.*

*However, if the SSBA is stored within the freezer in a locked box that cannot be easily removed, then access controls should be on the locked box and access to the box recorded. In this scenario it is not necessary to record all access to the freezer itself.*

## 8.3 Transport

### 8.3.1 Transport requirements for a sending facility

- (1) This clause applies when transporting a suspected SSBA, or a sample of a suspected SSBA, for the purposes of confirmatory testing, and transport for the purposes of destruction.
- (2) The entity responsible for the sending facility must ensure that the facility:
  - (a) has documented policies and procedures in place to ensure compliance with Commonwealth, State and Territory legislation governing the transport of biological and toxin agents
  - (b) ensures that the receiving facility will accept the shipment prior to dispatch of the agent. A record must be kept of this acceptance
  - (c) notifies the receiving facility of the shipment details (such as the waybill, consignment note or tracking number, together with details of the transport agent and the expected time of delivery) at the time of shipment
  - (d) immediately informs the Australian CDC and State/Territory police if the shipment is lost, stolen (once the entity is aware of the loss or theft) or if the shipment is reported as an unsuccessful transfer (see 8.3.2) by the receiving facility (once the entity is aware of the unsuccessful transfer)

*The sending facility should contact the receiving facility within a maximum of two business days after the expected delivery time to ensure the shipment has been received if it has not already received confirmation from the receiving facility.*

*The transport of SSBA's by air is covered by the Civil Aviation Safety Regulations 1998 and by road and rail by the Australian Dangerous Goods Code for Road and Rail, as incorporated by each State and Territory in relevant legislation.*

*Air transport consistent with the International Air Transport Association (IATA) Dangerous Goods Regulations is permitted by the Civil Aviation Safety Regulations. SSBA's usually fall into Category A infectious substances and require packing in accordance with Packing Instruction 620. Personnel that pack the SSBA for shipment are required by the Civil Aviation Safety Regulations to have current training in shipping dangerous goods.*

*Under the Civil Aviation Safety Regulations 1998 and Australian Dangerous Goods Code for Road and Rail, SSBA's are transported as Class 6 dangerous goods. Toxins are outlined in Division 6.1 and infectious substances are outlined in Division 6.2.*

### 8.3.2 Transport requirements for a receiving facility

- (1) This clause applies when receiving a suspected SSBA, or a sample of a suspected SSBA, for the purposes of confirmatory testing, or for the purposes of destruction.
- (2) The entity responsible for the receiving facility must ensure that the facility:
  - (a) verifies that the transfer has been successful. Verification of successful transfer includes that:

- i. the complete shipment (quantity and type), as covered in the shipment details, has been received
  - ii. there is no evidence of tampering of the shipping container
- (b) notifies the sending facility of the receipt of the shipment and if the transport has been successful (as defined under clause 8.3.1)
- (c) contacts the transport agent (if used) and sending facility as a matter of urgency, if a shipment fails to arrive at the expected time to seek confirmation of the location of the shipment and its expected time of delivery
- (d) immediately informs the sending facility, the Australian CDC and State/Territory police if the shipment is lost, stolen (once the entity is aware of the loss or theft) or identifies the transfer has been unsuccessful (see clause 8.3.1)

*If the receiving facility has any concerns about the shipment, they should contact the sending facility to verify the details and if there are any discrepancies then the receiving and sending facility should notify the Australian CDC, as required under the NHS Regulations and these Standards.*

*Tampering refers to the deliberate altering or damaging of the package. It does not refer to accidental damage sustained to the outer packaging during transport where the inner packaging is unaltered or undamaged.*

## 8.4 Destruction

- (1) The entity must ensure that:
  - (a) If destruction takes place prior to confirmatory testing results being received — processes for destruction of suspected SSBA are such that no suspected SSBA leaves the entity without being destroyed or inactivated, unless it is being transported to another entity or facility for confirmatory testing or for destruction
  - (b) If destruction takes place following receipt of confirmatory testing results — processes for destruction of biological agents confirmed as SSBA are such that no SSBA leaves the entity without being destroyed or inactivated, unless the SSBA is being transferred in its entirety for the purposes of disposal under Division 4A of the NHS Act

*It is likely that several effective destruction methods will be available for the suspected SSBA handled. The entity should ensure that there is data available to demonstrate that the methodology selected can inactivate the agent under the specific conditions encountered in the facility. For more information, see clause 7.2 of these Standards.*

## 8.5 Waste Disposal

- (1) The entity must have validated procedures for the decontamination of waste materials potentially contaminated with the suspected SSBA.

*Waste can be decontaminated at another part of the entity if permissible by the entity's policies and procedures and if it is securely transported.*

*If the waste is to be disposed of outside of the facility through a waste disposal contractor, then waste should be moved from secure areas to collection points as*

*close as practical to the time of pickup. Entities should have arrangements with any waste contractors used to ensure that destruction will take place as soon as possible after the waste arrives at the treatment facility.*

*Decontamination should take place as soon as possible.*

## 8.6 Record Keeping

- (1) Once the initial tester forms a reasonable suspicion that the biological agent is an SSBA, the entity must maintain records of all activities related to the requirements of Part 8 of these Standards.
  - (a) Records relating to Part 8 of these Standards must be maintained for a minimum of 12 months for Tier 1 SSBAs and a minimum of 6 months for Tier 2 SSBAs, unless otherwise specified in these Standards
- (2) Records do not need to be kept if confirmatory testing shows that the agent is not an SSBA.

*Records may consist of records of destruction and waste disposal (including validation data) and transport.*

# Part 9 Handling SSBA's following a positive confirmatory test result

9

## 9.1 Objective

- (1) Entities must ensure that biological agents that were suspected of being SSBAs, and have now been confirmed as SSBAs, are handled securely.
- (2) Entities must meet the handling and reporting requirements under the NHS Act and the NHS Regulations in respect of any SSBA or suspected SSBA held by the entity.

The requirements contained in Part 9 follow on from the requirements under Part 8 of these Standards.

These requirements commence when the entity or facility that was handling a suspected SSBA receives a positive result from a confirmatory test.

If the entity or facility intends to continue handling the SSBA (including storage), then it must register to do so. Registration includes making a declaration of compliance with the requirements of Parts 1-7 of the SSBA Standards. Registration documentation must be submitted to the Australian CDC within two business days of receiving confirmation of an agent being an SSBA.

If the entity or facility does not intend to continue handling the SSBA, under the NHS Act it must dispose of the SSBA by complete transfer of the SSBA or by destruction of all the SSBA (or a combination of both). Disposal must take place within two business days of receiving confirmation that the biological agent is an SSBA, or within a longer period if an application for extension is granted by the Australian CDC.

These requirements end upon submission of a report to the Australian CDC by the entity confirming disposal of the SSBA or an intention to continue handling the SSBA (via an Initial Registration report or a Start to Handle a New SSBA report).

Further information and registration and reporting forms can be found at [www.cdc.gov.au/ssba](http://www.cdc.gov.au/ssba).

## 9.2 Access and Storage

- (1) The entity must ensure that physical access to the SSBA is restricted to persons that have a need to handle the agent.
- (2) The entity must store SSBAs securely to ensure that physical access is restricted to persons that have a need to handle the agent.
- (3) The entity must maintain a record of who accesses the SSBA, including the identity of the person and the date and time of access.

*Controls to restrict access and the point at which access to the storage unit is recorded, should be at the last physical barrier to the SSBA. Storage may include a locked freezer, a locked cupboard, a locked liquid nitrogen storage tank or locked containers within these devices for which the access is controlled.*

*However, if the SSBA is stored within the freezer in a locked box that cannot be easily removed, then access controls should be on the locked box and access to the box recorded. In this scenario it is not necessary to record all access to the freezer itself.*

## 9.3 Transport

### 9.3.1 Transport requirements for a sending facility

- (1) This clause applies when transporting confirmed SSBA following a positive confirmatory test for the purposes of disposal (complete transfer or destruction).
- (2) The entity responsible for the sending facility must ensure that the facility:
  - (a) has documented policies and procedures in place to ensure compliance with Commonwealth, State and Territory legislation governing the transport of biological and toxin agents
  - (b) ensures that the receiving facility will accept the shipment prior to dispatch of the agent. A record must be kept of this acceptance
  - (c) notifies the receiving facility of the shipment details (such as the waybill, consignment note or tracking number, together with details of the transport agent and the expected time of delivery) at the time of shipment
  - (d) immediately informs the Australian CDC and State/Territory police if the shipment is lost, stolen (once the entity is aware of the loss or theft) or if the shipment is reported as an unsuccessful transfer (see 9.3.2) by the receiving facility (once the entity is aware of the unsuccessful transfer)

*The sending facility should contact the receiving facility within a maximum of two business days after the expected delivery time to ensure the shipment has been received if it has not already received confirmation from the receiving facility.*

*The transport of SSBA by air is covered by the Civil Aviation Safety Regulations 1998 and by road and rail by the Australian Dangerous Goods Code for Road and Rail, as incorporated by each State and Territory in relevant legislation.*

*Air transport consistent with the International Air Transport Association (IATA) Dangerous Goods Regulations is permitted by the Civil Aviation Safety Regulations. SSBA usually fall into Category A infectious substances and require packing in accordance with Packing Instruction 620. Personnel that pack the SSBA for shipment are required by the Civil Aviation Safety Regulations to have current training in shipping dangerous goods.*

*Under the Civil Aviation Safety Regulations 1998 and Australian Dangerous Goods Code for Road and Rail, SSBA are transported as Class 6 dangerous goods. Toxins are outlined in Division 6.1 and infectious substances are outlined in Division 6.2.*

### 9.3.2 Transport for a receiving facility

- (1) This clause applies when receiving confirmed SSBA following a positive confirmatory test for the purposes of disposal (complete transfer or destruction).
- (2) The entity responsible for the receiving facility must ensure that the facility:
  - (a) verifies that the transfer has been successful. Verification of successful transfer includes that:
    - i. the complete shipment (quantity and type), as covered in the shipment details, has been received
    - ii. there is no evidence of tampering of the shipping container

- (b) notifies the sending facility of the receipt of the shipment and if the transport has been successful (as defined under clause 9.3.1)
- (c) contacts the transport agent (if used) and sending facility as a matter of urgency, if a shipment fails to arrive at the expected time to seek confirmation of the location of the shipment and its expected time of delivery
- (d) immediately informs the sending facility, the Australian CDC and State/Territory police if the shipment is lost, stolen (once the entity is aware of the loss or theft) or identifies the transfer has been unsuccessful (see clause 9.3.1)

*If the receiving facility has any concerns about the shipment, they should contact the sending facility to verify the details and if there are any discrepancies then the receiving and sending facility should notify the Australian CDC, as required under the NHS Regulations and these Standards.*

*Tampering refers to the deliberate altering or damaging of the package. It does not refer to accidental damage sustained to the outer packaging during transport where the inner packaging is unaltered or undamaged.*

## 9.4 Destruction

- (1) The entity must ensure that processes for destruction are such that no SSBA leaves the entity without being destroyed or inactivated, unless the SSBA is being transferred in its entirety for the purposes of disposal.

*Whatever the SSBA handled, it is likely that several effective destruction methods will be available. The entity should ensure that there is data available to demonstrate that the methodology selected can inactivate the agent under the specific conditions encountered in the facility. For more information, see clause 7.2 of these Standards.*

## 9.5 Waste Disposal

- (1) The entity must have validated procedures for the decontamination of waste materials potentially contaminated with the SSBA.

*Waste can be decontaminated at another part of the entity if permissible by the entity's policies and procedures and if it is securely transported.*

*If the waste is to be disposed of outside of the facility through a waste disposal contractor, then waste should be moved from secure areas to collection points as close as practical to the time of pickup. Entities should have arrangements with any waste contractors used to ensure that destruction will take place as soon as possible after the waste arrives at the treatment facility.*

*Decontamination should take place as soon as possible.*

## 9.6 Record Keeping

- (1) The entity must maintain records of all activities related to the requirements of Part 9 of these Standards.

- (2) Records relating to Part 9 of these Standards must be maintained for a minimum of 12 months for Tier 1 SSBAAs and a minimum of 6 months for Tier 2 SSBAAs.

*Records may consist of records of access, destruction, waste disposal (including validation data) and transport.*

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

# 10

---

## 10.1 Objective

- (1) Entities must ensure that SSBAs that are handled temporarily by a non-registered entity are handled securely prior to disposal.
- (2) Entities must meet the handling and reporting requirements under the NHS Act and the NHS Regulations in respect of any SSBA or suspected SSBA held by the entity.

*Division 5AA of the NHS Act sets out the requirements for the temporary handling of biological agents for non-registered entities that receive a known SSBA. If an entity is a registered entity its handling of SSBAs is not covered by Division 5AA and, therefore, Part 10 of the Standards do not apply to it.*

*In keeping with the mechanisms established by the NHS Act, the requirements in the Standards are imposed on entities rather than on the facilities for which they may be responsible.*

*These requirements apply when a non-registered entity receives a known SSBA (i.e. one that has already been confirmed as an SSBA).*

*These requirements cease to apply upon disposal of the SSBA. Under the NHS Act, disposal under the temporary handling provisions must occur within seven business days of receipt of the agent.*

*It should be noted that these requirements **do not** apply to an entity, acting as an initial tester under Part 3, Division 4A of the NHS Act, that has received a positive confirmatory testing result for a previously suspected SSBA. These SSBAs must be handled under Part 9 of these Standards.*

## 10.2 Access and Storage

- (1) The entity must ensure that physical access to the SSBA is restricted to persons that have a need to handle the agent.
- (2) The entity must store SSBAs securely to ensure that physical access is restricted to persons that have a need to handle the agent.
- (3) The entity must maintain a record of who accesses the SSBA, including the identity of the person and the date and time of access.

*Controls to restrict access and the point at which access to the storage unit is recorded, should be at the last physical barrier to the SSBA. Storage may include a locked freezer, a locked cupboard, a locked liquid nitrogen storage tank or locked containers within these devices for which the access is controlled.*

*However, if the SSBA is stored within the freezer in a locked box that cannot be easily removed, then access controls should be on the locked box and access to the box recorded. In this scenario it is not necessary to record all access to the freezer itself.*

## 10.3 Transport

### 10.3.1 Transport requirements for a sending facility

- (1) This clause applies when transporting an SSBA for the purposes of disposal.
- (2) The entity responsible for the sending facility must ensure that the facility:
  - (a) has documented policies and procedures in place to ensure compliance with Commonwealth, State and Territory legislation governing the transport of biological and toxin agents
  - (b) ensures that the receiving facility will accept the shipment prior to dispatch of the agent. A record must be kept of this acceptance
  - (c) notifies the receiving facility of the shipment details (such as the waybill, consignment note or tracking number, together with details of the transport agent and the expected time of delivery) at the time of shipment
  - (d) immediately informs the Australian CDC and State/Territory police if the shipment is lost, stolen (once the entity is aware of the loss or theft) or if the shipment is reported as an unsuccessful transfer (see clause 10.3.2) by the receiving facility (once the entity is aware of the unsuccessful transfer)

*The sending facility should contact the receiving facility within a maximum of two business days after the expected delivery time to ensure the shipment has been received if it has not already received confirmation from the receiving facility.*

*The transport of SSBA's by air is covered by the Civil Aviation Safety Regulations 1998 and by road and rail by the Australian Dangerous Goods Code for Road and Rail, as incorporated by each State and Territory in relevant legislation.*

*Air transport consistent with the International Air Transport Association (IATA) Dangerous Goods Regulations is permitted by the Civil Aviation Safety Regulations. SSBA's usually fall into Category A infectious substances and require packing in accordance with Packing Instruction 620. Personnel that pack the SSBA for shipment are required by the Civil Aviation Safety Regulations to have current training in shipping dangerous goods.*

*Under the Civil Aviation Safety Regulations 1998 and Australian Dangerous Goods Code for Road and Rail, SSBA's are transported as Class 6 dangerous goods. Toxins are outlined in Division 6.1 and infectious substances are outlined in Division 6.2.*

### 10.3.2 Transport requirements for a receiving facility

- (1) This clause applies when receiving an SSBA for the purposes of disposal.
- (2) The entity responsible for the receiving facility must ensure that the facility:
  - (a) verifies that the transfer has been successful. Verification of successful transfer includes that:
    - i. the complete shipment (quantity and type), as covered in the shipment details, has been received
    - ii. there is no evidence of tampering of the shipping container

- (b) notifies the sending facility of the receipt of the shipment and if the transport has been successful (as defined under clause 10.3.1)
- (c) contacts the transport agent (if used) and sending facility as a matter of urgency, if a shipment fails to arrive at the expected time to seek confirmation of the location of the shipment and its expected time of delivery
- (d) immediately informs the sending facility, the Australian CDC and State/Territory police if the shipment is lost, stolen (once the entity is aware of the loss or theft) or identifies the transfer has been unsuccessful (see clause 10.3.1)

*If the receiving facility has any concerns about the shipment, they should contact the sending facility to verify the details and if there are any discrepancies then the receiving and sending facility should notify the Australian CDC, as required under the NHS Regulations and these Standards.*

*Tampering refers to the deliberate altering or damaging of the package. It does not refer to accidental damage sustained to the outer packaging during transport where the inner packaging is unaltered or undamaged.*

## 10.4 Destruction

- (1) The entity must ensure that its waste management processes 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.

*It is likely that several effective destruction methods will be available for the SSBA handled. The entity should ensure that there is data available to demonstrate that the methodology selected can inactivate the agent under the specific conditions encountered in the facility. For more information, see clause 7.2 of these Standards.*

## 10.5 Waste Disposal

- (1) The entity must have validated procedures for the decontamination of waste materials potentially contaminated with the SSBA.

*Waste can be decontaminated at another part of the entity if permissible by the entity's policies and procedures and if it is securely transported.*

*If the waste is to be disposed of outside of the facility through a waste disposal contractor, then waste should be moved from secure areas to collection points as close as practical to the time of pickup. Entities should have arrangements with any waste contractors used to ensure that destruction will take place as soon as possible after the waste arrives at the treatment facility.*

*Decontamination should take place as soon as possible.*

## 10.6 Record Keeping

- (1) The entity must maintain records of all activities related to the requirements of Part 10 of these Standards.

- (2) Records relating to Part 10 of these Standards must be maintained for a minimum of 12 months for Tier 1 SSBAAs and a minimum of 6 months for Tier 2 SSBAAs, unless otherwise specified in these Standards.

*Records may consist of records of access, destruction and waste disposal (including validation data) and transport.*

Part 11 Registered entity  
handling an SSBA that  
they are not registered  
for, on a temporary  
basis

11

## 11.1 Objective

- (1) To ensure that SSBA that are handled temporarily by a facility of a registered entity are handled securely prior to disposal.
- (2) Entities must meet the handling and reporting requirements under the NHS Act and the NHS Regulations in respect of any SSBA or suspected SSBA held by the entity.

*Section 42 of the NHS Act provides for an entity to be registered in relation to one or more SSBA and one or more facilities.*

*Parts 1 – 7 of these Standards provide the requirements a registered entity is to comply with where a facility of a registered entity commences handling one or more SSBA on an ongoing basis.*

*The requirements under Part 11 apply where a facility of a registered entity commences handling an SSBA that they are not registered to handle, on a temporary basis. In this situation, Part 11 requirements apply to the handling of the SSBA rather than Parts 1 – 7 of the Standards.*

*These requirements cease to apply upon disposal of the SSBA. Under the NHS Act, disposal under the temporary handling provisions must occur within seven business days of receipt of the agent.*

*It should be noted that these requirements **do not** apply to an entity, acting as an initial tester under Part 3, Division 4A of the NHS Act, that has received a positive confirmatory testing result for a previously suspected SSBA. These SSBA must be handled under Part 9 of these Standards.*

## 11.2 Access and Storage

- (1) The registered entity must ensure that physical access to the SSBA is restricted to persons that have a need to handle the agent at any of its facilities.
- (2) The registered entity must store SSBA securely to ensure that physical access is restricted to persons that have a need to handle the agent at any of its facilities.
- (3) The registered entity must maintain a record of who accesses the SSBA, including the identity of the person and the date and time of access at any of its facilities.

*Controls to restrict access and the point at which access to the storage unit is recorded, should be at the last physical barrier to the SSBA. Storage may include a locked freezer, a locked cupboard, a locked liquid nitrogen storage tank or locked containers within these devices for which the access is controlled.*

*However, if the SSBA is stored within the freezer in a locked box that cannot be easily removed, then access controls should be on the locked box and access to the box recorded. In this scenario it is not necessary to record all access to the freezer itself.*

## 11.3 Transport

### 11.3.1 Transport requirements for a sending facility

- (1) This clause applies when transporting a SSBA for the purposes of disposal.
- (2) The registered entity responsible for the sending facility must ensure that the facility:
  - (a) has documented policies and procedures in place to ensure compliance with Commonwealth, State and Territory legislation governing the transport of biological and toxin agents
  - (b) ensures that the receiving facility will accept the shipment prior to dispatch of the agent. A record must be kept of this acceptance
  - (c) notifies the receiving facility of the shipment details (such as the waybill, consignment note or tracking number, together with details of the transport agent and the expected time of delivery) at the time of shipment
  - (d) immediately informs the Australian CDC and State/Territory police if the shipment is lost, stolen (once the entity is aware of the loss or theft) or if the shipment is reported as an unsuccessful transfer (see clause 11.3.2) by the receiving facility (once the entity is aware of the unsuccessful transfer)

*The sending facility should contact the receiving facility within a maximum of two business days after the expected delivery time to ensure the shipment has been received if it has not already received confirmation from the receiving facility.*

*The transport of SSBA's by air is covered by the Civil Aviation Safety Regulations 1998 and by road and rail by the Australian Dangerous Goods Code for Road and Rail, as incorporated by each State and Territory in relevant legislation.*

*Air transport consistent with the International Air Transport Association (IATA) Dangerous Goods Regulations is permitted by the Civil Aviation Safety Regulations. SSBA's usually fall into Category A infectious substances and require packing in accordance with Packing Instruction 620. Personnel that pack the SSBA for shipment are required by the Civil Aviation Safety Regulations to have current training in shipping dangerous goods.*

*Under the Civil Aviation Safety Regulations 1998 and Australian Dangerous Goods Code for Road and Rail, SSBA's are transported as Class 6 dangerous goods. Toxins are outlined in Division 6.1 and infectious substances are outlined in Division 6.2.*

### 11.3.2 Transport requirements for a receiving facility

- (1) This clause applies when receiving a SSBA for the purposes of disposal.
- (2) The registered entity responsible for the receiving facility must ensure that the facility:
  - (a) verifies that the transfer has been successful. Verification of successful transfer includes that:

- i. the complete shipment (quantity and type), as covered in the shipment details, has been received
  - ii. there is no evidence of tampering of the shipping container
- (b) notifies the sending facility of the receipt of the shipment and if the transport has been successful (as defined under clause 11.3.1)
- (c) contacts the transport agent (if used) and sending facility as a matter of urgency, if a shipment fails to arrive at the expected time to seek confirmation of the location of the shipment and its expected time of delivery
- (d) immediately informs the sending facility, the Australian CDC and State/Territory police if the shipment is lost, stolen (once the entity is aware of the loss or theft) or identifies the transfer has been unsuccessful (see clause 11.3.1)

*If the receiving facility has any concerns about the shipment, they should contact the sending facility to verify the details and if there are any discrepancies then the receiving and sending facility should notify the Australian CDC, as required under the NHS Regulations and these Standards.*

*Tampering refers to the deliberate altering or damaging of the package. It does not refer to accidental damage sustained to the outer packaging during transport where the inner packaging is unaltered or undamaged.*

## 11.4 Destruction

- (1) The registered entity must ensure that its waste management processes are such that no SSBA leaves the control of the registered entity without being inactivated or destroyed unless it is being transported to another entity or facility for further handling or destruction.

*It is likely that several effective destruction methods will be available for the SSBA handled. The registered entity should ensure that there is data available to demonstrate that the methodology selected is capable of inactivating the agent under the specific conditions encountered in the facility. For more information, see clause 7.2 of these Standards.*

## 11.5 Waste Disposal

- (1) The registered entity must have validated procedures for the decontamination of waste materials potentially contaminated with the SSBA at any of its facilities.

*Waste can be decontaminated at another part of the entity if permissible by the entity's policies and procedures and if it is securely transported.*

*If the waste is to be disposed of outside of the facility through a waste disposal contractor, then waste should be moved from secure areas to collection points as close as practical to the time of pickup. Entities should have arrangements with any waste contractors used to ensure that destruction will take place as soon as possible after the waste arrives at the treatment facility.*

*Decontamination should take place as soon as possible.*

## 11.6 Record Keeping

- (1) The registered entity must maintain records of all activities related to the requirements of Part 11 of these Standards at any of its facilities.
- (2) Records relating to Part 11 of these Standards must be maintained for a minimum of 12 months for Tier 1 SSBA and a minimum of 6 months for Tier 2 SSBA, unless otherwise specified in these Standards.

*Records may consist of records of destruction and waste disposal (including validation data) and transport.*

# Appendix

## Health Security

## Relevant Offences

| Item | Kind of offence                                                                                                                                                                                                                                                                                                                                                |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | An offence involving the supply of goods (such as weapons or missiles) for a Weapons of Mass Destruction program as mentioned in the Weapons of Mass Destruction (Prevention of Proliferation) Act 1995                                                                                                                                                        |
| 2    | An offence mentioned in Chapter 5 of the Criminal Code                                                                                                                                                                                                                                                                                                         |
| 3    | An offence involving the hijacking or destruction of an aircraft or vessel                                                                                                                                                                                                                                                                                     |
| 4    | An offence involving counterfeiting or falsification of identity documents, or assuming another individual's identity                                                                                                                                                                                                                                          |
| 5    | An offence involving the possession, supply, production, import or export of explosives or weapons                                                                                                                                                                                                                                                             |
| 6    | An offence involving: <ul style="list-style-type: none"> <li>a) the possession of a prohibited drug, but only if the penalty for the offence is imprisonment for 2 years or more; or</li> <li>b) the supply, production, import or export of a prohibited drug; or</li> <li>c) the possession of equipment for the manufacture of a prohibited drug</li> </ul> |
| 7    | An offence involving membership of, or association with an organised criminal group                                                                                                                                                                                                                                                                            |
| 8    | An offence: <ul style="list-style-type: none"> <li>a) involving treachery, sabotage, inciting mutiny, unlawful drilling, or destroying or damaging Commonwealth property; and</li> <li>b) mentioned in Part II of the Crimes Act 1914</li> </ul>                                                                                                               |
| 9    | An offence against Part 3 of the National Health Security Act 2007                                                                                                                                                                                                                                                                                             |
| 10   | An offence against the Crimes (Biological Weapons) Act 1976                                                                                                                                                                                                                                                                                                    |
| 11   | An offence against the Chemical Weapons Convention (Prohibition) Act 1994                                                                                                                                                                                                                                                                                      |
| 12   | An offence against the <i>Biosecurity Act 2015</i>                                                                                                                                                                                                                                                                                                             |
| 13   | An offence against the <i>Gene Technology Act 2000</i> .                                                                                                                                                                                                                                                                                                       |

*Definitions of 'imprisonment' and 'prohibited drug' can be found in Part 1 under Terms and Definitions.*

*When being assessed against the list of health security relevant offences, a person will be determined to have a result of 'adverse' if that person has been convicted of the offence and has received a sentence of imprisonment (including a suspended sentence). Individuals are rarely sentenced to imprisonment unless the offence is serious or the person has a prior criminal record. Under this scheme, a person who*

*has committed an offence listed above but who did not receive a sentence of imprisonment but instead received a fine, would not receive an adverse result from the NHS check. Offences with imprisonment that have expired under the Spent Convictions Scheme are also not taken into account.*

*Examples of the offences listed under Chapter 5 of the Criminal code include treason, sedition, espionage and terrorism.*

*Offences involving the possession of a prohibited drug will be assessed if the offence has a penalty of imprisonment for two or more years. Offences that have penalties of less than this time period will not be assessed as part of the NHS check. For example, a person convicted of possession of a prohibited drug who received a sentence of imprisonment of 3 months would still receive an adverse result if the maximum penalty a judge could impose for that offence was two or more years.*

# Bibliography

Australian Safeguards and Non-Proliferation Office, *Chemical Weapons Convention*, 2020

Australian signals directorate *Strategies to Mitigate Cyber Security Incidents*, 2017

Civil Aviation Safety Regulations 1998

Chemical Weapons (Prohibition) Act 1994

Customs (Prohibited Imports) Regulations 1956

Department of Agriculture, Fisheries and Forestry, approved arrangements under Chapter 7 of the *Biosecurity Act 2015*

European Committee for Standardisation, *CWA 15793:2008 Laboratory biorisk management standard*, CEN, Belgium.

European Committee for Standardisation, *EN 12128:1998 Biotechnology— Laboratories for research development and analysis - Containment levels of microbiology laboratories, areas of risk, localities and physical safety requirements* CEN, Belgium.

Health Canada, *Canadian Biosafety Standard*, Third Edition

International Air Transport Association, *Dangerous Goods Manuals*

International Air Transport Association (IATA), *Dangerous Goods Regulations*, Montreal: IATA Dangerous Goods Board, Current version.

International Organization for Standardization, *ISO 9000:2015 Quality management systems - Fundamentals and vocabulary*, ISO, Geneva.

International Organization for Standardization, *ISO 9001:2015 Quality management systems - Requirements*, ISO, Geneva.

International Organization for Standardization, *ISO 19011:2018 Guidelines for quality and/or environmental management systems auditing*, ISO, Geneva.

International Organization for Standardization, *ISO 14001:2015 Environmental management systems - Requirements with guidance for use*, ISO, Geneva.

International Organization for Standardization *ISO 15189:2022 Medical laboratories - Particular requirements for quality and competence*, ISO, Geneva.

International Organization for Standardization, *ISO 15190:2020 Medical laboratories - Requirements for safety*, ISO, Geneva.

International Organization for Standardization, *ISO/IEC 17025:2017 General requirements for the competence of testing and calibration laboratories*, ISO, Geneva.

International Organization for Standardization, *ISO/IEC 27002:2022 Information technology - Security techniques - Code of practice for information security management*, ISO, Geneva.

International Organization for Standardization, *ISO/IEC Guide 51:2014 Safety aspects - Guidelines for their inclusion in standards*, ISO, Geneva.

International Organization for Standardization, *ISO 45001:2018 Occupational health and safety management systems - Requirements with guidance for use*.

National Archives of Australia, *Information disposal*.

Office of the Gene Technology Regulator, 2001, *Guidelines for the certification of facilities/Physical containment requirements*, OGTR, Canberra.

Organisation for the Prohibition of Chemical Weapons, *Chemical Weapons Convention*, 2020

Safe work Australia, *Code of Practice: Managing psychosocial hazards at work*, 2022

Security Construction and Equipment Committee, *Endorsed Courier Services*

Standards Australia, *AS/NZS 2243.1:2021 Safety in laboratories, Part 1: Planning and operational aspects*, SAI Global, Sydney.

Standards Australia, *AS/NZS 2243.3:2022 Safety in laboratories, Part 3: Microbiological safety and containment*, SAI Global, Sydney.

Standards Australia, *AS/NZS 3816:1998 Management of clinical and related wastes*, SAI Global, Sydney.

Standards Australia, *AS/NZS ISO 3100:2018 Risk management- Principles and guidelines*, SAI Global, Sydney.

Standards Australia, *AS 4811:2022 Workforce screening*, SAI Global, Sydney.

Standards Australia, *HB 167:2025 Managing security related risks*, SAI Global, Sydney.

Standards Australia, *HB 292:2006 Practitioners guide to business continuity management*, SAI Global, Sydney.

United Nations, *Recommendations on the Transport of Dangerous Goods Model Regulations*, 23rd edition, Geneva, 2023.

World Health Organization, *Laboratory biosafety manual, fourth edition*, Geneva, 2020.

World Health Organization. WHO/CDS/ERP/2006.6 *Biorisk management: Laboratory biosecurity guidance*, World Health Organization, Geneva 2006.