Australian Government

Department of Health and Ageing

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

April 2013

Security Sensitive Biological Agent (SSBA) Standards 2013

ISBN: 978-1-74241-906-0
Online ISBN: 978-1-74241-907-7
Publications approval number: 10104

Copyright Statements:

Paper-based publications

© Commonwealth of Australia 2013

This work is copyright. You may reproduce the whole or part of this work in unaltered form for your own personal use or, if you are part of an organisation, for internal use within your organisation, but only if you or your organisation do not use the reproduction for any commercial purpose and retain this copyright notice and all disclaimer notices as part of that reproduction. Apart from rights to use as permitted by the *Copyright Act 1968* or allowed by this copyright notice, all other rights are reserved and you are not allowed to reproduce the whole or any part of this work in any way (electronic or otherwise) without first being given the specific written permission from the Commonwealth to do so. Requests and inquiries concerning reproduction and rights are to be sent to the Online, Services and External Relations Branch, Department of Health and Ageing, GPO Box 9848, Canberra ACT 2601, or via e-mail to *DoHA-Copyright* (copyright@health.gov.au).

Internet sites

© Commonwealth of Australia 2013

This work is copyright. You may download, display, print and reproduce the whole or part of this work in unaltered form for your own personal use or, if you are part of an organisation, for internal use within your organisation, but only if you or your organisation do not use the reproduction for any commercial purpose and retain this copyright notice and all disclaimer notices as part of that reproduction. Apart from rights to use as permitted by the *Copyright Act 1968* or allowed by this copyright notice, all other rights are reserved and you are not allowed to reproduce the whole or any part of this work in any way (electronic or otherwise) without first being given the specific written permission from the Commonwealth to do so. Requests and inquiries concerning reproduction and rights are to be sent to the Online, Services and External Relations Branch, Department of Health and Ageing, GPO Box 9848, Canberra ACT 2601, or via e-mail to *DoHA-Copyright* - (copyright@health.gov.au).

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 SSBAs and biological agents suspected of being SSBAs[1].

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.

[1] The List of Security-sensitive Biological Agents details which biological agents are considered to be security sensitive biological agents. The List can be found at *DoHA* (www.health.gov.au/ssba).

This page intentionally blank

CONTENTS

INTRODUCTION

The *National Health Security Act 2007* (NHS Act) was established to provide 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; these Standards; a National Register of Security-sensitive Biological Agents (supported by mandatory reporting); exemptions from the regulatory scheme; purposes for handling SSBAs that are considered legitimate; reporting requirements; and an inspection scheme.

SSBAs are defined to mean biological agents that are included in the List of SSBAs, established by the Minister for Health and Ageing and published on the Department of Health and Ageing (DoHA) web site. This list is defined in 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 include specific directions for dealing with biosecurity risks and issues as well as the establishment of a systematic approach to the management of the biosecurity of SSBAs.

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

- Part 1 of these Standards deals with the Scope, Normative References and Terms and Definitions. This part applies to all entities.
- Parts 2–8 of these Standards set out the requirements for entities that are handling SSBAs that have been registered with the DoHA. These parts apply to registered entities only.
- Part 9 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 9A 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 SSBAs which are being handled temporarily by a facility of a registered entity to ensure the SSBA is handled securely prior to disposal.

Because SSBAs are infectious agents or toxins, the requirements of AS/NZS 2243.3:2010 Safety in laboratories - Microbiological safety and containment, together with the other parts of AS/NZS 2243[1], need to be considered when developing plans as required by these SSBA Standards. The Commonwealth, States and Territories have occupational health and safety legislation that should be complied with when following these Standards.

[1] The Standards Australia web site (www.standards.org.au) should be consulted for the most up to date versions.

The Standards comprise:

(a) normative requirements, which are mandatory and use the word “must”; and

(b) informative requirements, which use the word “should” and comprise either recommended approaches to achieving the normative requirements, recommended extensions to them or further information about the requirement. The informative requirements should be used to develop equivalent best practice.

The normative requirements are presented in shaded boxes. Informative requirements, including any additional information or recommendations are presented as “Commentary” in *italic* text.

Electronic versions of the NHS Act, NHS Regulations and these Standards are available on the *DoHA website* – (www.health.gov.au/ssba)

Part 1 Scope and definitions

1

1.1 Scope

The NHS Act is complemented by the *National Health Security Regulations 2008* (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 handling, transport, and reporting of SSBAs and suspected SSBAs. Compliance with the NHS Act, NHS Regulations and these Standards is mandatory.

The objective of these Standards is to set requirements for the secure handling, storage, disposal (including destruction) and transport of known and suspected SSBAs.

In addition, complementary legislation, regulations and standards need to be considered when handling and transporting SSBAs. If an SSBA is of concern to quarantine authorities, then the Department of Agriculture, Fisheries and Forestry (DAFF) *Regulations for Quarantine Approved Premises* need to be addressed and registration with DAFF Biosecurity is required. Any dealings with genetically modified organisms are prohibited unless authorised by the Gene Technology Regulator. For transport of SSBAs, 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*.[1]

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 and by following AS/NZS 2243.3:2010 Safety in laboratories - Microbiological safety and containment .

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 *DoHA website* at (www.health.gov.au/ssba) or requested from SSBA (ssba@health.gov.au).

1.2 Normative references

Australian Code for the Transport of Dangerous Goods by Road and Rail (ADG Code) (current version) (Commonwealth)[2]

Civil Aviation Safety Regulations 1998 [3](Commonwealth)

National Health Security Act 2007 (Commonwealth)

National Health Security Regulations 2008 (Commonwealth)

1.3 Terms and definitions

Adverse criminal record—for the purposes of a result from a National Health Security (NHS) check, means that an individual has been convicted of a health security relevant offence and received a sentence (including a suspended sentence) of imprisonment.

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

1 All documents referenced throughout these Standards are current at the time of printing. Entities should ensure that they are using the most recent version of any document.

2 Available for free download from the National Transport Commission (www.ntc.gov.au)

3 CAS Regulations, NHS Act and NHS Regulations are available for free download from ComLaw (www.comlaw.gov.au)

Audit—means a systematic, independent and documented process for obtaining evidence and evaluating it objectively to determine the extent to which criteria are fulfilled. [Adapted from OHSAS 18001:2007]

COMMENTARY: 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 19011:2002*.*

Biological agents—include:

(a) bacteria and viruses

(b) toxins derived from biological sources, including animals, plants and microbes. [NHS Act]

Biosafety—means the containment principles, technologies and practices that are implemented to prevent unintentional exposure to biological agents, or their accidental release. [Adapted from WHO/CDS/EPR/2006.6]

Biosecurity—means the protection, control and accountability for biological agents and toxins within facilities, in order to prevent their loss, theft, misuse, diversion, unauthorised access or intentional unauthorised release. [Adapted from WHO/CDS/EPR/2006.6]

COMMENTARY: In the context of these Standards, biosecurity is restricted to SSBAs.

Competency—means having the appropriate education, training, skills and experience. [ISO 9000:2005]

Confirmatory testing – A confirmatory test is a test undertaken to confirm the suspicion that an agent is an SSBA.

Containment—means a system for confining biological agents within a defined space. [Adapted from EN 12128:1998]

Continual improvement—means a process of enhancing the SSBA management system on a regular, periodic and sustained basis in order to achieve improvements in overall SSBA management performance consistent with the organisation's SSBA management policy. [Adapted from OHSAS 18001:2007]

COMMENTARY: The process need not take place in all areas of activity simultaneously.

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) 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; or

(b) 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.

COMMENTARY:
Note 1: 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)).

Note 2: 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).

Note 3: 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.

Note 4: Under the Crimes Act 1914, a person need not disclose convictions that:
(a) have been quashed (see section 85ZT); or
(b) are spent (see section 85ZV).

Note 5: 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 that has as its primary purpose to eliminate the cause of a detected non-compliance or other undesirable situation. [Adapted from OHSAS 18001:2007]

COMMENTARY: There can be more than one cause for non-compliance. Corrective action is taken to prevent recurrence whereas preventive action is taken to prevent occurrence.

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 15190:2003]

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]

DoHA—means the Australian Government Department of Health and Ageing (www.health.gov.au).

Eligible—for the purposes of the SSBA Standards, means that a person has not received a 'qualified' or 'not eligible' result from an NHS check.

Entity—means any of the following:

(a) an individual; or

(b) a body corporate; or

(c) an agency or instrumentality of the Commonwealth, a State or a Territory. [NHS Act]

Event—means the occurrence of a particular set of circumstances. [Adapted from ISO/IEC Guide 73:2002]

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

Facility—includes:

(a) a building, or part of a building; and

(b) a laboratory (including a mobile laboratory). [NHS Act]

Handling—includes:

(a) receiving, holding, using and storing biological agents; and

(b) any operation incidental to, or arising out of, any of those operations. [NHS Act]

COMMENTARY: This meaning is affected by s 39(2) of the NHS Act. An entity that handles SSBAs only for the purpose of transporting them from one place to another place is exempt from the requirements of Division 5 of Part 3: see s 40(1) of the 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/IEC Guide 51:1999]

Hazard—means a situation or act with a potential for causing harm. [Adapted from OHSAS 18001:2007]

Hazard identification—means the process of recognising that a hazard exists and defining its characteristics. [OHSAS 18001:2007]

*COMMENTARY: This is sometimes defined as **risk identification** and involves determining what, where, when, why and how something could happen.*

Health security relevant 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.

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

(a) detention of a person until the rising of the court; or

(b) a sentence of community service.

Inactivation—means any process that:

(a) destroys the ability of a microorganism to replicate; or

(b) makes a toxin inactive. [Adapted from Health Canada, *Laboratory Biosafety Guidelines 1996*]

Incident—means a discrete event in time with the potential for causing harm.

Initial tester—means an entity that operates a laboratory 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 SSBAs.

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 SSBA (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 by AusCheck of a person's criminal history information.

NHS check—means a National Health Security check. For the purposes of the SSBA Standards, these checks consist of a national criminal history check and a national security assessment.

NHS Regulations—means the *National Health Security Regulations 2008*.

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

National security assessment—determines whether an individual has any known links to politically motivated violence, terrorism or other high-risk activities or groups. Conducted by the Australian Security Intelligence Organisation (ASIO).

Non-compliance—for the purposes of these Standards, means a failure or refusal to comply with the requirements of the NHS Act, 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 the SSBA Standards, means that a person has been found to have an adverse criminal record or an adverse or qualified security assessment.

Preventive action—means an action that is intended to eliminate the cause of a potential non-compliance or other undesirable potential situation. [OHSAS 18001:2007]

COMMENTARY: There can be more than one cause for a potential non-compliance. Preventive action is taken with the aim of preventing an occurrence whereas corrective action is taken with the aim of preventing recurrence.

Prohibited drug—means any of the following (all as defined in section 300.2 of the Criminal Code):

(a) a controlled drug; or

(b) a controlled plant; or

(c) a controlled precursor.

Qualified—for the purposes of the SSBA Standards, means that a person has been found to have a qualified criminal record.

Qualified criminal record—for the purposes of an NHS check, means that an individual has been convicted of a health security relevant offence on three or more separate occasions in the previous 10 years from the date of AusCheck providing the results of the NHS check to the entity, but has not received a sentence of imprisonment for these offences.

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

Record—means a document stating results achieved or providing evidence of activities performed. [OHSAS 18001:2007]

COMMENTARY: a document may be any written item or electronic data that meets the above requirement of a record.

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

Risk—means the chance of something happening that will have an impact on objectives.

COMMENTARY: Risk is usually a combination of the probability of occurrence of harm and the severity of that harm. [ISO/IEC Guide 51:1999]

Risk assessment—means a process of evaluating the risk(s) arising from a hazard(s), taking into account the adequacy of any existing controls and deciding whether or not the risk(s) is acceptable. [OHSAS 18001:2007]

Safety—means freedom from unacceptable risk. [ISO/IEC Guide 51:1999]

Sample of a biological agent—includes:

(a) a subculture of the agent; and

(b) a preparation made of the agent. [NHS Act]

Sensitive information—means any of the following:

(a) an entity's storage records for the SSBA handled at the facility;

(b) an entity's risk assessment plan for the SSBA agent handled at the facility;

(c) an entity's risk management plan for the SSBA handled at the facility;

(d) any other information that the entity identifies as being sensitive information under clause 5.3 of the SSBA Standards because it could compromise the security of the SSBA handled at the facility. [Adapted from NHS Regulations]

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

SSBA Standards—means the 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 SSBA. [Adapted from the NHS Act].

Temporary handling—means the handling of a known SSBA by a non-registered entity 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.

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 biosecurity risk and must be tightly regulated. The Minister for Health may vary this list from time to time. The current list is published on the Department of Health and Ageing web site (www.health.gov.au/ssba).

Tier 2 SSBAs—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 Minister for Health may vary this list from time to time. The current list is published on the Department of Health and Ageing web site (www.health.gov.au/ssba).

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 in regards to 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 SSBAs 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.

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 9000:2005]

Verification—means confirmation, through the provision of objective evidence, that specified requirements have been fulfilled. [Adapted from ISO 9000:2005]

Vulnerability analysis—means the determination of how each credible threat can be realised against critical assets. [Adapted from HB 167:2006]

COMMENTARY: This involves determining:

(a) potential means by which a successful "attack" against an asset could be carried out; and

(b) the effectiveness of each of the layers of security in managing this "attack" against the assets, people, information or infrastructure (including SSBAs).

This page intentionally blank

Part 2 Risk and incident management

2

2.1 Objective

(1) To ensure that all known biosecurity risks in relation to the SSBAs handled by the entity are identified and managed through risk assessment and risk management plans prior to commencement of SSBA related work.

COMMENTARY: The risk assessment and risk management plan processes are critical for managing the security requirements in the rest of these Standards. Tier 1 SSBAs are those that pose the highest biosecurity risk and are subject to the highest level of security and reporting, while Tier 2 SSBAs pose a high biosecurity risk and are subject to proportionately high security and reporting. Therefore, the risks identified for Tier 1 versus Tier 2 SSBAs may be different and the risk management plan should reflect these differences.

AS/NZS ISO 31000:2009 Risk management – Principles and guidelines *and* HB 167:2006 Security risk management *should be consulted regarding the risk assessment processes and the development of plans for managing the risks.*

2.2 Risk assessment

2.2.1 Timing and scope

(1) The entity must ensure that the scope, nature and timing of the risk assessment is proactive rather than reactive.

COMMENTARY: The roles and responsibilities of personnel who perform and verify work affecting risk management should be defined and documented.

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 2.5.

2.2.2 Hazard/risk identification

(1) The hazards/risks associated with handling the SSBA must be identified and documented.

(2) At a minimum the following hazard/risk should be identified and documented for inclusion into the risk assessment document at clause 2.2.3:

(a) determination of the potential for and possible causes of an incident, including those listed as reportable events;

(b) human behavioural risks (see also clause 3.10);

(c) periods of reduced staff availability (for example, during weekends and holiday periods);

(d) identifying potential emergency situations involving SSBAs to:

- prepare for their occurrence and to limit possible illness or

other damage that may be associated with them;

- ensure 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; and
- identify risks surrounding the safe removal, transport, treatment and accommodation of contaminated people or objects.

COMMENTARY: Hazards/risks to be identified should include what can happen, when and where it can happen, and how and why it can happen.

Some examples of potential hazards are:

- *theft of SSBAs;*
- *failure to properly screen staff;*
- *loss of records required to remain secure (for example, inventories);*
- *infection of personnel or visitors with an SSBA;*
- *disgruntled personnel causing a non-compliance or theft of an SSBA;*
- *inadequate access control and/or physical security allowing unauthorised access to SSBAs or secure records;*
- *inability of the entity to properly account for the storage or handling of an SSBA; and/or*
- *loss of an SSBA during transport.*

Any hazards/risks identified may require further assessment under the risk assessment and risk management processes to ensure that they are adequately managed. Hazards/risks can be documented as part of the risk assessment and risk management plans.

2.2.3 Risk assessment process

(1) The entity must undertake and document a risk assessment for the SSBAs handled and the facility/facilities in which they are handled.

(2) At a minimum the risk assessment must include the following:

(a) communication and consultation plans with internal and external stakeholders;

the internal, external and security risk context;

the risks identified under Clause 2.2.2 (2);

analysis of the 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 also part 4 of these Standards);

iii. effectiveness of the processes for decontamination/inactivation of contaminated and potentially contaminated items (see also 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 2.3).

for Tier 1 SSBAs, a vulnerability analysis.

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

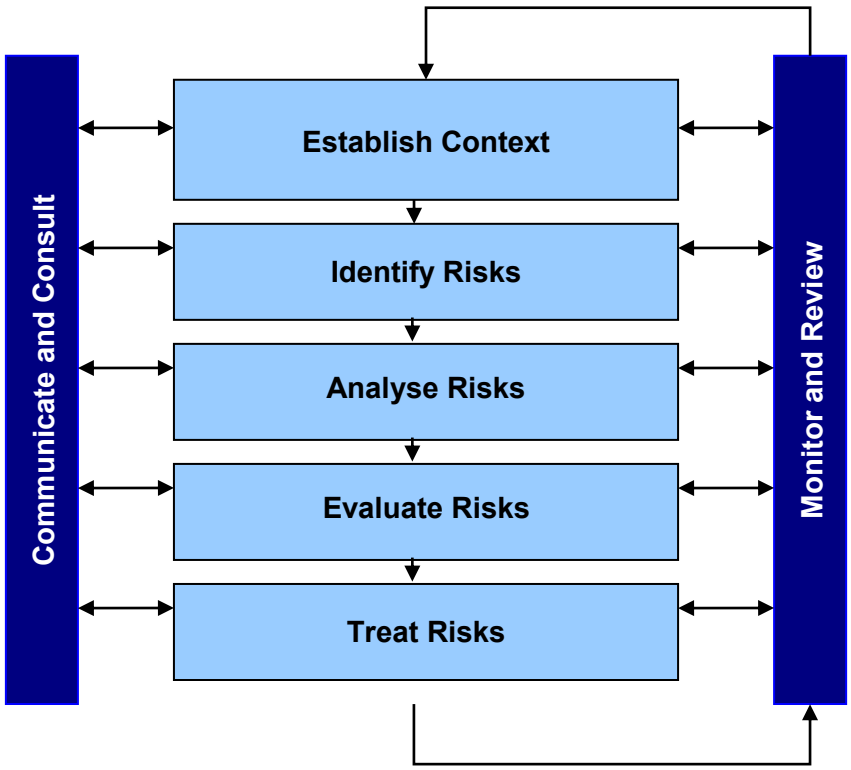

Figure 1 - Illustration of the Risk Assessment process

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:

- *The 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.*
- *The 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 what needs to be communicated and to whom.*

- *The communication methods (e.g. formal documents, emails, newsletters, verbal communications etc).*
- *Evaluations of the effectiveness of the communication.*
- *Timeframes.*

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.

In the event of an emergency or unforseen event there may be disruption to normal operating conditions. The risk assessment should address the need for adequate redundancy, replacement or other measures such as alternative means of decontamination in the case of an autoclave failure, maintenance of physical security systems in power outage, or a complete secure shutdown of operations in extreme circumstances. Australian Standard AS3745:2010 – Planning for emergencies in facilities may be useful as a reference guide.

The risk assessments 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.

The Department of Health and Ageing has developed a template to assist with risk assessment and risk management. The Security Risk Template is available through the DoHA web site at (www.health.gov.au/ssba).

The vulnerability analysis should be performed utilising guidelines found in HB167:2006. *A vulnerability is defined as any weakness that can be exploited to make an asset susceptible to change (HB 167:2006). 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 are the consequences of the attack, 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.

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

2.3 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 Subclause 2.2.2 and

plans for monitoring and review of the risk management process.

(2) The risk management plan must be effectively communicated to all personnel handling SSBAs or sensitive information relating to SSBAs and to others as relevant.

(3) As part of the risk management plan, standard operating procedures (SOPs) for secure handling of SSBAs must be developed, documented and implemented.

COMMENTARY: In treating risks, options for controlling the risks need to be identified and these options assessed. From this, treatment and implementation plans are prepared. The 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 depend on personnel compliance at all times to work effectively, are the least effective controls to manage risk.

Management plans can be monitored by regular review, 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.

The areas of the risk management plan communicated to personnel and others should be those relevant to the activities undertaken, for example risk management plans relating to decontamination should be related to all personnel handling SSBAs 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 SSBAs 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.

2.4 Incident management

(1) The entity must establish, document and maintain procedures to define, report, record and analyse incidents involving SSBAs, 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.

(2) Analysis must include:

(a) determining the cause(s) of incidents;

evaluating the need for corrective action to ensure that incidents do not re-occur;

determining and implementing the action needed;

recording results of action taken; and

reviewing the effectiveness of the corrective action taken.

(3) The entity must put in place processes to encourage learning from incidents involving SSBAs.

COMMENTARY: 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 accident is an incident which has resulted in harm. An incident where no harm is caused may also be referred to as a "near miss", "near hit", "close call" or "dangerous occurrence". An emergency situation is a particular type of incident.

Communication of what constitutes an incident should be included in the risk communication plan developed under clause 2.2.2.

Incidents involving SSBAs may or may not be reportable events or non-compliances under the NHS Act, NHS Regulations or these Standards. Incidents that are reportable events, as defined by the NHS Act and the NHS Regulations, must be reported to DoHA and to jurisdictional law enforcement (if required by the NHS Act, NHS Regulations or these Standards) as per the timeframes set out in the NHS Regulations, and to any other appropriate authorities. Whether reportable or not, incidents should be addressed by corrective action and findings from investigations of incidents should be used to educate staff.

2.5 Review

(1) The entity must ensure that the risk assessment and risk management plan are reviewed at least every 12 months for risks involving Tier 1 SSBAs and every two years for risks involving Tier 2 SSBAs or more frequently as required. Outcomes of the review must be documented.

COMMENTARY: 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.

It may be necessary to undertake a review more frequently (i.e. more than every year or two years), for example:

- *following an incident;*
- *when there are changes in SSBAs handled;*
- *when there are changes in procedures;*
- *when national threat levels change*[6]*;*
- *at the request of DoHA.*

[6] Information about the national threat level can be found at Australian National Security (www.nationalsecurity.gov.au). Changes in the threat level will be communicated to entities by DoHA.

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.

This page intentionally blank

Part 3 Personnel

3

3.1 Objective

(1) To have personnel management systems in place to implement and manage the security of SSBAs 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.

(2) 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;

overseeing internal review, audit and reporting measures to provide assurance that the requirements of these Standards are being met and maintained;

verifying, in conjunction with other relevant personnel, that all known SSBA risks have been addressed;

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 8.3);

ensuring that all work relating to SSBAs is conducted in accordance with established policies, SOPs, the NHS Act, the NHS Regulations and these Standards;

advising top management as to whether staff levels, facilities and equipment are sufficient to effectively carry out work involving SSBAs in accordance with technical protocols, approved policies and SOPs;

maintaining lists of authorised and approved persons. The list must include:

i. the period for which the person is authorised or approved;

ii. the review date of the authorisation or approval; and

iii. what they are authorised or approved for.

any other responsibilities allocated under these Standards.

(3) The entity must only appoint as a Responsible Officer and Deputy Responsible Officer a person who is an authorised person under clause 3.3.1 of these Standards.

COMMENTARY: 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 choose to appoint one Responsible Officer and one Deputy Responsible Officer for each facility or have a Responsible Officer/ Deputy Responsible Officer who is responsible for multiple facilities.

Lists of authorised and approved persons may be kept in hard copy and/or electronic form.

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

3.3 Authorised persons

(1) The entity must authorise all unescorted or unsupervised persons in order for a person to:

(a) handle SSBAs;

access the facility where SSBAs are handled; or

access sensitive information related to SSBAs (unless the person meets the requirements in line with Part 5 of these Standards.

(2) The entity may choose to authorise a person to do all of the above or may choose to limit the authorisation to any combination of the above.

(3) A person's status as an authorised person is limited to the entity in relation to which it is given and cannot be transferred between entities.

(4) Students who handle SSBAs must become either authorised persons or approved persons (see also clause 3.4), depending on the requirements of the facility.

(5) An entity must revoke a person's authorisation if that person no longer has a need to handle SSBAs, access a facility where SSBAs are handled or access sensitive information relating to SSBAs (see also clause 3.11).

COMMENTARY: For definitions of 'eligible', 'qualified' and 'not eligible' under the SSBA Standards, see Terms and Definitions under Part 1.

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.

A person's status as an authorised person is limited to the entity as training procedures will be specific to that entity. However, for personnel who work in more than one entity or who move between entities, the results of NHS checks may be verified through AusCheck for the purposes meeting the requirements of clause 3.3 (see also clause 3.6).

3.3.1 Authorisation of a person

(1) An entity must only authorise a person who:

(a) has been trained in the requirements listed under subclause 3.9.1 as relevant to their authorisation (see also clause 3.3 for authorisation categories);

has signed, dated and provided to the entity a record of the training referred to in 3.3.1(a) above;

has not been excluded from handling SSBAs by the entity nor

directed not to handle SSBAs by the Secretary of the DoHA;

has undergone an identity check (clause 3.5);

is 18 years or over; and

if required under these Standards to have an NHS check (clause 3.6), holds a current 'eligible' or 'qualified' NHS check result.

3.3.2 Authorisation of a person with an NHS check

(1) If a person to be authorised has undergone an NHS check (clause 3.6) (even if not required under clause 3.6) then the following requirements also 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.

if the person received an NHS check result of 'qualified', the entity must not authorise the person for more than 12 months. Following this period, the person must undergo a new NHS check before they can be re-authorised.

if the person received an NHS check result of 'not eligible', the entity must not authorise the person.

COMMENTARY: Even if a person receives an NHS check finding 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.

When deciding if a person is to be re-authorised following a new NHS check, the entity may choose not to re-authorise the person until they have undergone refresher training on the requirements of the NHS Act, NHS Regulations and the SSBA Standards and provided a record of that training to the Responsible Officer.

3.4 Approved persons

(1) The entity must establish, document and implement processes to ensure that contractors, visitors, suppliers, students and other such persons do not compromise the facility's SSBA security. These processes must include policies and procedures for the approval of persons who need to:

(a) handle SSBAs;

(b) access the facility where SSBAs are handled; and/or

(c) access sensitive information related to SSBAs.

(2) The entity may choose to approve a person to do all of the above or may choose to limit the approval to one or any combination of the above.

(3) For facilities handling Tier 1 SSBAs, approved persons must be escorted by an authorised person at all times.

(4) For facilities handling Tier 2 SSBAs, approved persons must be supervised by an authorised person at all times. The degree of supervision of and responsibility for an approved person by an authorised person must be determined through and documented in the risk assessment.

(5) Students who handle SSBAs must become either authorised persons (see clause 3.3) or approved persons depending on the requirements of the facility.

(6) An entity must revoke a person's approval if that person no longer has a need to handle SSBAs, access a facility where SSBAs are handled or access sensitive information relating to SSBAs (see also clause 3.11).

COMMENTARY: Escorted is taken to mean that the approved person should remain in line of sight of the authorised person escorting them while the approved person is within the secure area or handling sensitive information.

Supervision is taken to mean that an authorised person is responsible for the approved person within the facility or when accessing sensitive information.

When determining the degree of supervision for an approved person, the risk assessment should take into account factors such as the set up of the facility, the SSBA involved, the role of the approved person and the results of an NHS check (if undertaken).

For example, following the risk assessment it may be determined that as an approved person has access to locked storage facilities containing Tier 2 SSBAs 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 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 choose to restrict 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 SSBAs, even when under escort or supervision by the authorised person.

Supervision plans 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 Identity check

(1) The entity must conduct an identity check on a person prior to authorising the person under clause 3.3. The purpose of the identity check is to establish that a person is who they claim to be.
(2) If an NHS check is to be conducted (clause 3.6), the identity check must be completed prior to the submission of the NHS check application to AusCheck.
(3) The entity must ensure that the documentation provided for proof of identity by a person includes:

(a) evidence of commencement of identity in Australia;

(b) linkage between identity and the person;

(c) evidence of operation in the community; and

(d) evidence of residential address.

(4) The documentation to satisfy criteria a – d can be found at Table 1 – Proof of Identity Documents.

(5) The entity must keep a record of which documents are provided.

COMMENTARY: Identity checks are recommended for persons who will be approved persons, especially if they will have regular access to the SSBA, the facility in which the SSBA is handled or to sensitive information relating to the SSBA.
It is important that the identity check is completed for both new and any current personnel who are to be authorised under clause 3.3, even if the person has been employed by the entity for a period of time.

Documentation that is used in an identity check should be able to be linked to the person. This will be especially important for persons who may use more than one name (for example – a person who uses their married name as well as their maiden name or a person who has a title or honorific that may be used in some documentation but not in others). Entities should take steps to check the validity of documents by checking security marks (for example water marks), checking for signs of tampering and, if possible to do so, checking with the relevant issuing authority that the credential is valid. Documentation provided should either be an original document or a certified copy. Records of which document was provided may be a record of the type of document with the document's ID number (if available), it does not need to be a copy of the document itself.

Table 1 – Proof of Identity Documents

Category of document	*Documents that satisfy the criteria*

a) – Evidence of commencement of identity in Australia	• *Birth certificate*
	• *Record of immigration status*
	  ○ *Foreign passport and immigration visa*
	  ○ *Travel documents and current Australian visa*
	  ○ *Certificate of evidence of residential status*
	  ○ *Citizenship certificate*

b) – Linkage between identity and person *(should include a photo and signature)*	• *Australian drivers licence (current)* • *Australian passport (current)* • *Firearms licence (current)* • *Foreign passport*
c) – Evidence of identity operating in the community	• *Medicare card* • *Document that provides evidence of a change of name (for example a legal name change document such as a Deed Poll) showing link to previous name* • *Credit or account card*

	• *Government issued concession card* • *Births, Deaths and Marriages (BDM) issued marriage certificate* • *Tertiary student ID card*
d) – Proof of residential address (if not supplied under categories a, b or c)	• *Utility notice* • *Rental notice*

Table 1 adapted from the Gold Standard Enrolment Framework.

A person may only need to supply one document from each of categories a to c to satisfy the requirement of clause 3.5. A document from category d will only need to be supplied if proof of residential address does not form part of the documentation supplied for categories a to c.

3.6 National Health Security (NHS) checks

(1) The entity must apply to AusCheck for an NHS check of all persons that it is considering authorising to handle Tier 1 SSBAs, to access a facility where Tier 1 SSBAs are handled or to access sensitive information relating to Tier 1 SSBAs*, except those who currently hold a national security clearance of Negative Vetting Level 1, Negative Vetting Level 2.or Positive Vetting. An NHS check consists of a national criminal history check, against the list of health security relevant offences set out in Appendix 1 of these Standards, and a national security assessment.

** Note: some persons may be able to access sensitive information relating to Tier 1 SSBAs without undergoing an NHS check or holding a national security clearance if they meet the requirements in line with Part 5 of these Standards.*

(2) At the time of applying for an NHS check, the entity must supply AusCheck with a recent photograph, taken by the entity, of the person to undergo an NHS check.

(3) The entity must take into account the results of the NHS check as notified by AusCheck as part of the assessment of a person's eligibility to become an authorised person under clause 3.3.

(4) The entity must ensure that NHS checks are conducted at intervals of no greater than two years to maintain eligibility for authorised person status under clause 3.3. Under certain circumstances, NHS checks will be required every 12 months to maintain eligibility for authorised person status (see clause 3.3).

(5) An NHS check undertaken under this clause is valid for the entity that requested the check.

(6) The entity must have in place 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.

COMMENTARY: Although an NHS check is only mandatory in respect of a person who the entity is considering authorising to handle Tier 1 SSBAs, access facilities handling Tier 1 SSBAs or access sensitive information relating to Tier 1 SSBAs, it is recommended that all persons who will be authorised to handle Tier 2 SSBAs, access a facility that handles Tier 2 SSBAs or sensitive information relating to Tier 2 SSBAs undergo an NHS check. This assists in providing another layer of security to reduce the risk of persons with malicious intent gaining access to the SSBA, the facility or to sensitive information.

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. Information about the specific requirements of the photograph can be found under Frequently Asked Questions on the AusCheck website – (www.ag.gov.au/AusCheck).

AusCheck is required to destroy criminal history information received from CrimTrac after six months, unless subject to review by the Administrative Appeals Tribunal. Other information, such as personal details, is retained under the Archives Act 1983 and subject to the Attorney-General's Department record disposal arrangements. Personal information is subject to the Privacy Act 1988 and AusCheck is required to apply strict privacy controls to all areas of operation.

Changes in 2010 to the national security clearance protocols have resulted in changes in the nomenclature of national security clearances. From 1 October 2010, clearance levels previously named as Confidential, Secret and Top Secret have the following nomenclature:

- *Confidential and Secret are now Negative Vetting Level 1.*
- *Top Secret is now Negative Vetting Level 2.*
- *Positive Vetting is the highest level of clearance.*

These security clearances are managed by the Australian Government Security Vetting Agency (AGSVA) through the Department of Defence. If you require more information on any impact these changes may have on the security clearances within your entity, you should contact your entity's security advisor. Further information can also be obtained through the AGSVA website – (www.defence.gov.au/agsva).

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 3.3.2 and do not have to undergo an NHS check.*

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

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 from DoHA (www.health.gov.au/ssba).

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.

COMMENTARY: 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) a person who has undergone an NHS check must report any new convictions that is a kind of offence listed in Appendix 1, to the entity within two business days of being informed of the conviction; and

b) the entity must inform AusCheck of the information reported under 3.6.2(a) within two business days from being informed of the conviction.

(2) As soon as the above is reported to the entity, the entity must suspend the person's authorised status pending the outcome of a new NHS check.

COMMENTARY: 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 SSBAs, access the facility where SSBAs are handled or access sensitive information relating to SSBAs 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.

3.7 Provisional authorisation

(1) An entity may provisionally authorise a person to become a Responsible Officer, Deputy Responsible Officer, handle SSBAs, access a facility where SSBAs are handled or to access sensitive information relating to SSBAs if:

(a) the person is to undergo an NHS check;

(b) the requirements of paragraphs (a) to (e) of clause 3.3.1 have been met; and

(c) the relevant facility has no authorised persons (as under clause 3.3) in place.

(2) For an entity/facility that has not previously registered with AusCheck, an NHS check must be commenced 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.

COMMENTARY: The provisional authorisations outlined in clause 3.7 are temporary arrangements for newly registered entities/facilities to enable persons to handle SSBAs, access a facility where SSBAs are handled or access sensitive information relating to SSBAs, 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 DoHA during the entity/facility registration process.

Persons who commence handling SSBAs, who access the facility where SSBAs are handled or access sensitive information relating to SSBAs 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.

For entities that have multiple facilities handling SSBAs, AusCheck will register each facility as an 'entity' within their system. Registering each facility as an 'entity' ensures that applications, and any subsequent correspondence, are sent to the relevant contacts within the facility. These administrative arrangements are for NHS checks only and have no effect on the registration status of the entity/facility with the DoHA SSBA Regulatory Scheme.

3.8 Recruitment

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

COMMENTARY: AS 4811:2006 Employee screening *and* HB 323:2007 Employment Screening Handbook *should be consulted for guidance on staff recruitment. Some checks will require consent from the applicant.*

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 regards to checking a person's work entitlements and visa conditions can be obtained from the* Department of Immigration and Citizenship – (www.immi.gov.au).

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.

3.9 Training and competency

(1) The entity must ensure that all personnel who have responsibilities or perform tasks that may impact on SSBAs have the 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;

provision of required SSBA training;

determination of the effectiveness of SSBA training;

provision of SSBA refresher training;

restrictions on staff to ensure they do not perform tasks for which they are not trained; and

records management including the maintenance of adequate records.

COMMENTARY:

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.

The entity should 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. 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.

3.9.1 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:

- An overview of the NHS Act and Regulations and why the SSBA Regulatory Scheme is in place.
- Reporting requirements.
- Records management.

(b) For persons who will handle SSBAs:

- The requirements of the NHS Act, NHS Regulations and all parts of the SSBA Standards.

(c) For persons who will access the facility where SSBAs are handled, training on the following parts of the SSBA Standards:

- Physical security.
- Risk Management.
- Information security.
- Personnel security.
- Management system requirements.

(d) For persons who will access sensitive information relating to SSBAs, training on the following parts of the SSBA Standards:

- Risk Management
- Information security
- Personnel security
- Management system requirements.

(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 SSBAs, such as policies and procedures for handling SSBAs and sensitive information, requirements for supervision or escorting approved persons etc.

(3) Training for personnel handling Tier 1 SSBAs must include personal security awareness.

(4) Entities may choose to impose further training requirements on each category of authorisation.

COMMENTARY: 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 SSBAs.*

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 SSBAs. Information about this training material can be obtained by contacting the* SSBA Regulatory Scheme *at* SSBA (ssba@health.gov.au)*.*

Personal security awareness is concerned with staff security during off-duty hours away from the facility. During these times, staff members may be vulnerable because of their function or position. 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 SSBAs may also include personal security awareness.

3.9.2 Competency levels

(1) The entity must define required competency levels, including the appropriate technical competencies to handle SSBAs 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 SSBAs, competencies of personnel must be reviewed at least annually. For facilities handling Tier 2 SSBAs, competencies of 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.

*COMMENTARY: Technical competency is taken to mean that the personnel have worked at the Physical Containment Level (*AS/NZS2243.3:2010*) for the relevant risk group of the SSBA and have demonstrated competency in the procedures required at that level.*

3.10 Behavioural factors

(1) The entity must establish and implement measures to address risks

associated with human behaviour, including reliability, of persons who handle SSBAs, access a facility where SSBAs are handled or access sensitive information relating to SSBAs.

(2) These measures must be documented as part of risk assessment and management processes, and evidence of their application recorded.

COMMENTARY: 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 SSBAs is the possibility of a "trusted insider" accessing the SSBAs 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 frailties, 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; and*
- *respect for individual privacy and dignity*

HB 323—2007 Employment Screening Handbook *may be consulted for guidance on personnel reliability policies.*

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.

A guideline on Indicators of Suspicious Behaviour in Laboratories Handing SSBAs *is available on request from SSBA (ssba@health.gov.au).*

3.11 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 SSBAs from the Secretary of the Department of Health and Ageing.

(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 SSBAs held in linked storage units (see Part 4A);

prompt removal of access to sensitive information relating to SSBAs;

suspension or revocation of a person's authorised or approved status; and

immediate physical removal of personnel if deemed necessary.

COMMENTARY: 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.

This page intentionally blank

Part 4 Physical security

4

4.1 Objective

(1) To have in place physical security measures, based on requirements identified in the risk assessment and risk management plan, to minimise the risk of unauthorised access to SSBAs.

COMMENTARY: SSBAs might be found as cultures, 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 SSBAs are handled.

(2) External walls that form part of the secure perimeter must be of solid construction and physically sound. External doors of the secure perimeter must be self-closing and suitably protected against unauthorised access with control mechanisms.

(3) 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. Windows must be non-opening and sealed at all times.

(4) Unauthorised recording, photography or filming must be prohibited within the secure area. Policies on this prohibition must be documented.

(5) For the physical security requirements for linked storage units, see clause 4A.5.

COMMENTARY: The location and strength of the perimeter should depend on the security requirements of the SSBAs contained within the secure area and the results of risk assessment. To ensure that the exact location of the secure perimeter is understood, it is recommended that the entity uses a marked floor plan to assist in defining the secure area. 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 area within the secure perimeter must be either an authorised or approved person and is subject to the requirements of the NHS legislation. 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 be alarmed at all times.

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 could be sought from State or Territory Police Counter-terrorism and Infrastructure Protection branches, the Australian Security Intelligence Organisation Protective Security and T4 Branch or professional security consultants.

Video monitoring of access points should be considered for Tier 1 SSBAs, 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.

4.2.1 Stand-alone facilities

(1) A facility that is a stand-alone facility 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 easily transportable;

(c) have barriers to prevent vehicles from approaching the facility;

(d) have good external lighting; and

(e) conduct regular inspections to ensure that the outer walls have not been tampered with. Outcomes of these inspections must be documented.

Mobile laboratories, such as police forensic mobile laboratories, are not subject to the requirements of this clause.

COMMENTARY: A stand-alone facility is 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). These laboratories are subject to additional risks, especially relating to access and security.

4.3 Physical access controls

(1) Access to secure areas containing SSBAs 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 SSBAs.

(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 SSBAs, the time of exit from the secure area (specific to the person) must also be recorded.

(5) Access control records must be kept in line with Part 5 of these Standards.

(6) Access control systems must be tested at least every 6 months for Tier 1 SSBAs and at least annually for Tier 2 SSBAs.

(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 Responsible Officer must ensure that access to the area is removed (for example, by deactivation of card access or returning of keys).

COMMENTARY: Clauses 3.3 and 3.4 respectively refer to authorised persons and approved persons (for example, contractors/visitors/suppliers). Exit control and recording should be by a pass back control reader on the secure side of the access door.

Records of access, as outlined above, may be kept in either electronic or hard copy form.

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 should determine how access is handled in emergencies and policies documented and 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.

"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.

The additional access control to further control access to Tier 1 SSBAs does not have to be at the secure perimeter but may be within the secure area itself. For example, 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.

Part 4A Storage

4A

4A.1 Objective

(1) To ensure that SSBAs are stored securely to reduce the risk of unauthorised access.

COMMENTARY: Secure storage may include storing SSBAs in a dedicated locked freezer, a dedicated locked liquid nitrogen storage tank or locked containers within these devices.

4A.2 Working cultures and Toxin Extracts

(1) The entity must have in place documented policies and procedures to track the creation of working cultures from SSBAs held in long term storage and to track and control the distribution of working cultures and toxin extracts of SSBAs.

COMMENTARY: Requirements for access controls to working (active) SSBAs should be determined as part of the risk assessment.

The entity is not required to record the 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, 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.

4A.3 SSBA inventory

(1) The entity must establish and maintain an accurate and up-to-date inventory of any SSBAs held in storage. The inventory must identify and document which SSBAs are held by the entity and the location of each of the storage containers of the SSBAs.

(2) The entity must ensure that measures are put in place to minimise the quantities of SSBAs stored.

COMMENTARY: Inventory records are not intended to capture working cultures where the sample size may change on a day to day basis.

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.

The inventory may be held electronically.

There is less risk when the range and amount of SSBAs 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, or if required for diagnostic purposes, then reduced to the required reference quantities.

4A.3.1 Audit of inventory

(1) The entity must ensure that an audit of the inventory is conducted at predetermined intervals, determined through risk assessment, and at a level and frequency such that materials can be accounted for. The results of this audit must be documented.

COMMENTARY: Additional audits of inventories may occur outside the predetermined intervals, for example when there are changes such as transfer of inventories to new areas, changes in who is responsible for the inventory, changes in the risk assessment or threat level.

4A.4 Storage of Tier 1 SSBAs

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

4A.5 Storage of Tier 2 SSBAs

(1) An entity may store Tier 2 SSBAs in a storage unit that is either 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.

(2) The entity must ensure that the SSBAs are only handled in the linked storage unit for the purpose of storage or preparation for storage.

(3) If the storage unit is linked to the facility then it:

(a) must be within the same building as the facility, preferably on the same floor;

(b) must be included as part of the registration of the facility;

(c) must be included in the risk assessment and risk management plans for the facility; and

(d) must be fixed in place or non-transportable.

4A.5.1 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. Records of access must be kept in line with Part 5 of these Standards.

(2) 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.

(3) 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).

COMMENTARY: The point at which access is recorded should be at the final access control barrier to the SSBA. For example: if the 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.

Storage units that may be easily transportable, for example locked boxes or wheeled cabinets should be secured to a larger structure to prevent easy removal.

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

(1) Transport of SSBAs 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 SSBAs between the linked storage unit and the registered facility but does not need to report these movements to DoHA.

4A.6 Record keeping

(1) The entity must ensure that records relating to the storage, inventory and transport of SSBAs, are current, complete and stored securely with adequate backup. These records must be kept in accordance with clause 5.2 of these

Standards.

COMMENTARY: Records may be kept either as hard copies or as electronic data.

Part 5 Information management

5

5.1 Objective

(1) To ensure that information, including sensitive information, relating to the security of SSBAs is current, complete and stored securely.

COMMENTARY: The information generated by a facility can be as valuable or dangerous as the SSBA stored. 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 records of:

- receipt;
- holding;
- transport;
- disposal;
- decontamination and inactivation;
- policies and procedures;
- internal and external reviews;
- inspections;
- incident investigations; and
- risk assessment and risk management plans.

(2) Records must be kept for a minimum of 5 years for Tier 1 SSBAs and 2 years for Tier 2 SSBAs unless otherwise specified in these Standards.

(3) The entity must develop and document policies for access to and retention of these records and for their destruction, including timeframes, consistent with these Standards.

COMMENTARY: 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 their responsibilities under the NHS Act, including the requirements to make records available for the purposes of inspections.

Entities should be aware of other legislation related to the storage of records.

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).

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 Commonwealth agency, it will be subject to the provisions of the Information Privacy Principles (IPPs) *contained in the* Commonwealth Privacy Act 1988 (Privacy Act).

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* National Privacy Principles (NPPs) *contained in the* Privacy Act.

Records may be kept either as hard copies or as electronic data.

5.3 Information security

(1) The entity must identify and document what is considered by the NHS Regulations as sensitive information relating to the security of SSBAs. This documentation may be part of a larger document, such as the risk assessment and risk management plan.

(2) A review and approval process must be used to control access to such information. Access to such information must be limited to those who need to know and have been permitted such access by the Responsible Officer, and must be controlled at all times.

(3) Access permissions must be reviewed at least every 6 months for facilities handling Tier 1 agents and at least annually for facilities handling only Tier 2 agents. Outcomes from the review must be documented.

(4) Sensitive information relating to Tier 1 SSBA must be stored in a secure system and securely backed up at regular intervals.

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

- *the entity's storage records for the SSBAs handled at the facility;*
- *the entity's risk assessment for the SSBAs handled at the facility;*
- *the entity's risk management plans for the SSBAs handled at the facility; and*
- *any other information that the entity identifies as being sensitive information because it could compromise the security of the SSBA 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 or identity checks.*

- *Incident reports that may indicate vulnerability in the security of an SSBA.*

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

Sensitive information may either be in hardcopy or information saved on electronic or other media.

At a minimum, procedures addressing information security should consider:

- *secure storage of all sensitive records, including electronic records and electronic signatures;*
- *computer security including robust internet firewalls and encryption protocols;*
- *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;*
- *destruction of unwanted paper files and complete erasure of unwanted electronic files;*
- *security measures and procedures; and*
- *adequate backup strategies for sensitive electronic data, including keeping backup copies at other secure locations, either within the entity or externally.*

ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management *should be consulted to assist the entity in developing its guidelines.*

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 all accesses to the information itself, unless warranted by the risk assessment.

See Subclause 8.4.2 for more information regarding records, documentation and data control.

5.3.1 Provision of sensitive information to other regulatory authorities

(1) The entity may provide information deemed as sensitive information under the *National Health Security Regulations 2008* (see also Clause 5.3) to persons from the regulatory authorities listed under clause 5.3.1(2) 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) State or Territory or Federal law enforcement.

(d) Any other authority approved in writing by the Department of Health

and Ageing.

(3) Information must only be supplied under the following conditions:

(a) The regulatory authority has a need to know 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 supplied to the regulatory authority.

COMMENTARY: From time to time 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.

Before 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.

Any information that is supplied to the regulatory authority electronically should have measures in place, where possible, to prevent copying. Hard copies should be clearly marked as copies with the appropriate security classification indicated.

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.*
- *Ensuring a clear desk policy.*
- *Destroying information using a Class B shredder or* ASIO *approved destruction service.*

5.4 Disposal of records

(1) The entity must ensure that there are documented policies and procedures in place for the disposal of records consistent with the requirements of Clause 5.2 and Subclause 8.4.2.

COMMENTARY: This policy should include electronic records as well as paper and other types of records.

Part 6 Transport

6

6.1 Objective

(1) To have policies and procedures in place for the secure movement of SSBAs.

COMMENTARY: Policies and procedures should cover all relevant forms of transportation of the SSBA, including walking an SSBA to another facility.

These Standards apply to the transport of SSBAs within Australia. Imports of SSBAs that are of concern to DAFF *will require an import permit from DAFF. Imports of ricin require a permit from the* Australian Safeguards and Non-Proliferation Office *under the provisions of* the Customs (Prohibited Imports) Regulations 1956. *Exports of SSBAs require a permit from the* Department of Defence (Defence Export Control Office*) 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 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 number or consignment number, together with details of the transport agent and the expected time of delivery*)* at the time of shipment;

d) immediately informs DoHA and State/Territory police if the shipment is lost in transit (once the facility is aware of the loss); and

e) immediately informs DoHA and State/Territory police if the shipment is reported as an unsuccessful transfer by the receiving facility (once the facility is aware of the unsuccessful transfer).

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

The transport of SSBAs 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. SSBAs are transported as Class 6 dangerous goods; toxins are Division 6.1 and infectious substances are Division 6.2.*

In addition, air transport consistent with the IATA Dangerous Goods Regulations *is permitted by the* Civil Aviation Safety Regulations. *These are updated regularly*

and a current version should be consulted. SSBAs usually fall into Category A infectious substances and require packing in accordance with Packing Instruction 602. Personnel that pack the SSBA for shipment are required by the Civil Aviation Safety Regulations to have current training in shipping dangerous goods.

A record of acceptance for confirming that the receiving facility is willing to accept the shipment may be a phone log, file note, log book note or other such record.

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 documents, has been received; and

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 6.2 (a));

(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; and

(d) immediately reports the loss to the sending facility, DoHA and State/Territory police if a shipment is lost in transit.

COMMENTARY: 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 DoHA*, as required under the* NHS Regulations. *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.*

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 SSBAs, the entity responsible for the sending facility 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.

(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: policies (including response to higher threat conditions and new employee/employment verification); training; and 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 SSBAs, 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.

COMMENTARY: 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 may supply the transport agent with a copy of the Standards requirements and request that the transport agent supplies, in writing, an assurance that these requirements have been met in the transport security plan.

It is recommended that where possible the transport agent is a Security Construction and Equipment Committee (SCEC) endorsed courier.

6.4 Transport of SSBAs 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 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.

COMMENTARY: 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 4A.5.1). 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 SSBAs. The transport risk assessment should cover when double or triple packaging must be used.

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 *should be consulted for determining minimum packaging requirements.*

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.

6.5 Transport of SSBAs 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 must occur within a single building only;

(b) Transport may only be between the reception area and the registered facility

(c) The person handling the SSBA must do so only for the purposes of receiving the package and transporting to the registeredfacility;

(d) The SSBA must be delivered to an authorised person for the registered facility;

(e) The entity must ensure that this transport is covered by a documented policy and procedure and included in the risk assessment;

(f) 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 DoHA;

(g) 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 undergone an identity check;

(c) Have not been excluded from handling the SSBA by the entity nor directed not to handle SSBAs by the Secretary of the Department of Health and Ageing; and

(d) 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.

COMMENTARY: The basic training for all authorised persons includes 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 SSBAs.

Part 7 Inactivation and decontamination

7

7.1 Objective

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

COMMENTARY: 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 identified. It is not necessary to individually identify items for each cycle of decontamination.

7.2 Procedures

(1) Risk assessment must be an integral part of the process to identify and develop effective decontamination and inactivation regimes.

(2) Effective procedures and detailed protocols must be documented and put in place to decontaminate or inactivate the SSBA, or waste products potentially contaminated with the SSBA, prior to destruction or further use. These protocols must include validation data on the inactivation procedures and quality assurance to ensure inactivation has been correctly performed.

COMMENTARY: 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.

It is likely that a number of effective inactivation methods will be available for the SSBA. The entity should ensure that there is data available to demonstrate that the methodology selected is capable of inactivating the SSBA under the specific conditions encountered in the facility. Validation procedures should take into account 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; and/or*
- *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.

(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.

COMMENTARY: 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. 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 *should be consulted 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 those for transporting waste out of PC3 and PC4 facilities.

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) Risk assessment must be an integral part of the process to identify records of decontamination/deactivation and validation data that must be kept. Records of decontamination/inactivation and validation data must be kept in accordance with Part 5 of these standards for both Tier 1 and Tier 2 SSBAs.

COMMENTARY: 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.

This page intentionally blank

Part 8 SSBA management system

8

8.1 Objective

(1) To establish a systematic approach to the management of the biosecurity of SSBAs that takes into account risk and incident management, personnel management, physical security, information management, transport, and inactivation and decontamination in accordance with the requirements of the NHS Act, the NHS Regulations and these Standards.

COMMENTARY: 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 SSBAs.

The SSBA management system should meet more rigorous requirements for Tier 1 SSBAs, 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 the 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; and*
- *establishing resource constraints 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) principle:

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 biosecurity management. These Standards are compatible with other systems and risk management standards, such as those listed in the bibliography of these Standards, in order to facilitate the integration of all such management systems within an entity. Entities that have already implemented systems for quality, environmental or occupational health and safety management, will find significant synergy between these systems and systems for management of SSBAs that are based on the SSBA Standards.*

In order to improve SSBA management the entity needs to specifically focus on the causes of non-compliance and undesirable events. Systematic identification and correction of system deficiencies leads to improved performance and control of SSBAs.

8.2 Policy

(1) The entity must develop, document, authorise, and implement policy concerning the management of SSBAs. This policy must clearly state the overall SSBA management objectives and commitment to improving biosecurity management. This policy must be in place prior to the handling of SSBAs.

(2) The entity must continually assess and improve the effectiveness of the SSBA management system through the use of policies, objectives, procedures, self-review programs, analysis of data, risk assessment and management, corrective and preventive actions and management review.

(3) The entity must ensure that relevant information relating to its SSBA management system and activities is communicated to personnel and other relevant parties.

COMMENTARY: The policy should specifically include provisions covering:

- *meeting the reporting requirements under the* NHS Act *and the* NHS Regulations *in respect of any SSBA held within the entity;*
- *justification for all legitimate uses of any SSBA held in the entity;*
- *documentation and communication of roles, responsibilities and authorities for SSBA management within the entity;*
- *effectively informing all personnel and other relevant parties of individual obligations with regard to SSBA management;*
- *a requirement for all projects/work involving SSBAs to be assessed for risks and for mitigation strategies to be prepared before any work is approved to commence; and*
- *review of the management system at least every two years or following an incident.*

The review of the management system should include assessment and evaluation of opportunities for improvement and the need for changes to the system, procedures, policies and objectives.

The policy should be appropriate to the nature and scale of risk associated with the facility and associated activities, and should commit to:

- *complying with legal requirements in relation to handling SSBAs and their transport;*
- *reducing the level of biosecurity risk to an acceptable level (refer to Part 2 of these Standards), ensuring that the need for effective SSBA management takes precedence over all non "health and safety" operational requirements; and*
- *continually improving SSBA management performance.*

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, cleaners, security personnel, maintenance staff and other support groups.

8.3 Roles, responsibilities and authorities

8.3.1 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 in the facility 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 put in place documented procedures for monitoring the effectiveness of the controls being applied to reduce or eliminate the hazards identified in risk assessment processes;

(h) ensures that staff levels, facilities and equipment are sufficient to effectively carry out work involving SSBAs in accordance with technical protocols, approved polices and SOPs; and

(i) ensures that all requirements for reporting to DoHA are met.

COMMENTARY: While overall responsibility for management of SSBAs 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.

In assigning roles and responsibilities, potential conflicts of interest should be considered.

The SSBA Standards identify roles that need to be covered in 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 and accidents, by improving controls and their implementation, and by ensuring that adequate resources are provided to maintain the effectiveness of the controls.

8.3.2 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) have documented terms of reference;

(b) include a representative cross-section of expertise, appropriate to the nature and scale of the activities undertaken;

(c) include both the Responsible Officer and the Deputy Responsible Officer; and

(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 SSBAs;

(c) reviewing information relating to significant incidents, non-compliance, data trends, associated local/entity actions and associated communication needs; and

(d) ensuring biosecurity issues are formally recorded; actions allocated, tracked and closed out effectively; and internal inspection reports are reviewed.

COMMENTARY: The SSBA Management Committee *may be a stand-alone committee, or it may be part of another committee such as the* Institutional Biosafety or Safety or Management Committee. *The list of functions under clause 8.3.2 is neither exhaustive nor comprehensive, but includes minimal areas to be addressed. When determining membership of the committee, the entity will need to balance the need for expertise versus the need to restrict the number of persons with knowledge about the SSBAs.*

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 short 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 will 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.

8.4 Checking and corrective action

8.4.1 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. Outcomes of this process must be documented.

COMMENTARY: The analysis should include consideration of data generated as a result of 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 SSBAs (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 SSBAs, and records of reporting to DoHA. 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.

8.4.2 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 its SSBA record retention policies and ensure that these are implemented.

COMMENTARY: 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; and/or*
- *training records.*

8.4.3 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 SSBAs) 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.

COMMENTARY: Reviews may range from frequent checks on specific areas to ensure standards are being maintained (for example, storage of SSBAs, disinfectant levels/concentrations for inactivation of SSBAs 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 if records have been altered or tampered with, especially if any other instances of suspicious behaviour have occurred.

Reviews should be undertaken by a team, which may or may not include the Responsible Officer or Deputy Responsible Officer. 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 DoHA.

An Internal Review Template has been developed by DoHA to assist with these reviews. This template is available from DoHA (www.health.gov.au/ssba).

8.4.4 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.

(2) The entity must ensure action is taken to eliminate the causes of non-compliance in order to prevent recurrence.

(3) Records of the nature of the non-compliance and any subsequent action taken must be maintained in accordance with Part 5 of these Standards.

COMMENTARY: Non-compliance, if not addressed may lead to a reportable event as defined by the NHS Act and NHS Regulations.

A procedure should be established to define requirements for:

- *reviewing all non-compliances;*
- *determining the cause(s) of non-compliance;*
- *evaluating the need for action to ensure that non-compliance does not recur;*
- *determining and implementing action needed;*
- *recording results of action taken; and*
- *reviewing corrective actions taken.*

Refer to Clause 2.4 for incident management.

8.4.5 Preventive action

(1) The entity must ensure action is taken to identify, through risk assessment or other sources, potential non-compliance in order to eliminate its causes and prevent occurrence or recurrence. Preventive action must be appropriate to the effects of the potential non-compliance.

COMMENTARY: A procedure should be established to define requirements for:

- *determining the potential for non-compliance and its causes;*
- *evaluating the need for action to prevent occurrence of non-compliance;*
- *determining and implementing action needed;*
- *recording the results of actions taken; and*
- *reviewing preventive action taken.*

This page intentionally blank

Part 9 Handling biological agents suspected of being SSBAs

9

9.1 Objective

(1) To ensure that biological agents suspected, on the basis of testing in a laboratory, of being an SSBA are handled securely prior to the outcome of confirmatory testing or destruction.

COMMENTARY: Division 4A of the NHS Act *sets out the requirements for handling biological agents that are suspected to be SSBAs. 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 SSBAs.*

The requirement for compliance, with this Part begins when the initial tester forms a reasonable suspicion, on the basis of testing in the laboratory, that the biological agent is an SSBA.

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 SSBAs. If the entity intends to handle the SSBA, compliance will include meeting the requirements of Parts 2-8 of the SSBA Standards.

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.

COMMENTARY: Records of access, as outlined above, may be kept in electronic or hard copy form.

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 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 the Commonwealth, State and Territory legislation governing the transport of biological agents.

b) ensures that the confirmatory testing facility will accept the shipment prior to dispatch of the agent. A record of this acceptance must be kept

c) notifies the receiving facility of the shipment details at the time of shipment

d) if the shipment goes missing in transit—immediately informs DoHA once they are aware of the loss

e) if the shipment is reported as an unsuccessful transfer by the receiving facility—immediately informs DoHA once they are aware of the unsuccessful transfer.

COMMENTARY: The sending facility should supply the receiving facility with the waybill number or consignment number, together with details of the transport agent and the expected time of delivery of the shipment. Standards such as AS 4834-2007 – Packaging for Surface Transport of Biological Material *that may cause disease in humans, animals and plants may be useful for determining packaging requirements. 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.*

A record of acceptance for confirming that the receiving facility will accept the shipment may be a phone log, file note, log book note or other such record.

The transport of suspected SSBAs 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. Suspected SSBAs should be transported as Class 6 dangerous goods; toxins are Division 6.1 and infectious substances are Division 6.2.*

In addition, air transport consistent with the IATA Dangerous Goods Regulations *is permitted by the* Civil Aviation Safety Regulations. *These are updated regularly and a current version should be consulted. Suspected SSBAs will usually fall into Category A infectious substances and require packing in accordance with Packing Instruction 602. Personnel that pack the biological agent for shipment are required by the* Civil Aviation Safety Regulations *to have current training in shipping dangerous goods.*

9.3.2 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 documents, has been received; and

   ii. there is no evidence of tampering with the shipping container

b) notifies the sending facility of the receipt of the shipment and if the transfer was successful or unsuccessful; and

c) if a shipment fails to arrive at the expected time, the receiving facility, as a matter of urgency, contacts the transport agent and sending facility to seek confirmation of the location of the shipment and its expected time of delivery.

9.4 Destruction

(1) The entity must ensure that:

(2) If destruction takes place prior to confirmatory testing results being received—processes for destruction of suspected SSBAs 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.

(3) If destruction takes place following receipt of confirmatory testing results—processes for destruction of biological agents confirmed as SSBAs 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.

COMMENTARY: It is likely that a number of 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 is capable of inactivating the agent under the specific conditions encountered in the facility.

9.5 Waste Disposal

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

COMMENTARY: 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. 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 *should be consulted for determining minimum packaging requirements.*

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) Once the initial tester forms the reasonable suspicion that the biological agent is an SSBA, 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 SSBAs and a minimum of 6 months for Tier 2 SSBAs, unless otherwise specified in these Standards

(3) Records do not need to be kept if confirmatory testing shows that the agent is not an SSBA.

COMMENTARY: Records may consist of records of destruction and waste disposal (including validation data) and transport. Records may be kept either as hard copies or as electronic data.

Part 9A Handling following a positive confirmatory test result

9A

9A.1 Objective

(1) To ensure that biological agents that were suspected of being SSBAs and have now been confirmed as SSBAs are handled securely.

COMMENTARY: The requirements contained in Part 9A follow on from the requirements under Part 9 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 compliance with the requirements of Parts 2-8 of the SSBA Standards. Registration documentation must be submitted to DoHA 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 of 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 DoHA.

These requirements end upon submission of a report to DoHA regarding if the entity has disposed of the SSBA or intends to continue handling (an initial registration report or a new SSBA report).

Further information and registration and reporting forms can be found at DoHA (www.health.gov.au/ssba).

9A.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.

COMMENTARY: Records of access, as outlined above, may be kept in electronic or hard copy form.

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.

9A.3 Transport

9A.3.1 Transport requirements for a sending facility

(1) This clause applies when transporting confirmed SSBAs 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 policies and procedures in place to ensure compliance with the Commonwealth, State and Territory legislation governing the transport of biological agents.

(b) Ensures that the receiving facility will accept the shipment prior to dispatch of the agent. A record of this acceptance must be kept.

(c) Notifies the receiving facility of the shipment details at the time of shipment.

(d) If the shipment goes missing in transit—immediately informs DoHA and state / territory police once they are aware of the loss.

(e) If the shipment is reported as an unsuccessful transfer by the receiving facility—immediately informs DoHA and state/territory police once they are aware of the unsuccessful transfer.

COMMENTARY: The sending facility should supply the receiving facility with the waybill number or consignment number, together with details of the transport agent and the expected time of delivery of the shipment. Standards such as AS 4834-2007 – Packaging for Surface Transport of biological material that may cause disease in humans, animals and plants *may be useful for determining packaging requirements. 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.*

A record of acceptance for confirming that the receiving facility will accept the shipment may be a phone log, file note, log book note or other such record.

The transport of SSBAs 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. SSBAs are transported as Class 6 dangerous goods; toxins are Division 6.1 and infectious substances are Division 6.2.*

In addition, air transport consistent with the IATA Dangerous Goods Regulations *is permitted by the* Civil Aviation Safety Regulations. *These are updated regularly and a current version should be consulted. SSBAs usually fall into Category A infectious substances and require packing in accordance* with Packing Instruction 602. *Personnel that pack the SSBA for shipment are required by the* Civil Aviation Safety Regulations *to have current training in shipping dangerous goods.*

9A.3.2 Transport for a receiving facility

(1) This clause applies when receiving confirmed SSBAs 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 shipment has been successful. Verification of successful transfer includes that:

   i. the complete shipment (quantity and type), as covered in the shipment documents, has been received,; and

   ii. there is no evidence of tampering with the shipping container.

b) Notifies the sending facility of the receipt of the shipment and if the transfer was successful or unsuccessful,

c) If a shipment fails to arrive at the expected time, the receiving facility, as a matter of urgency, contacts the transport agent and sending facility to seek confirmation of the location of the shipment and its expected time of delivery.

9A.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.

COMMENTARY: Whatever the SSBA handled, it is likely that a number of effective destruction methods will be available. The 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.

9A.5 Waste Disposal

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

COMMENTARY: Decontamination should take place as soon as possible. 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. 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 *should be consulted for determining minimum packaging requirements.*

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.

9A.7 Record Keeping

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

(2) Records relating to Part 9A 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.

COMMENTARY: Records may consist of records of access, destruction, waste disposal (including validation data) and transport. Records may be kept either as hard copies or as electronic data.

This page intentionally blank

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

10

10.1 Objective

(1) To ensure that SSBAs that are handled temporarily by a non-registered entity are handled securely prior to disposal.

COMMENTARY: 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 9A 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.

COMMENTARY: Records of access, as outlined above, may be kept in electronic or hard copy form.

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 a SSBA for the purposes of disposal.

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

(a) ensures that the receiving facility will accept the shipment prior to dispatch of the agent. A record of this acceptance must be kept;

(b) notifies the receiving facility of the shipment details at the time of shipment;

(c) has documented policies and procedures in place to ensure compliance with Commonwealth and State and Territory legislation governing the transport of biological agents;

(d) if the shipment goes missing in transit—immediately informs DoHA when the entity become aware of the loss; and

(e) if the shipment is reported as an unsuccessful transfer by the receiving facility—immediately informs DoHA once they are aware of the unsuccessful transfer.

COMMENTARY: The sending facility should supply the receiving facility with the waybill number or consignment number, together with details of the transport agent and the expected time of delivery of the shipment. Standards such as AS 4834-2007 – Packaging for Surface Transport of biological material *that may cause disease in humans, animals and plants may be useful for determining packaging requirements. 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.*

A record of acceptance for confirming that the receiving facility will accept the shipment may be a phone log, file note, log book note or other such record.

The transport of SSBAs 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. SSBAs should be transported as Class 6 dangerous goods; toxins are Division 6.1 and infectious substances are Division 6.2.*

In addition, air transport consistent with the IATA Dangerous Goods Regulations *is permitted by the* Civil Aviation Safety Regulations. *These are updated regularly and a current version should be consulted. SSBAs will usually fall into Category A infectious substances and require packing in accordance with* Packing Instruction 602. *Personnel that pack the biological agent for shipment are required by the* Civil Aviation Safety Regulations *to have current training in shipping dangerous goods.*

10.3.2 Transport requirements for a receiving facility

(1) This clause applies when receiving a 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 documents, has been received; and

   ii. there is no evidence of tampering with the shipping container.

b) notifies the sending facility of the receipt of the shipment and if the transfer was successful or unsuccessful; and

c) if a shipment fails to arrive at the expected time, as a matter of urgency, contacts the transport agent and sending facility to seek confirmation of the location of the shipment and its expected time of delivery (see 6.2.2 for further information).

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.

COMMENTARY: It is likely that a number of 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 is capable of inactivating the agent under the specific conditions encountered in the facility.

10.5 Waste Disposal

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

COMMENTARY: 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. 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 *should be consulted for determining minimum packaging requirements.*

If the waste is to be disposed of outside of a facility of the entity 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.

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 SSBAs and a minimum of 6 months for Tier 2 SSBAs, unless otherwise specified in these Standards.

COMMENTARY: Records may consist of records of destruction and waste disposal (including validation data) and transport. Records may be kept either as hard copies or as electronic data.

This page intentionally blank

Part 11 Registered entity handling an SSBA on a temporary basis

11

Objective

(1) To ensure that SSBAs that are handled temporarily by a facility of a registered entity are handled securely prior to disposal.

COMMENTARY: Section 42 of the NHS Act *provides for an entity to be registered in relation to 1 or more SSBAs and 1 or more facilities.*

Parts 1 – 8 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 SSBAs on an ongoing basis.

The requirements under Part 11 apply where a facility of a registered entity commences handling an SSBA on a temporary basis. There are situations where a registered entity is not registered in relation to the handling of that SSBA at that facility. In this situation, Part 11 requirements apply to the handling of the SSBA rather than Parts 1 – 8 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 SSBAs must be handled under Part 9A of these Standards.*

11.1 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 SSBAs 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.

COMMENTARY: Records of access, as outlined above, may be kept in electronic or hard copy form.

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.

11.2 Transport

11.2.1 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) ensures that the receiving facility will accept the shipment prior to dispatch of the agent. A record of this acceptance must be kept;

(b) notifies the receiving facility of the shipment details at the time of shipment;

(c) has documented policies and procedures in place to ensure compliance with Commonwealth and State and Territory legislation governing the transport of biological agents;

(d) if the shipment goes missing in transit—immediately informs DoHA when the entity become aware of the loss; and

(e) if the shipment is reported as an unsuccessful transfer by the receiving facility—immediately informs DoHA once they are aware of the unsuccessful transfer.

COMMENTARY: The sending facility of a registered entity should supply the receiving facility with the waybill number or consignment number, together with details of the transport agent and the expected time of delivery of the shipment. Standards such as AS 4834-2007 – Packaging for Surface Transport of biological material *that may cause disease in humans, animals and plants may be useful for determining packaging requirements. The sending facility of a registered entity 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.*

A record of acceptance for confirming that the receiving facility will accept the shipment may be a phone log, file note, log book note or other such record.

The transport of SSBAs 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. SSBAs should be transported as Class 6 dangerous goods; toxins are Division 6.1 and infectious substances are Division 6.2.*

In addition, air transport consistent with the IATA Dangerous Goods Regulations *is permitted by the* Civil Aviation Safety Regulations*. These are updated regularly and a current version should be consulted. SSBAs will usually fall into Category A infectious substances and require packing in accordance with* Packing Instruction 602. *Personnel that pack the biological agent for shipment are required by the* Civil Aviation Safety Regulations *to have current training in shipping dangerous goods.*

11.2.2 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:

d) verifies that the transfer has been successful. Verification of successful transfer includes that:

iii. the complete shipment (quantity and type), as covered in the shipment documents, has been received; and

iv. there is no evidence of tampering with the shipping container.

e) notifies the sending facility of the receipt of the shipment and if the transfer was successful or unsuccessful.

f) if a shipment fails to arrive at the expected time, as a matter of urgency, contacts the transport agent and sending facility to seek confirmation of the location of the shipment and its expected time of delivery (see 6.2.2 for further information).

11.3 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.

COMMENTARY: It is likely that a number of 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.

11.4 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.

COMMENTARY: Waste can be decontaminated at another part of the facility of a registered entity if permissible by the entity's policies and procedures and if it is securely transported. 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 *should be consulted for determining minimum packaging requirements.*

If the waste is to be disposed of outside of a facility of the entity 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. facility of a registered entity 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.

11.5 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 facilties.

(2) Records relating to Part 11 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.

COMMENTARY: Records may consist of records of destruction and waste disposal (including validation data) and transport. Records may be kept either as hard copies or as electronic data.

This page intentionally blank

Appendix 1

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: a. the possession of a prohibited drug, but only if the penalty for the offence is imprisonment for 2 years or more; or b. the supply, production, import or export of a prohibited drug; or c. the possession of equipment for the manufacture of a prohibited drug.
7	An offence involving membership of, or association with an organised criminal group.
8	An offence: a) involving treachery, sabotage, inciting mutiny, unlawful drilling, or destroying or damaging Commonwealth property; and b) mentioned in Part II of the Crimes Act 1914.
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 Quarantine Act 1908.
13	An offence against the *Gene Technology Act 2000*.

COMMENTARY: 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 'not eligible' 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 Quarantine and Inspection Service, *Quarantine approved premises regulations.* (Commonwealth).

European Committee for Standardisation, *CWA 15793:2008 Laboratory biorisk management standard*, CEN, Belgium. [Available from SAI Global].

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. [Available from SAI Global].

Health Canada 1996, *Laboratory biosafety guidelines*, 2nd edition, Ottawa: Minister of Supply and Services Canada.

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

International Organization for Standardization, *ISO 9000:2005 Quality management systems - Fundamentals and vocabulary*, ISO, Geneva.

International Organization for Standardization, *ISO 9001:2000 Quality management systems - Requirements*, ISO, Geneva.

International Organization for Standardization, *ISO 19011:2002 Guidelines for quality and/or environmental management systems auditing*, ISO, Geneva.

International Organization for Standardization, *ISO 14001:2004 Environmental management systems - Requirements with guidance for use*, ISO, Geneva.

International Organization for Standardization *ISO 15189:2007 Medical laboratories - Particular requirements for quality and competence*, ISO, Geneva.

International Organization for Standardization, *ISO 15190:2003 Medical laboratories - Requirements for safety*, ISO, Geneva.

International Organization for Standardization, *ISO/IEC 17025:2005 General requirements for the competence of testing and calibration laboratories*, ISO, Geneva.

International Organization for Standardization, *ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management*, ISO, Geneva.

International Organization for Standardization, *ISO/IEC Guide 51:1999 Safety aspects - Guidelines for their inclusion in standards*, ISO, Geneva.

International Organization for Standardization, *ISO/IEC Guide 73:2002 Risk management – Vocabulary - Guidelines for use in standards*, ISO, Geneva.

Occupational Health & Safety Group, *OHSAS 18001:2007 Occupational health and safety management systems – Requirements*, The Occupational Health & Safety Group, Macclesfield, UK.

Office of the Gene Technology Regulator, 2001, *Guidelines for the certification of facilities/Physical containment requirements,* OGTR, Canberra. [Available from Office of the Gene Technology Regulator (www.ogtr.gov.au)].

Standards Australia, *AS/NZS 2243.1:2005 Safety in laboratories, Part 1: Planning and operational aspects,* SAI Global, Sydney.

Standards Australia, *AS/NZS 2243.3:2010 Safety in laboratories, Part 3: Microbiological aspects and containment facilities,* SAI Global, Sydney.

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

Standards Australia, *AS/NZS ISO 3100:2009 Risk management- Principles and guidelines,* SAI Global, Sydney.

Standards Australia, *AS 4811:2006 Employment screening,* SAI Global, Sydney.

Standards Australia *AS 4834-2007 Packaging for the surface transport of biological materials that may cause disease in humans, animals and plants.* SAI Global, Sydney.

Standards Australia, *HB 167:2006 Security risk management,* SAI Global, Sydney.

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

Standards Australia, *HB 293:2006 Executive guide to business continuity management,* SAI Global, Sydney.

Standards Australia, *HB 323:2007 Employment screening handbook,* SAI Global, Sydney.

United Nations, *Recommendations on the Transport of Dangerous Goods Model Regulations*, 15th edition, United Nations, Geneva, 2007.

World Health Organization. WHO/CDS/CSR/LYO/2004.11 *Laboratory biosafety manual*, 3rd edition, World Health Organization, Geneva, 2004.

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