Release Date: January 2014

Guideline 11
SSBAS AND OTHER REGULATORY SCHEMES

INTRODUCTION

This guideline covers situations where entities/facilities are required to provide access to secure SSBA areas or information that is considered sensitive under the Security Sensitive Biological Agents (SSBA) Regulatory Scheme to other regulatory schemes, in particular the Office of the Gene Technology Regulator (OGTR) and the Department of Agriculture - Biosecurity (formerly DAFF Biosecurity).

This document is guidance material only and is provided to assist in understanding the SSBA Regulatory Scheme.

SSBA LEGISLATIVE REQUIREMENTS

The aim of the SSBA Regulatory Scheme is to limit opportunities for acts of bioterrorism or biocrime involving SSBAs.

Entities and facilities handling SSBAs are required to comply with the *National Health Security Act 2007* (NHS Act), the *National Health Security Regulations 2008* (NHS Regulations) and the SSBA Standards. Some of the SSBA Regulatory Scheme requirements that may impact on the requirements of other regulatory schemes could include:

- clearly defining a secure perimeter that encloses the area where SSBAs are handled.
- restricting access to the secure area or linked storage units to Authorised or Approved Persons.
- prohibiting unauthorised recording, photography or filming within the secure area.
- identifying sensitive information relating to the security of SSBAs and restricting access to this information to those who need to know and have been permitted access by the Responsible Officer.

SENSITIVE INFORMATION

The NHS Regulations define ‘sensitive information’ as:

- the entity’s storage records (including inventory records) for any SSBAs handled at the facility;
- the entity’s risk assessment plans for any SSBAs handled at the facility;

- the entity's risk management plans for any SSBAs handled at the facility; and
- any other information identified by the entity that could compromise the security of the SSBAs handled at the facility. Additional sensitive information could include:
    - lists of authorised and approved persons.
    - lists of access codes or key numbers.
    - floor plans that outline the secure perimeter and access points.
    - incident reports that may indicate a vulnerability in the security of the SSBA

Sensitive information may be either hardcopy or electronic documentation and may be stored outside of the secure area.

Clause 5.3 of the SSBA Standards covers the requirements for Information Security and states that the entity must identify and control access to sensitive information. Requirements include:

- that access must be limited to persons who have a need to know, and have been granted access by the Responsible Officer.
- access permissions must be reviewed 6 monthly for facilities handling Tier 1 SSBAs and 12 monthly for facilities handling Tier 2 SSBAs.
- sensitive information related to Tier 1 SSBAs must be stored in a secure system and securely backed up at regular intervals.

COMPLYING WITH OTHER REGULATORY SCHEMES

A facility regulated under the SSBA Regulatory Scheme may also be subject to requirements of other Australian Government regulatory schemes or legislation which could include, but is not limited, to:

- the *Gene Technology Act 2000* (GT Act) which regulates genetically modified organisms in Australia and is administered by OGTR.

- the *Quarantine Act 1908* and the *Export Control Act 1982* which are administered by the Department of Agriculture's Biosecurity area.

To comply with the requirements of other regulatory schemes, an SSBA facility may be required to allow Regulatory Officers into the secure area where SSBAs are held or to access documents that are considered sensitive information. Regulatory Officers may also require copies of certain documents as evidence of compliance with their regulatory scheme.

ACCESS TO AN SSBA FACILITY OR TO SENSITIVE INFORMATION

Registered facilities may allow other Regulatory Officers into an SSBA registered facility as an Approved person under clause 3.4 of the SSBA Standards. Clause 3.4 sets out the requirements for Approved persons and states that an entity must put in place processes to ensure that contractors, visitors, suppliers, students and other such persons do not compromise the facility's SSBA security.

An entity can approve an Approved person to:

- handle SSBAs;
- access the facility where SSBAs are handled;
- access sensitive information related to SSBAs.

Approvals may relate to one or any combination of the above.

Approved persons in a Tier 1 SSBA facility must be escorted (line of sight) by an Authorised person at all times while in the secure area or handling sensitive information. An Approved person in a Tier 2 facility must be supervised by an Authorised person at all times. The degree of supervision must have been determined previously as part of the facility's risk assessment.

For example: A Regulatory Officer from another regulatory scheme is required to inspect a facility where SSBAs are handled and to view records that contain information relating to SSBAs. The Responsible Officer may approve the Regulatory Officer as an Approved person to permit access to the facility and to the sensitive information. This approval and the information about what the Regulatory Officer is approved for must be included in the Approved persons list held by the facility's Responsible Officer.

When determining access requirements, facilities may also need to take into consideration safety requirements such as the need for the Regulatory Officer to know in advance of the visit any biosafety risks in the facility.

PROVIDING COPIES OF DOCUMENTS RELATING TO SSBAS

The facility 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.

In the first instance, an entity should determine if the information can be de-identified or the sensitive information removed. The entity should also check if the Regulatory Officer can sight the information, rather than take copies for their records. If the above is not possible and sensitive information must be supplied to the regulatory authority then the information must only be supplied under the following conditions (as set out under Clause 5.3.1 of the SSBA Standards):

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[1] 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.

[1] The PROTECTED security classification involves:
- The person accessing the information must have a Baseline Vetting security clearance or higher
- Information must be stored in a PROTECTED file
- Information must be stored in a C class security container or, at a minimum, in a lockable container
- Information must be secured when not in use (clear desk policy)
- Information must be transported in an opaque envelope and double enveloped for transport
- Information must be destroyed using a secure B class shredder or ASIO approved destruction service.

The entity must record what information is supplied to the regulatory authority. Information that is supplied electronically should have, where possible, measures in place to prevent copying and hard copies should be marked as copies with a clear security marking in place.

FURTHER INFORMATION

Further information can be obtained from the SSBA Regulatory Scheme on (02) 6289 7477 or ssba@health.gov.au.