SSBA – Fact sheet 10 – Information security

September 2013

This fact sheet provides an overview of the information security requirements of the Security Sensitive Biological Agents (SSBA) Regulatory Scheme, and is designed to assist entities and facilities in meeting the information security requirements under the SSBA Standards.

Sensitive Information

The SSBA Standards state that entities must identify sensitive information and limit access to that information. It is this identified sensitive information that is subject to the information security requirements.

Sensitive information is defined in the *National Health Security Regulations 2008* as any of the following:

a. the entity's storage records for the security-sensitive biological agent handled at the facility
b. an entity's risk assessment plan for the security-sensitive biological agent handled at the facility
c. an entity's risk management plan for the security-sensitive biological agent handled at the facility
d. any other information that the entity identifies as being sensitive information because it could compromise the security of the SSBA handled at the facility.

Sensitive information may also include records of authorised and approved persons or floor plans outlining the secure perimeter. Sensitive information may be held either as a hardcopy, electronic document or information saved on electronic media.

While records of research, 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 SSBAs.

Policy and procedures

In order to comply with the SSBA Standards, the entity must have in place policies and procedures for identification of, access to, storage of, and destruction of sensitive information. The policies should also encourage and promote a security-conscious culture within the entity and facility.

Need-to-know principle

Sensitive information should be handled on a need-to-know basis. The need-to-know principle refers to those who have a legitimate reason to use or have access to the information to do their work. For example, information technology (IT) staff may need access to information about passwords and user access to reset such information, but they would not require access to records of storage of the SSBA.

The SSBA Standards require that if IT staff have access to sensitive information regarding SSBAs they are either authorised or approved persons under Part 3 of the SSBA Standards.

Security measures

Hard copy documents

Hard copies of sensitive information should be stored securely, for example in a locked filing cabinet. The entity should have a clear desk policy where, during absences from the workplace, employees must ensure that sensitive information is secured appropriately. Sensitive information should not be copied unnecessarily and any copies made should be clearly identified as sensitive information. If necessary, copies may need to be tracked and copies that are no longer needed should be securely destroyed.

Electronic media

It is recommended that sensitive information is stored on a stand-alone system, such as a laptop, stand-alone computer, removable hard drive or a portable storage device. Portable systems such as laptops and portable drives should be stored securely when not in use, for example by locking in a safe or a secure cabinet. Any system chosen must be able to be backed-up and the back-ups stored securely, preferably in a place separate to the original data. Computers should be accessed via an individual log-on (if possible) and locked, if left unattended.

Destruction

Entities must have policies and procedures in place for destruction of sensitive information (both hard and electronic copies) collected for the SSBA Regulatory Scheme. Electronic media used to store sensitive information should not be reused as deleting or wiping a drive will not completely remove the information. Hard drives, storage media (e.g. CDs) and portable storage devices should be disposed of securely for example, through secure destruction services. Hard copies of information may be disposed of by such means as secure destruction services, incineration or cross shredders.

Networked computers

Information stored on a network is not as secure as that stored on a stand-alone system. This level of storage is not recommended for information concerning Tier 1 SSBAs. As with the stand-alone systems, access to the information must be restricted. This may be through password protection and restricting access to secure areas of the system (password

protected folders or access restricted folders can be set up by IT personnel in your organisation).

Passwords

The Department of Health (Health) recommends that passwords should be at least seven characters long and a mix of numbers and upper and lower case letters. Health recommends that passwords should be changed regularly (for example every 90 days) and should not be repeatable for at least eight password changes.

Provision of sensitive information to other regulatory authorities

From time to time an entity may be required to provide evidence of compliance containing sensitive information to other regulatory schemes. Clause 5.3.1 of the SSBA Standards provides for this occurrence. In the first instance, an entity should determine if the sensitive information can be de-identified or removed from the document before hand over. The entity should also check if the information can be sighted by the regulatory officers at the entity, rather than providing the regulatory authority 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:

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 the information to what is identified in a) above. This means ensuring that other sensitive information that is not required for the regulatory authority’s work is not provided inadvertently.

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 reading

The following publications may be useful when determining IT security measures for your organisation:

ASCI 33 — Australian Government Information Security Manual (ISM). Available from the Department of Defence, Australian Signals Directorate. (http://www.asd.gov.au/).

ISO/IEC 17799 — Information technology – Security techniques – Code of practice for information security management. (http://www.standards.com.au).

ISO/IEC 27001:2005 — Information technology – Security techniques – Information security management systems – Requirements. (http://www.standards.com.au).