Government of Canada | Gouvernement du Canada

CANADIAN BIOSAFETY GUIDELINE

DEVELOPING A COMPREHENSIVE BIOSECURITY PLAN

Canada

Canadian Biosafety Guideline - Developing a Comprehensive Biosecurity Plan is available on the Internet at the following address: http://canadianbiosafetystandards.collaboration.gc.ca/

Egalement disponible en français sous le titre :
Ligne directrice canadienne sur la biosécurité : Élaboration d'un plan de biosûreté exhaustif

To obtain additional copies, please contact:

Public Health Agency of Canada
100 Colonnade Road
Ottawa, ON K1A 0K9
Tel.: 613-957-1779
Fax.: 613-941-0596
PHAC email: PHAC.standards-normes.ASPC@canada.ca
CFIA email: standardsnormes@inspection.gc.ca

This publication can be made available in alternative formats upon request.

Publication date: June 2016

Publication Number: 160076
Cat.: HP45-12/2016E-PDF
ISBN: 978-0-660-05674-6

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

PREFACE

PREFACE

The *Canadian Biosafety Guidelines* have been developed by the Public Health Agency of Canada (PHAC) and the Canadian Food Inspection Agency (CFIA) as an ongoing series of biosafety and biosecurity themed guidance documents.

In Canada, most facilities where human and terrestrial animal pathogens or toxins are handled and stored are regulated by the PHAC and the CFIA under the *Human Pathogens and Toxins Act* (HPTA), *Human Pathogens and Toxins Regulations* (HPTR), *Health of Animals Act* (HAA), and *Health of Animals Regulations* (HAR). Regulated facilities are required to develop and maintain a biosecurity plan, in accordance with the requirements established in the *Canadian Biosafety Standard* (CBS), 2nd Edition. The *Canadian Biosafety Handbook* (CBH), 2nd Edition aims to provide stakeholders with support and guidance on how to conduct biosecurity risk assessments and the core components of a robust biosecurity plan to appropriately address biosecurity risks with the pathogens and toxins in their possession. The *Developing a Comprehensive Biosecurity Plan* guideline elaborates on a number of the biosecurity topics introduced in the CBH and serves as a resource for stakeholders seeking additional information and guidance to establish a more detailed and robust biosecurity plan.

The *Developing a Comprehensive Biosecurity Plan* guideline is a continuously evolving document and subject to ongoing improvement. The PHAC and the CFIA welcome comments, clarification, and suggestions for incorporation into future versions of the guideline. To this end, please send information with references (where applicable) for continual improvement of the *Developing a Comprehensive Biosecurity Plan* guideline to:

PHAC e-mail: PHAC.standards.normes.ASPC@canada.ca
CFIA e-mail: standardsnormes@inspection.gc.ca

ABBREVIATIONS AND ACRONYMS

ABBREVIATIONS AND ACRONYMS

BSO	Biological safety officer
CBH	*Canadian Biosafety Handbook*
CBS	*Canadian Biosafety Standard*
CCTV	Closed circuit television
CFIA	Canadian Food Inspection Agency
CL	Containment level (i.e., CL1, CL2, CL3, CL4)
CSIS	Canadian Security Intelligence Service
ERP	Emergency response plan
HAA	*Health of Animals Act*
HAR	*Health of Animals Regulations*
HPTA	*Human Pathogens and Toxins Act*
HPTR	*Human Pathogens and Toxins Regulations*
HPTA Security Clearance	*Human Pathogens and Toxins Act* Security Clearance
IT	Information technology
LAN	Local area network
LRA	Local risk assessment
PHAC	Public Health Agency of Canada
RCMP	Royal Canadian Mounted Police
RG	Risk group (i.e., RG1, RG2, RG3, RG4)
SOP	Standard operating procedure
SSBA	Security sensitive biological agent
TDGR	Transportation of Dangerous Goods Regulations
VPN	Virtual private network

CHAPTER 1

1
2

INTRODUCTION

CHAPTER 1 - INTRODUCTION

1.1 Scope

All **facilities**, including **containment level** 2 (CL2), that are subject to the *Canadian Biosafety Standard* (CBS), 2nd Edition (i.e., facilities licensed under the *Human Pathogens and Toxins Act* [HPTA] or **importing** under the *Health of Animals Act* [HAA] and *Health of Animals Regulations* [HAR]) are required to develop a **biosecurity** plan.[1,2,3,4] All regulated facilities require a biosecurity plan (CBS matrix 4.1). There can be one plan for each campus, site and containment level, or a single plan that covers multiple sites, **licences**, and containment levels.

In Canada, facilities that conduct **controlled activities** with human **pathogens** or **toxins** are regulated under the HPTA and the *Human Pathogens and Toxins Regulations* (HPTR), unless they meet the exclusion criteria specified in the HPTA.[5] Facilities that are not excluded or otherwise exempted from the HPTA or HPTR require a licence to conduct controlled activities with human pathogens or toxins. The importation into Canada of **animal pathogens**, infected animals, animal products or by-products, or other organisms carrying an animal pathogen or part of one (i.e., toxins), and activities with the imported material, are regulated under the HAA and HAR and require an animal pathogen import permit or **transfer** authorization. Activities in Canada involving human and animal pathogens, toxins, and other regulated **infectious material** are regulated by the Public Health Agency of Canada (PHAC) or the Canadian Food Inspection Agency (CFIA) in accordance with the HPTA, HPTR, HAA and HAR.

The CBS describes the minimum requirements for compliance of any **containment zone** in a facility regulated under the HPTA, HPTR, HAA and HAR, as applicable. The *Canadian Biosafety Handbook* (CBH), 2nd Edition, 2016, is a companion document to the CBS that provides core information and guidance on how the requirements outlined in the CBS can be achieved.[6] The CBH also provides guidance on the development and maintenance of a risk-based **biosafety** program.

The biosecurity plan is a key component of the biosafety program. The *Developing a Comprehensive Biosecurity Plan* guideline expands on the biosecurity guidance provided in the CBH to help facilities meet the biosecurity requirements specified in the CBS.

1.2 Overview

The **handling or storing** of human and animal pathogens or toxins poses a **risk** to personnel, the **community**, and the environment. Management of these risks necessitates an awareness and application of biosafety and biosecurity practices among personnel in laboratories and other containment zones where work with pathogens, toxins, infectious material, or infected animals is conducted.

The purpose of a biosecurity program is to prevent the loss, theft, misuse, diversion, or intentional **release** of biological **assets** (i.e., pathogens, toxins and other regulated infectious material) and related facility assets (e.g., non-infectious **biological material**, equipment, animals, sensitive information). The *Developing a Comprehensive Biosecurity Plan* guideline

outlines the development of a comprehensive biosecurity plan that is based on an assessment of the biosecurity risks associated with the assets possessed by, and activities conducted at, a facility. Although all facilities must have a biosecurity plan, its complexity (e.g., level of detail, security measures) is proportional to the risk posed by the compromise of assets possessed by the facility, as determined during the **biosecurity risk assessment**.

This document provides detailed guidance on the elements required for a biosecurity plan in facilities where pathogens and toxins are handled or stored. The guidance is intended to assist facilities in meeting the minimum biosecurity requirements outlined in the CBS, HPTA, and HPTR, and to provide more in depth considerations beyond the core guidance included in the CBH. This includes guidance on developing a comprehensive biosecurity plan and implementing effective biosecurity controls and procedures commensurate with the risks identified in the biosecurity risk assessment.

1.3 How to Use the *Canadian Biosafety Guideline: Developing a Comprehensive Biosecurity Plan*

The information provided in the *Developing a Comprehensive Biosecurity Plan* guideline, including any examples provided, is only intended as guidance to enhance a biosecurity plan, and not to be interpreted as requirements. Some sections include a table outlining a biosecurity plan element, the risk to be mitigated, and an example on how that risk may be mitigated in a CL2, a CL3, or an area where **security sensitive biological agents** (SSBAs) are handled or stored. The purpose of these examples is to reinforce that a given risk can be common to all containment levels but the mitigation strategy selected is proportionate to the risk identified for a particular containment zone or area. Where the guidance relates to a requirement from the CBS, the requirement matrix or matrices are referenced (e.g., CBS Matrix 4.1). Likewise, where the guidance relates to a requirement from the legislation (i.e., HPTA, HPTR, HAA, HAR), the specific section and subsection(s), where applicable, will be referenced (e.g., HPTA 33). This document will guide the user in identifying the appropriate controls to implement, commensurate with the specific risks identified by the biosecurity risk assessment. The minimum requirements for a biosecurity plan are specified in CBS Matrix 4.1.

The *Developing a Comprehensive Biosecurity Plan* guideline includes a detailed list of all abbreviations and acronyms used throughout; this list is located at the beginning of the document. Each abbreviation or acronym is spelled out upon first use, with the abbreviation immediately following in brackets; the abbreviation is used exclusively throughout the remainder of the document.

This guideline also contains a comprehensive glossary of definitions for technical terms, located in Chapter 9; words defined in the glossary appear in **bold type** upon first use. Chapter 10 provides a list of the resources that were used to develop the guideline. In-text citations are listed in the references at the end of each chapter. Additional information on biosafety and biosecurity can be found in the CBH and on the PHAC elearning portal (publichealth.gc.ca/training).

References

1 Government of Canada. (2015). *Canadian Biosafety Standard* (2nd ed.). Ottawa, ON, Canada: Government of Canada.

2 *Human Pathogens and Toxins Act* (S.C. 2009, c. 24). (2015).

3 *Health of Animals Act* (S.C. 1990, c. 21). (2015).

4 *Health of Animals Regulations* (C.R.C., c. 296). (2015).

5 *Human Pathogens and Toxins Regulations* (SOR/2015-44). (2015).

6 Government of Canada. (2016). *Canadian Biosafety Handbook* (2nd ed.). Ottawa, ON, Canada: Government of Canada.

CHAPTER 2

GETTING STARTED

CHAPTER 2 - GETTING STARTED

2.1 Roles and Responsibilities

Senior management within the facility is the ultimate authority and is responsible for delegating appropriate authority for biosecurity. The delegated individual may be the **biological safety officer** (BSO) or other biosafety representative, or it could be security personnel or another appropriate individual; however, the successful development and implementation of a biosecurity plan will often require the contribution of a multidisciplinary team of subject matter experts with a wide range of knowledge, skills, and expertise. The team members can include management, financial officer(s), architect(s), engineering firm, the BSO or biosafety representative, security personnel, scientists, **laboratory** workers, maintenance staff, and local law enforcement, depending on the particular situation.

This delegated person's responsibilities will include assembling a team (as required), developing, implementing, and improving the biosecurity plan, and may include acting as the point of contact for any biosecurity-related **incidents**, maintaining a list of individuals with access to pathogens, toxins, and other regulated infectious material, maintaining training records, and ensuring that measures are in place to adequately protect sensitive information. The CBS specifies that it is the BSO (or biosafety representative) that communicates with the PHAC and the CFIA on behalf of the licence holder or animal pathogen import permit holder.[1,2]

In addition, other individuals play key roles in maintaining biosecurity. Identifying these individuals in the biosecurity plan, along with their contact information, is essential for the development and implementation of the plan. Such key individuals may include:

- the individual(s) identified as the Pathogen and Toxin Licence holder and the animal pathogen import permit holder(s);
- the individual(s) responsible for the management and oversight of the **scientific research** program or project (e.g., the principal investigator, laboratory/facility manager or director);
- on-site security personnel (where applicable). The biosecurity plan should describe their responsibilities (e.g., monitoring intrusion detection systems, responding to alarms, maintaining visitor entry/exit records, issuing identification [ID] cards) specifically with respect to biosecurity;
- local law enforcement. Any additional roles for local law enforcement could be outlined in a memorandum of understanding (MOU) (where applicable);
- all personnel who have access to higher risk pathogens and toxins (i.e., SSBAs, **risk group** 3 [RG3], and RG4);
- the individual(s) responsible for conducting personnel suitability screening and evaluating the results;
- human resources, who may be involved in managing behavioural issues, and can facilitate communications with employee assistance programs and employee unions, as applicable;
- the individual(s) responsible for information technology (IT) and network security; and,

- all individuals (maintenance staff, animal handlers, security personnel, etc.) who may have the ability to remotely override **controlled access systems** from inside or outside the facility (e.g., via building automation systems, computers, or security consoles).

2.2 Biosecurity Risk Assessment

The CBS specifies that a biosecurity plan is to be developed, based on a site-specific assessment of the biosecurity risks associated with the assets (i.e., pathogens, toxins, and related assets) possessed by, as well as activities conducted in, a facility.[3] Risk is based on the probability of an event occurring, and the severity of the consequences of that event should it occur. The biosecurity risk assessment is an evaluation of the probability of an *intentional* event, such as the theft of assets (e.g., pathogen, toxin, infectious material, equipment, animals, information), and the consequences of that event (e.g., public health impact resulting from intentional release of a pathogen, or theft of proprietary information). It will identify and prioritize risks that will be mitigated through the recommended strategies and best practices described in the biosecurity plan.

The biosecurity risk assessment differs from biosafety risk assessments (i.e., overarching, pathogen and toxin, and **local risk assessments** [LRA]), in that the individuals or groups that may have malicious interest in the asset (i.e., threats) also need to be considered when evaluating of the probability of an event occurring. Threats can be categorized into two groups: individuals or groups without authorized access to the assets are considered **outsider threats**, and individuals or groups with authorized access to the assets are considered **insider threats**.[4]

In addition, the biosecurity risk assessment needs to consider the increased security requirements of assets with **dual-use potential**. That is, assets that can be used for legitimate scientific applications, but that pose an increased biosecurity risk due to an inherent potential for development and use as a biological weapon. Assets with dual-use potential include SSBA pathogens and toxins, but can also include assets related to their handling and storing (e.g., equipment, information).[5] The steps to conduct a biosecurity risk assessment are described in Chapter 6 of the CBH.

Risk statements and levels identified through the biosecurity risk assessment can be captured in a variety of ways (e.g., risk register) and are the beginning point for the development of any biosecurity plan.

2.3 Developing the Biosecurity Plan

The biosecurity plan details the mitigation strategies for identified biosecurity risks associated with biological assets. The biosecurity plan describes both the physical and operational controls implemented to prevent unauthorized access to assets, as well as to detect and respond to incidents where unauthorized access was attempted.

The biosecurity plan should complement existing mitigation measures in the **Biosafety Manual**, the **emergency response plan** (ERP), institutional security plans, and employee assistance

programs. Access controls may already exist at some level within such plans or documents (e.g., there may be some biosecurity risks already managed through measures implemented to address biosafety risks). For example, personnel screening and physical security measures can be used to mitigate both biosafety and biosecurity risks. (CBS Matrix 4.1). Integrating the elements of the biosecurity plan within the overall biosafety program will allow for more efficient management of biosafety and minimize duplication of information.

2.3.1 Elements of a Biosecurity Plan

Every biosecurity plan must address six elements, which are discussed in this document. These are listed below, along with its performance objective.

- Physical Security: Reduce the risk of unauthorized access to identified assets and other sensitive materials by instituting appropriate physical security controls.
- Personnel Suitability and Reliability: Reduce the risk that an individual with access will compromise assets by assessing an individual's current and ongoing suitability for a position.
- Pathogen and Toxin Accountability: Establish "ownership" of pathogens and toxins, and individuals' responsibilities and authorities.
- Inventory Control: Deter insider threats by tracking pathogens, toxins, infectious material, and other related assets, and allowing for the rapid identification of missing items.
- Incident and Emergency Response: promote personnel safety and the security of pathogens and toxins; provide an evidence basis for the continual improvement of biosecurity measures.
- Information Management and Security: Protect sensitive information from unauthorized access or theft and ensure the requisite level of confidentiality.

2.3.2 Development of Risk Mitigation Measures

The development of biosecurity risk mitigation measures should employ a systematic approach built upon well documented operational processes to identify, assess, understand, decide, and communicate risk issues in an effort to determine the best course of action. All measures to secure a given asset should achieve the same level. For example, the main entrance, windows and emergency exits should be secured to the same level, and all individuals (personnel and visitors) with access to a containment zone should meet the same entry requirements.

Every organization will have a distinct risk culture (i.e., the attitudes and behaviours found within an organization regarding risk management) and risk tolerance (i.e., the willingness of an organization to accept or reject a given level of residual risk).[6] Risk culture and tolerance can change based on organizational priorities, stakeholders, and availability of resources. This

must be clearly understood by the multidisciplinary team conducting the biosecurity risk assessment and subsequently developing mitigation measures that will be detailed in the biosecurity plan.

2.3.2.1 Mitigation Measures Commensurate with Biosecurity Risks

Since the biosecurity plan is based on the biosecurity risk assessment, it will be tailored to each facility or containment zone, and its level of detail and complexity will vary depending on the nature (i.e., size, structure, complexity) of the facility and the activities performed within each containment zone (e.g., a CL2 facility undertaking *in vitro* work will likely have fewer biosecurity risks to mitigate than a CL3 facility undertaking *in vivo* work with an SSBA).

While all regulated facilities are required to develop a biosecurity plan that addresses the six elements described in Section 2.3.1, many of the mitigation measures described in this document exceed those needed to mitigate risks in many CL2 facilities. In the development of a biosecurity plan for a given facility, the performance objective for each component of the biosecurity plan should be considered in relation to the risks identified in the biosecurity risk assessment. Following this, the controls that would be appropriate to address the identified risks would be carefully considered.

The following chapters further elaborate the theory behind each component of biosecurity and provide examples of physical and operational controls that can be used to mitigate biosecurity risks.

2.3.3 Accessing the Biosecurity Plan on a Need-to-know Basis

The complete, detailed biosecurity plan contains sensitive information, such as vulnerabilities, risks, specific mitigation measures, floor plans, security systems, and access control details. Access to the detailed biosecurity risk assessments, including the risk register, and the complete biosecurity plan should be limited to authorized individuals (e.g., the BSO, security personnel, senior management, PHAC and CFIA inspectors designated under the HPTA or HAA) with a need to know to carry out their functions. The detailed information contained in the plan is not intended for all facility personnel. Further details on information classification and security can be found in Chapter 7.

A description of the biosecurity plan is required to appear in the Biosafety Manual (CBS matrix 4.1). The description can be an overview or an abridged version of the biosecurity risk mitigation measures that apply to all personnel, while leaving out sensitive details. This version can be used for personnel training, and would include biosecurity-specific **standard operating procedures** (SOPs). Where it is deemed appropriate, the training can be geared to groups of individuals with similar functions (e.g., laboratory workers handling only RG2 pathogens versus those handling SSBAs).

References

1 *Human Pathogens and Toxins Act* (S.C. 2009, c. 24). (2015).

2 *Human Pathogens and Toxins Regulations* (SOR/2015-44) (2015).

3 Government of Canada. (2015). *Canadian Biosafety Standard* (2nd ed.). Ottawa, ON, Canada: Government of Canada.

4 Salerno, R. M., & J. Gaudioso. (2007). *Laboratory Biosecurity Handbook*. Boca Raton, FL, USA: CRC Press.

5 CEN Workshop 55 – CEN Workshop Agreement (CWA) 16393:2012, *Laboratory biorisk management – Guidelines for the implementation of CWA 15793:2008*. (2012). Brussels, Belgium: European Committee for Standardization. Retrieved on 2/8, 2016 from http://www.valvira.fi/documents/14444/259268/CWA+16393/36d5eeb3-a206-4aec-a0b3-2bea97459835.

6 Government of Canada (2012). *Guide to Integrated Risk Management: A recommended approach for developing a Corporate Risk Profile*. Retrieved 2/9, 2016 from https://www.tbs-sct.gc.ca/tbs-sct/rm-gr/guides/girm-ggir01-eng.asp

CHAPTER 3

PHYSICAL SECURITY

CHAPTER 3 - PHYSICAL SECURITY

Physical security refers to barriers or measures put in place to physically prevent unauthorized access to a facility, part of a facility, or assets, and to protect them from damage, theft, or misuse. Adequate physical security should be implemented to minimize opportunities for the unauthorized entry of individuals into containment zones and other areas (e.g., storage areas), and the unauthorized removal of pathogens, toxins, other regulated infectious material, or other assets from the facility.

The complexity of the physical security system should be proportional to the level of risk associated with the assets as determined by a biosecurity risk assessment. The CBS should be consulted for the physical **containment** requirements and the **operational practice requirements** specific to each containment level.[1]

The physical security component of the biosecurity plan should identify and describe security systems in place that limit or restrict access to the areas containing pathogens, toxins, and other assets. Each physical security system in place performs one or more functions to control or deter access to assets, detect unauthorized access attempts (e.g., tamper-evident devices, alarms, closed-circuit television system [CCTV], lighting), and respond to incidents.[2]

The following sections will help determine the appropriate level of physical security. Examples of possible measures that may be implemented to mitigate biosecurity risks related to physical security are provided in Table 3-2.

3.1 Physical Barriers and Graded Protection

Measures to physically deter unauthorized individuals usually begin at the site perimeter, with additional barriers at the perimeters of increasingly secure areas within the facility. Some examples of measures to deter unauthorized individuals include perimeter fencing, electronic controlled access systems, locking hardware, high-security windows, and high-security doors.

The first step in determining the most appropriate physical **security barriers** is identifying all points of access leading to or into the containment zone (i.e., doors, windows, and other penetrations). In facilities where SSBAs are present and accessible, consideration is to be given to the mechanism for restricting access to the part of the facility where SSBAs are handled and stored to authorized persons with a valid *Human Pathogens and Toxins Act* Security Clearance (HPTA Security Clearance).

Physical security measures can be implemented in a graded manner to provide a greater level of protection to higher risk biological assets (e.g., SSBAs). This is achieved by creating multiple, nested areas, requiring individuals to cross an access control barrier at each area in order to reach more secure areas within the facility (Figure 3-1).

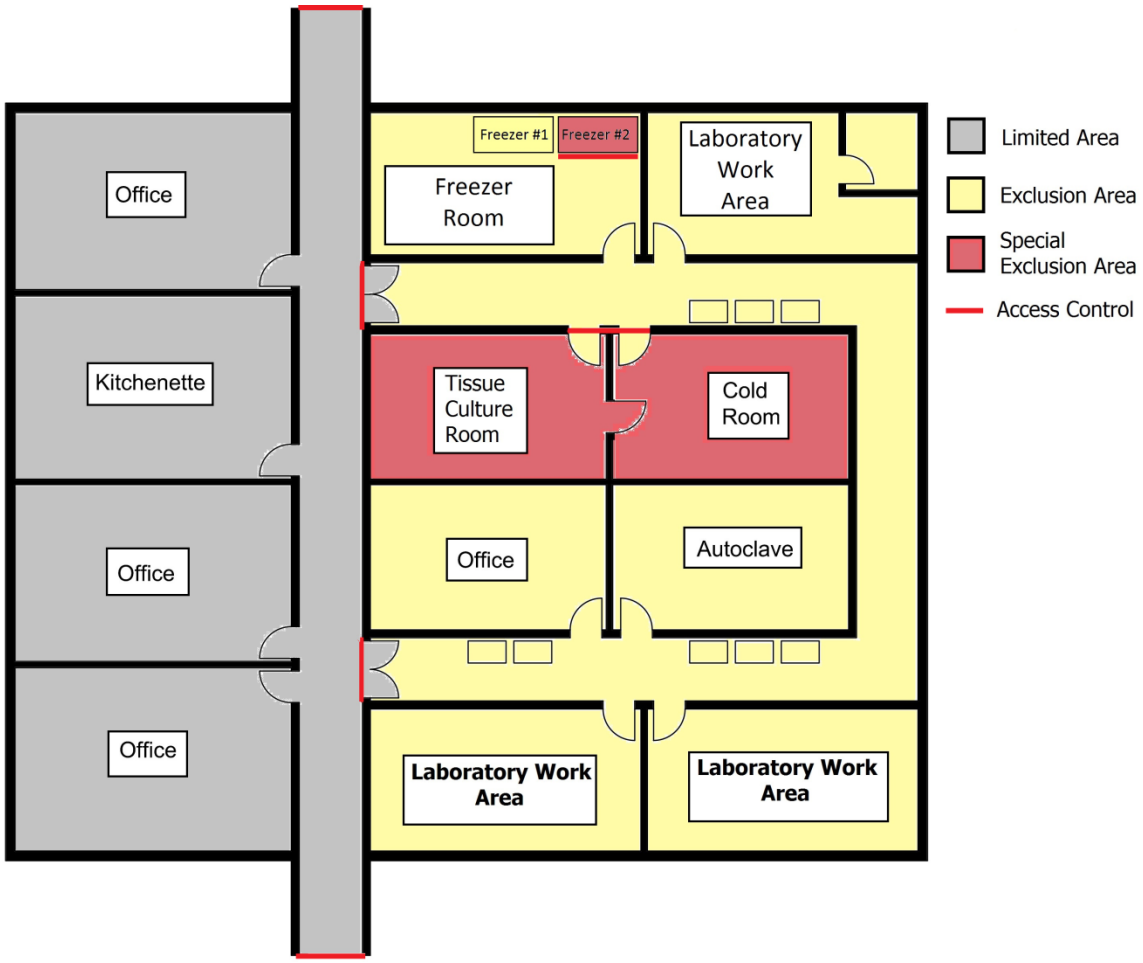

Figure 3-1: Example of graded protection areas in a facility.
Access to facility offices and common areas (kitchenette), indicated by gray shading, is limited to personnel authorized to access the facility. Additional access controls, indicated by red lines at entry points, restrict access to a laboratory wing (yellow shading) to authorized laboratory personnel. An additional level of access control restricts access to specific areas (red shading) within the laboratory wing to authorized personnel. The access control to freezer #2 in the Freezer Room can be in the form of a high security padlock on the freezer.

3.1.1 Additional security barriers

Multiple barriers may also force unauthorized individuals to use different strategies to defeat each barrier, thereby delaying the individual and providing response personnel time to intervene. Additional security barriers include locks or restraints to secure equipment, and lock boxes or lockable freezers for material stored in common or shared spaces. For example, locked storage equipment that is fixed in place, such as a cabinet, freezer, or refrigerator, that has been fastened to the wall or floor in such a manner that it is not moveable, is necessary if SSBAs are stored outside of the CL2 or CL3 containment zone.

A secure storage location or container should:

- be equipped with a robust locking mechanism or have other measures to prevent unauthorized access or removal;
- enable contents to remain protected when left unattended; and,
- be equipped with a system or mechanism to detect unauthorized entry or access.

3.1.2 Identifying SSBA Areas

The "part of the facility in which controlled activities with SSBAs are authorized" is a decision that will be made by the facility, taking into consideration what is most ideal for their particular situation. This can be a single room with the unique security features required for SSBA and access restricted to a small number of personnel, or a larger area that includes many rooms or the entire building that meet the same biosecurity requirements and that is accessible by many personnel.

For example, in Figure 3-1, the SSBA part of the facility can be defined as:

- the entire area shown;
- the laboratory wing including the cold room and tissue culture room; or,
- the tissue culture room, the cold room, and freezer #2.

Each scenario will have advantages and disadvantages, such as the need for additional physical security and operational biosecurity procedures; for example, the number of personnel requiring an HPTA Security Clearance, and the operational procedures that will need to be in place to accommodate entry of personnel without an HPTA Security Clearance.

3.2 Access Control

Physical and operational access controls restrict or limit entry to parts of a facility where pathogens or toxins are handled or stored or other sensitive assets reside, to **authorized personnel**. The type of controlled access system that is most suitable (e.g., key-locks with non-reproducible keys, electronic access card reader systems, keypads, key code systems, biometric readers) will depend on the particular situation.

The following measures are examples of ways to control access to assets:

- establish "controlled" entry points;
- implement manually activated locking devices, padlocks, card reader access, or biometric devices/systems at "controlled" entry points;
- implement a local alarm in the vicinity of the secure areas to alert nearby personnel of an intrusion or other problem.

Examples of access control measures are summarized in Table 3-1. Operational access controls are discussed in Section 3.4.

Table 3-1: Overview of access control measures and considerations for selection and implementation[3]

Access control	Security practices and considerations
Mechanical key	• use of non-reproducible keys • tracking of all keys issued to authorized personnel in a key log that is kept on file and up to date • change or rekeying of locks if a key is lost or compromised • immediate return of keys when personnel no longer need access, or upon resignation or termination • secure storage of unissued keys (e.g., in a key box)
Cipher key/ Combination lock	• keeping on file a list of individuals with access codes or keys • changing access codes or locks if codes or keys are compromised • documenting all changes to access codes or locks and considering this document sensitive information • keeping key log records on file and up to date • keeping on file a list of personnel who can change codes
Electronic keycard	• tracking all keycards issued to authorized personnel in a keycard log or database • keeping keycard records on file and up to date • including photo identification, name, and an expiry date on electronic keycards • return of keycards immediately upon resignation or termination of personnel • programming keycards to allow access to restricted areas only as required. (i.e., access to these areas is removed when personnel no longer need access)
Biometrics	• potential conflict of biometric systems with biosafety requirements (e.g., a fingerprint scan would be inappropriate in an area where personnel are required to wear gloves) • information security requirements of biometric data
Remote opening (e.g., "buzzing" a person in)	• keeping on file a list of individuals with authorized access • developing and following protocols or SOPs • information security requirements of this system
Visual recognition by a security guard	• locating a security guard at points of entry to visually verify access credentials
Multiple types of access control on same door	• Use of complementary security practices (e.g., electronic keycard and visual recognition by a security guard) for increased security

3.2.1 Windows

Windows and other openings that could provide access to secure enclosures, such as vent ducts, can be fitted with bars, a metal grille, or expanded metal mesh to provide enhanced security. Safety and security films and glazing can also help hold glass fragments together and prevent the window coming out of its frame if it is broken. Privacy films may also be of security value in some situations (e.g., windows on animal containment zones), but such films provide privacy only in certain lighting conditions. Window security hardware should be affixed from the inside to prevent tampering, or be fitted with tamper-resistant anchors if affixed from the outside. Windows located on the ground floor are more accessible and should therefore have additional measures in place (e.g., smaller openings) to prevent access.

In terms of glass strength, most types of glass can be easily broken with a solid object (e.g., rock). However, tempered glass and laminated glass are thicker and stronger than sheet glass. Some types of glass (e.g., laminated glass) also resist shattering when they are broken.

3.2.2 Doors

Doors that provide access to areas where assets are handled or stored should be locked when the areas are not in use. A door that is metal clad or constructed of solid-core wood, and that is installed in a reinforced frame of equivalent material clad, will offer a significant level of protection. Using non-removable pinned hinges in cases where the hinges are mounted on the non-secure side will help prevent the door from being removed. Where windows or vents are present on doors, fitting security glazing on the windows, or bars, a metal grille, or equivalent on any large vents (grilles) will prevent them from being broken or removed. Grilles should be secured in place with tamper-resistant anchors. It is a requirement in the CBS that doors to containment zones have biohazard signage, which helps avoid unintentional entry by unauthorized personnel. Similarly, signage on other doors, such as emergency exit doors, may also help avoid unintentional entry (e.g., "emergency exit only").

3.2.3 Fences and Gates

Facilities that contain high risk assets may consider installing a fence around the outer perimeter of the building. Fences that are less than 2.13 metres tall are not considered to be effective deterrents.[4] The number of entry/exit points in the fence should be kept to a minimum. They can be controlled by keeping gates locked when not in use, or having an entry control station at each gate that is continuously staffed with security personnel. Additional deterrent features include topping the fence with barbed wire or razor ribbon.

3.2.4 Locking Hardware

The effectiveness of a mechanical lock depends on the quality of the manufacturing (e.g., pin alignment), installation, lock design (e.g., number of pins, materials used), and state of repair. There are many types of key-operated locks that can be differentiated from each other by the mechanism (e.g., disc tumbler, pin tumbler, lever tumbler). Keyless locks such as combination locks use a wheel mechanism. Locks with combination codes or cipher-based keyless locks may not be suitable to protect assets that require a high level of security. Cipher locks with an alpha or numeric keypad may be vulnerable to individuals or groups who are able to deduce the access code from the appearance of the keys. No lock will offer guaranteed protection, but the expertise and time required to successfully defeat a high-security lock with force or skill may be sufficient to deter unauthorized individuals. When conventional locks and keys are used, they should be of high quality or of a high-security lock design such as key models with high security cylinders that contain a second set of pins, anti-picking resistance or non-reproducible keys (i.e., duplication by locksmiths, hardware stores, or home cutters not permitted). In terms of padlocks; high security steel shrouded models can be used.

Portable locks (e.g., key-operated padlocks) can be used to fasten multiple objects together, generally using a shackle. Locks should be made of hard materials to resist attacks using force, and have shielded shackles to prevent cutting of the lock. Spring-loaded padlocks are not recommended when a reasonable level of security is needed as it may be possible to disengage the locking mechanism using a shim, and if the body of the padlock is forcibly damaged or drilled out, the lock may spring open.

Master and grand master keying are sometimes used in facilities to allow individuals with a need to access many rooms to unlock multiple doors with a single key. In a grand master keyed lock series, a grand master key can open all of the locks in the series, and the master key can open a subset of locks in the series. Lock systems that have a master and a grand master key are discouraged largely because the loss or theft of a single key could compromise the security of an entire area, and also because these locks are generally easier to pick (multiple shear points in the chamber).

There are two types of lock bodies on doors: latch bolts and dead bolts. Latch bolts have a beveled end and are spring-loaded so the door will latch (or lock) automatically when it is closed. A disadvantage of latch bolts is that they are less secure than a deadbolt; unless the latch is equipped with an anti-shim device, a door locked with a single latch can be opened relatively easily using a thin shim (e.g., credit card). A deadbolt can only be moved to the locked or open position using a key (or the turn button from the inside). Deadbolts that extend at least 2.4 cm into the door frame provide good protection.

3.2.5 Electronic Controlled Access Systems

Electronic controlled access systems such as biometric and keycard/reader systems can be used to provide **restricted access** to authorized personnel only. Access credentials are presented to the controlled access system at an entry point. A database connected to the reader identifies the information about the individual, including whether or not the individual has authorization to gain entry at a particular entry point. The keycard may have a magnetic

stripe that is read by the reader, or contain a pattern that is scanned by the reader when the keycard is held in close proximity. Keycard/reader systems are currently the most common form of electronic controlled access, and the keycard is also often used as an ID card. Where an electronic system is in place, an alternate or auxiliary power backup source, should be in place in the event of a loss of primary power. Alternatively, if the access control is fail-secure, a backup restricted access system (e.g., using key-lock with non-reproducible keys) can be implemented.

One advantage of keycard/reader systems is that privileges associated with the card can be easily changed in the database in the event of a change in employment status, or if a keycard is lost or stolen.

Some general features of electronic controlled access systems include:

- the ability to identify and record where entry was made and which access credentials were used;
- the ability to permit or deny access depending on the time of day;
- the ability to change permission to access without changing any hardware;
- the ability to monitor the status of a door to indicate whether it is open, shut, or locked;
- the ability to link the information about individuals (e.g., photo, employee status, access expiration date); and
- the ability to be linked with other electronic security devices such as cameras.

One limitation to electronic controlled access systems that should be considered is the possibility of remote interference (e.g., overriding), whether through a building automation system or security console on the premises, or from a computer or device from a location off the premises. Another limitation is **tailgating**, which is allowing someone to enter with you into the controlled area. This is common in workplaces, as it is considered polite to hold the door open for co-workers. A possible solution could be for the person holding the door open to verify the ID cards of co-workers. Organizational policies and expectations for personnel should be clearly described during security awareness training. Security training is further discussed in Section 7.2.

There are many types of biometric devices that can be used to restrict access to a facility or parts of a facility. The systems can be based on recognition of an individual's eye, hand, finger, face, voice, or vasculature. A scanner is used to capture information from an individual and the information is searched against a database containing scanned patterns of authorized individuals. If a match is identified, the individual is granted access. The error rates of biometric systems can vary depending on the degree that the characteristic changes from day to day. For example, a voice recognition system may falsely reject an authorized individual who has a sore throat.

Table 3-2: Possible measures that may be implemented to mitigate biosecurity risks related to physical security in a CL2, a CL3, and an SSBA area

Biosecurity plan element	Risk	Possible Mitigation Measures		
		CL2	CL3	SSBA area
Physical Security	Unauthorized individual accessing the containment zone.	• Key-lock on door leading into the containment zone. • Procedure prohibiting employees from duplicating keys.	Option A • Key-lock with non-reproducible keys on door leading into the containment zone. • Procedure for removal of access authorization. Option B • Electronic key card access to containment zone. • Backup restricted access system using key-lock with non-reproducible keys. • Access control reverts to fail secure during emergencies.	Option A • Key-locks with non-reproducible keys on door leading into the containment zone. • Procedure for controlling access when individuals do not hold a valid HPTA Security Clearance. • Procedure for removal of access authorization. Option B • Electronic key card access to containment zone. • Backup restricted access system using key-lock with non-reproducible keys. • Access control reverts to fail secure during emergencies.
	Unauthorized individual accessing pathogens or toxins stored outside the containment zone.	• Storage equipment located outside the containment zone to be locked with a key-lock system (e.g., freezers are kept locked).	• Storage equipment located outside the containment zone to be locked with a non-reproducible key-lock system and located within an area with limited access.	• Storage equipment located outside the containment zone to be fixed in place (e.g., bolted to the wall) and locked with a non-reproducible key-lock system.

3.3 Detection of Unauthorized Access and Attempted Access

Detection systems in a facility are generally used to monitor and protect an area (e.g., site perimeter, restricted access area) rather than an object. For some CL2 facilities, it may be sufficient to implement operational procedures to challenge an unrecognized individual. In higher security areas, physical means of detection may be warranted to monitor (e.g., via security cameras, CCTV, or alarms) and record (e.g., electronic record of access) individuals entering or leaving the areas.

The following measures may enable the detection of attempted or successful unauthorized access in a timely manner:

- visual observation;
- alarm assessment via video;
- intrusion detection devices;
- inventory records (if verified frequently); and,
- seals or other tamper-indicating devices.

Areas that are not physically occupied (e.g., during off-hours) can be protected by intrusion detection systems and alarms. The various types of intrusion detection systems are described in Table 3-3. The sensors of an intrusion detection system are often placed at potential points of intruder entry (e.g., windows). If the intrusion detection system is triggered, it is desirable that a response team (e.g., security personnel, law enforcement) be alerted early so that a timely response can be initiated. If keypads are used to arm and disarm an intrusion detection system, the device and its electric junction box should be installed in a secure area to reduce the risk of tampering.

3.3.1 Intrusion Alarm Systems

To detect unauthorized access, attempted access or tampering, an alarm system should:

- activate immediately upon detecting an intrusion or tamper event;
- stay in an alarmed state until acknowledged by an authorized person;
- use more than one sensor or sensor type in order to provide redundancy;
- include overlapping sensor detection areas;
- use dedicated supervised communication links that are continually monitored;
- have an alternate or auxiliary power backup source, or equivalent, to maintain detection capability in the event of a loss of primary power; and
- have a low nuisance and false alarm rate with a high probability of detection.

In addition, the following general recommendations should be considered when using interior alarm systems:

- alarm monitoring devices and backup battery power should be protected against tampering by unauthorized individuals (e.g., electronic panel or junction box);
- dedicated alarm zones can be used in storage area (i.e., separate from other alarm zones such as a laboratory work area);
- an audit trail should be maintained to record the cause of any alarms; and,
- the alarm monitoring station should be continuously staffed.

3.3.2 Closed Circuit Television Surveillance

CCTV systems provide security personnel the ability to see into many secure areas from a central location. Many systems can also include audio. The most basic system consists of a camera, a means to transmit the video feed from the camera to a viewing site, a viewing screen, and a person who monitors the live video feed or recorded video. More complex systems may have multiple cameras, video motion detectors, a switcher to switch between cameras or a multiplexer to view multiple video feeds simultaneously, an annotator to record the time and date of the video, and computers that perform image processing functions (e.g., object recognition, search and playback functions). Cameras can be placed at strategic locations within the facility and on the facility perimeter (e.g., points of entry and exit, at sensors that are connected to alarms). Video captured from CCTV systems can provide a critical record of incidents, which can be used as evidence in incident investigations.

With the evolution from analog to digital imaging technology, various computational functions can be integrated into the security system. For example, videos can be screened for infrequent image sequences, such as the presence of a person, object, or vehicle, that may be of significance. Cameras can also be controlled remotely. Improvements in technology have also led to the use of colour cameras with higher resolution, making objects easier to identify.

CCTV systems can also play a role in emergency response. It allows security personnel to remotely view locations and assess the situation. If the CCTV system is integrated with an intrusion detection system, it can be used to determine the cause of an intrusion alarm (e.g., if it was triggered by a human). Electronic files can be copied to other media (e.g., DVD, USB flash drive) to be stored long term, should they be needed as evidence.

Table 3-3: Summary of Intrusion detection systems.

Detection System	Description	Possible Uses	Limitations	Dependencies
Infrared Motion Detector	Detects a change in ambient temperature.	• inside restricted access areas • along halls that lead to restricted access areas • through closed doors that lead to restricted access areas • near storage equipment that contain pathogens or toxins	• areas that contain items/ equipment that produce heat • very large areas • rooms housing animals	Needs to be placed in strategic areas throughout a facility.
Contact Switches	Detects when a circuit is broken (e.g., door or window opened).	• windows or doors that lead into restricted access areas	• areas with glass windows or doors that provide direct access to restricted access area	May also require broken glass sensors.
Broken Glass Sensors	Detects the sound frequencies and vibrations generated by breaking glass.	• laboratories with glass windows that provide access to a restricted access area	• facilities in regions with frequent severe storms • facilities with non-glass windows	All doors and windows need to be equipped with a sensor.
Acoustic Motion Sensor	Detects motion by emitting and detecting sound waves that reflect off objects.	• inside restricted access areas • along halls that lead to restricted access areas • near doors that lead to restricted access areas • near storage equipment containing pathogens or toxins	• animal rooms and animal cubicles • rooms containing loud equipment (e.g., shakers, incubators) • very large areas	System needs to be placed in specific key areas.
Acoustic Sensor	Monitors sounds to determine when an intrusion occurs or to determine the nature of the intrusion.	• inside restricted access areas • along halls that lead to restricted areas	• animal rooms and animal cubicles • rooms with background noise (e.g., rooms containing loud equipment) • facilities without exterior sound dampening	Exterior sounds need to be sufficiently blocked (e.g., sounds from laboratory next door).
Visual Monitoring	Video image is captured by a camera and monitored by security personnel (e.g., CCTV).	• cameras can be placed at points of entry on the facility perimeter	• video quality is affected by visibility conditions (e.g., light levels, heavy rain)	Image needs to be either continuously staffed, or video feed recorded and integrated with the intrusion alarm system.

3.3.3 Tamper-Evident Technology

Tamper-evident tapes, labels, and seals can be used to visually detect unauthorized access to protected assets such as freezers, vials, boxes, or other vessels containing pathogens or toxins. Commercially available devices include flip-top vials and screw-cap containers that can be secured with plastic mechanisms that detach upon opening.

3.3.4 Lighting

Outdoor lighting at a facility can be used to enhance safety for authorized individuals entering and exiting the building. It can also serve to deter or detect intrusion by improving image quality of video from outdoor cameras. There are several types of lighting including incandescent lamps, high intensity discharge lamps, fluorescent lamps, and light emitting diodes (LED). Lighting should be selected based on its intended application. For example, motion activated lighting needs to reach maximum output quickly, and lighting for video monitored areas may need a particular colour output in order to capture image detail.

Some experts argue that dim lighting conditions are worse than providing no light at all. Consider that bright light allows for easy visual detection of intruders, and while complete darkness provides cover, it also makes it difficult for an intruder to defeat a barrier. However, dim light may be sufficient for an intruder to manipulate a lock and may be insufficient to enable detection from a camera.

3.4 Operational Considerations for Access Control

Operational access control measures can be used alone or in combination with physical measures to restrict access to a facility or parts of a facility. Having policies and procedures in place (e.g., for key control, access codes, and visitors) and training staff so that they understand and follow established procedures are fundamental to maintaining a secure facility. The policies and procedures should also outline the responsible authority within the facility who can approve the personnel authorization process and identify those individuals who are permitted to authorize personnel to access given areas. The authorization process can involve a series of approvals (e.g., from human resources, facility security, and supervisors), with the individual having to meet all access requirements (e.g., appropriate professional qualifications, completion of biosafety and biosecurity training, and if required, HPTA Security Clearance) prior to being granted access.

3.4.1 Identify Authorized Personnel

A process or policy should be established to grant, alter, or remove access authorization when personnel (e.g., containment zone personnel, trainees, visitors, management personnel, students, maintenance staff, emergency response personnel) need temporary access, no longer need access, resign, or are terminated. The process can involve deactivation of electronic keycards, surrender of keys, keycards, and ID cards, or the change of key codes. The policy should define the criteria that must be met before access is granted, which may

include medical clearance, training requirements, and HPTA Security Clearance or accompaniment and supervision.

The list of authorized individuals should be reviewed on a regular basis. The review may be more frequent in facilities where:

- there are SSBAs being handled or stored;
- there are a large number of individuals with access (e.g., larger facilities);
- there is frequent turnover of individuals with access (e.g., academic facilities);
- there is frequent turnover of projects (e.g., animal studies).

Consideration should also be given to restricting access to security management systems and software in order to prevent unauthorized interference.

3.4.2 Develop Access Control Procedures

SOPs or written protocols should be developed to assist staff in determining whether or not an individual is authorized to access a facility, including the steps to take for identifying, challenging, removing, and reporting unauthorized and suspicious persons. There should also be policies and procedures in place for access to the facility by cleaning, maintenance, and repair personnel (e.g., with an escort, pathogens or toxins secured and inaccessible). A policy on the wearing of photo IDs (e.g., always displayed within the facility, and never worn outside) would help identify authorized individuals.

Where key codes or cards are used in electronic access control systems, a policy should be established forbidding personnel from sharing access credentials (e.g., sharing one's card or code, or tailgating). Key cards used in conjunction with a key code increase the level of security.

Finally, an SOP should be established for reporting lost, stolen, or compromised access keys, cards, or codes so that corrective measures can be implemented in a timely fashion.

3.4.2.1 Keys

Records should be maintained for keys and related systems (e.g., keycards, codes, and combination locks) that limit or restrict access to containment zones, infectious material, or toxins. These records should include:

- the names of the individuals to whom the key, code, or combination has been issued;
- the date of issuance, or revocation.

The organization should have a process in place to retrieve keys or have them returned by personnel when access is no longer required, and to securely store unissued keys (e.g., secured key cabinet or safe).

It is considered good key control practice to:

- limit the number of individuals with keys to those who need access;
- restrict the number of master keys to management and individuals who may require access to all areas (e.g., the BSO);
- conduct a review of the key inventory and key holders on a regular basis (e.g., monthly, semi-annually, annually) based on staff turnover to account for all issued and unissued keys, and for keys that have been reported lost or stolen;
- have established communication channels between the key issuer(s) and the human resources department to facilitate timely notification of changes in employment status of individuals;
- prohibit personnel from duplicating keys;
- use a patented non-reproducible key or dedicated keyway to prevent unauthorized duplication;
- ensure that keys issued to security personnel such as master keys are handed over from shift to shift and never leave the facility; and
- change access codes from the factory default when a lock is installed, if applicable.

An emergency access key should be kept in a secure location (e.g., secured key box) for use in emergency situations. If the emergency access key is used, an entry should be made in the key records, and the responsible individual (e.g., BSO) should be notified.

3.4.2.2 ID Cards

An ID card is photo identification issued by the organization that is not linked to an electronic access control system; however, electronic keycards can also serve as an ID card if the authorized individual's name and photo appear on the card.

ID cards should contain a photo of the authorized individual for security and other personnel to compare against, the name of the individual, and the expiry date. ID cards may be colour-coded to indicate authorization to access specific restricted parts of a facility. This system enables personnel inside the restricted area to monitor and detect unauthorized individuals. For example, a security guard can allow an individual to pass a manned security checkpoint based on visual verification of employee credentials (e.g., valid ID card with photo, photo identification and the name of the individual appears on the list of authorized personnel). Depending on the level of security required, visual identification by a security guard may not be a suitable controlled access option for organizations that have many employees (e.g., more than 30 per shift).

In order for an ID card system to function, all authorized individuals need to display their cards at all times while in the facility, except where biosafety requirements do not permit it (e.g., CL3, CL4). Personnel should routinely verify the identities of other personnel they happen across throughout the day and any employee found without their ID card escorted out of the restricted area or reported to the appropriate internal authority.

ID cards issued to personnel who require access to a facility or parts of a facility should be documented in a manner similar to keys as described above. ID cards should also be promptly returned to the individual responsible for issuing them when access is no longer required (e.g., change in duties, retired, dismissed). Access privileges associated with electronic keycards can be easily changed in the electronic access system.

An operational control that can be used to reduce the risk associated with ID card tampering involves an exchange system. Employees are issued two ID cards with identical photographs of the employee. One simply serves as identification of the employee, while the other is coded (e.g., with a different border or background colour) to clearly indicate the parts of the facility that the individual is authorized to access. The employee exchanges the non-coded ID card for the coded one at the start of their shift. At the end of the shift, the employee returns the coded ID card in exchange for the non-coded one.

3.4.2.3 Electronic Key Cards

Electronic key cards, whether generic or serving as an ID card, can be used to provide electronic access to a containment zone (e.g., swipe, proximity, or chip card reader). In lower security areas, the card alone may be sufficient. To access higher security areas, the use of a key code linked to the card will prevent unauthorized access from individuals who find or steal a card.

3.4.2.4 Accompaniment and Supervision

Protocols for the entry of trainees, visitors, students, maintenance staff, emergency response personnel, and other individuals who require temporary access are important considerations when evaluating access control. This may include documenting the individual's name and date of entry, issuing a temporary ID card that clearly identifies the purpose of that individual (e.g., visitor, repair technician), and the name of the individual's escort, if applicable.

Authorized individuals entering the part of the facility with restricted access are to meet all requirements in the CBS, HPTA, and HPTR. Additional organizational requirements may also apply as determined by an LRA.

Procedures to allow visitors to enter areas of a facility where access is limited or restricted to authorized personnel should be included in the biosecurity plan. Depending on the containment zone, this could include varying levels of supervision. For example, one supervisor may be sufficient for a group of university students visiting a CL2 laboratory.

For facilities where SSBAs are handled or otherwise accessible, authorized individuals are to have an HPTA Security Clearance. Granting access to persons without an HPTA Security Clearance (including visitors) is permitted only when the SSBAs are secured and inaccessible, or when the person is properly accompanied and supervised by an authorized individual with an HPTA Security Clearance. The authorized escort can only accompany and supervise one individual at a time (HPTR 23), and monitor their activities at all times while accompanying and supervising the escorted individual. The authorized escort should remain alert for suspicious behaviour by the individual being escorted.

An individual who has previously been denied an HPTA Security Clearance or had it suspended or revoked is not permitted to enter the area, even under supervision, unless a new HPTA Security Clearance has been issued to them since the refusal, suspension or revocation (HPTR 24).

3.4.2.5 Removal of Access Authorization

When an individual no longer needs access to an area, or their authorization to access an area has been revoked, the responsible authority of the facility should take steps to remove that individual's access authorization to the areas where access is no longer needed. In areas where SSBAs are handled or stored, removal of access authorization must take place immediately. Appropriate measures may include retrieving keys and ID card, changing locks, and updating electronic access records.

In SSBA areas, the responsible authority should immediately inform the affected person of the parts of the facility, or the entire facility, that they are no longer authorized to access. In addition, it is a requirement under the HPTA and HPTR (HPTA 32, HPTR 7) that the PHAC be immediately notified in such cases. Notifications can be submitted electronically to the PHAC through the Biosecurity Portal, accessible through the PHAC website (www.publichealth.gc.ca/pathogens), by telephone, fax, or email (PHAC.LINC-DILC.ASPC@canada.ca).

3.4.3 Security and Shared Spaces

A shared laboratory space is a laboratory model that is becoming more common. It is a model that creates laboratory environments that are responsive to present needs and capable of adapting to future demands. Shared spaces located inside the part of a facility where controlled activities with SSBAs have been authorized under a licence may present challenges for all personnel needing access. Facility management, directors, and the licence holder will need to determine how best to address these challenges.

One option is for all individuals who work in the shared spaces to hold a valid HPTA Security Clearance so that they can freely access the part of the facility when SSBAs are present at any time. Alternatively, access by persons without an HPTA Security Clearance (e.g., those who do not actually need access to the SSBAs) to shared facilities can be limited to times when there are no SSBAs present, when the SSBAs are locked away and inaccessible, or when they are accompanied and supervised by an individual who holds an HPTA Security Clearance for that part of the facility. This alternative option may be achievable through the use of schedules and secure storage areas for the SSBAs.

Shared laboratory space usage should consider:

- the type of activity to be undertaken in the shared space;
- the individuals who will require access;
- the potential to separate activities by time (specific hours when activities requiring

enhanced security measures are to be undertaken);
- procedures for SSBA waste management; and
- the need for locks and alarms on specific pieces of equipment such as freezers and incubators that contain assets, and for information or asset storage areas.

References

1 Government of Canada. (2015). *Canadian Biosafety Standard* (2nd ed.). Ottawa, ON, Canada: Government of Canada.

2 Fennelly, L. (2013). *Effective Physical Security* (4th ed.). Waltham, MA, USA: Elsevier Inc.

3 U.S. Centers for Disease Control and Prevention (CDC) Division of Select Agents and Toxins and Animal and Plant Health Inspection Service (APHIS) Agricultures Select Agent Program. (2013). *Security Guidance for Select Agent or Toxin Facilities* (2nd Revision). Retrieved 2/9, 2016 from http://www.selectagents.gov/resources/Security_Guidance_v3-English.pdf

4 United States Geological Survey, United States Department of Interior. (2005). *Physical Security Handbook*, 440-2-H. Retrieved 15/03, 2016 from http://www.usgs.gov/usgs-manual/handbook/hb/440-2-h/440-2-h.html

CHAPTER 4

PERSONNEL SUITABILITY AND RELIABILITY

CHAPTER 4 - PERSONNEL SUITABILITY AND RELIABILITY

Personnel suitability and reliability policies and procedures should be developed to define and document the training, experience, competency, and suitability requirements for personnel who have access to pathogens, toxins, or other infectious material. Employee pre-hiring screening protocols should be developed to evaluate the integrity of individuals with access to pathogens, toxins, or other regulated infectious material and may include background checks and HPTA Security Clearances; behavioural indicators should also be assessed at this time. An ongoing reliability program which seeks to promote acceptable behaviour can also be beneficial in reducing the risks associated with personnel. For example, the availability of programs (e.g., counselling services) that offer assistance to employees is one method to reduce the risks that an employee experiencing personal difficulties will become an insider threat. Examples of possible measures that may be implemented to mitigate biosecurity risks related to personnel suitability and reliability are provided in Table 4-1.

4.1 Personnel Suitability and Reliability Screening

Personnel suitability and reliability policies and procedures for the collection and verification of information from applicants should be established to address the risk from a potential insider threat. The policies and procedures should include a description of how this information will be evaluated and used to determine applicant suitability. The training, experience, competency, and other suitability requirements for personnel who have access to pathogens or toxins should be clearly defined and documented. It is also prudent to outline procedures to evaluate personnel suitability in the biosecurity plan. The rigor of the pre-screening process (e.g., years of historical data reviewed, number of references contacted, number of topics examined) should be appropriate to the level of risk associated with the assets.

Through the hiring process, screening of candidates confirms they have the appropriate credentials, skills, and personal traits to undertake work with pathogens or toxins, and that they are the best fit for the position prior to being offered a position and granted access to pathogens, toxins, or other assets. Academic and professional credentials, prior experience, and publication history (e.g., information contained in a *curriculum vitae* [CV]) qualify an individual's scientific ability and credibility, while personal and professional references can provide an indication of the individual's suitability to handle or access pathogens and toxins.

In addition to the points listed above, pre-hiring screening protocols may include verification of:

- immigration and visa status;
- criminal record history; and
- other criteria, as deemed appropriate by your institution (e.g., credit history checks, occupational health evaluation, drug testing).

If the hiring organization does not have access to the tools needed to conduct these screening processes, local law enforcement agencies may be able to provide assistance.

Table 4-1: Possible measures that may be implemented to mitigate biosecurity risks related to personnel suitability and reliability in a CL2, a CL3, and an SSBA area

Biosecurity plan element	Risk	Possible Mitigation Measures		
		CL2	CL3	SSBA area
Personnel Suitability and Reliability	Individual not meeting minimum suitability and reliability requirements is given access to pathogens and toxins	• Pre-hiring policy includes verification of candidate CV, references, and proof of education. • References assess candidate's technical and behavioral competencies.	• Pre-hiring policy includes verification of candidate CV, references, proof of education and other criteria as deemed appropriate (e.g., credit check). • References assess candidate's technical and behavioural competencies.	• Pre-hiring policy includes verification of candidate CV, references, proof of education and a valid HPTA Security Clearance. • References assess candidate's technical and behavioural competencies.
	Individual who no longer meets minimum requirements for reliability continues to have access to pathogens and toxins	Ongoing reliability assessment: • Procedures include self and peer reporting procedure. • Graduated disciplinary actions are established for individuals not complying with established biosecurity practices. • Procedures for removing or temporarily suspending an individual's access to pathogens and toxins or the containment zone.	Ongoing reliability assessment: • Procedures include self and peer reporting procedure. • Graduated disciplinary actions are established for individuals not complying with established biosecurity practices. • Procedures for removing or temporarily suspending an individual's access to pathogens and toxins or the containment zone. • Policy requiring assessment of individual returning from relevant leave (e.g., stress).	Ongoing reliability assessment: • Procedures include self and peer reporting procedure. • Graduated disciplinary actions are established for individuals not complying with established biosecurity practices. • Procedures for removing or temporarily suspending an individual's access to pathogens and toxins or the containment zone. • Policy requiring assessment of individual returning from relevant leave (e.g., stress). • Procedure for reporting information regarding circumstances that may affect the status of an individual's HPTA Security Clearance.

4.2 Ongoing Reliability Assessment Program

An ongoing reliability program aims to verify that an individual authorized to access pathogens, toxins, or other assets continues to meet the established criteria for personnel suitability and seeks to reinforce acceptable behaviour. This type of program can be beneficial in reducing the risks associated with personnel (i.e., insider threat) by identifying and offering assistance to employees who are experiencing problems. It is important for an organization to remain engaged and to regularly verify current information to ensure continued employee suitability for access to pathogens and toxins.

Personnel should be encouraged to report any information that may impact the safety or security of individuals, facility assets, or the community at large to internal authorities or facility security personnel. This information may include:[1]

- circumstances that may affect the status of an individual's HPTA Security Clearance;
- circumstances that may affect the ability of an individual to perform his or her duties in a safe and secure manner (e.g., significant increase in distraction or mistakes; increase in risk-taking behaviours);
- significant changes in behaviour, attitudes, demeanor, or actions such as:
  - increasingly withdrawn,
  - significant and prolonged deterioration in appearance,
  - unjustified anger or aggression,
  - signs of alcohol/drug abuse,
  - criminal activity,
  - unexplained absences;
- stated or implied threats to colleagues, institutions, the security of assets, the well-being of laboratory animals, or the general public;
- willful non-compliance with institutional policies and SOPs, as well as applicable legislation and the CBS;
- information that causes an individual to have concerns about his or her own ability to perform a job safely and securely;
- circumstances that appear suspicious such as:
  - laboratory work that does not correspond to official project work or goals,
  - unjustified requests for security or laboratory information,
  - acts of vandalism or property damage,
  - attempts to enable friends or colleagues to gain unauthorized access to parts of a facility; and
- unauthorized work performed during off-hours.

Organizations should consider denying or removing access to individuals who exhibit qualities or behaviours that suggest the individual is incapable of safely working with, or protecting the security of, the pathogens, toxins, or other assets handled or stored in the facility. Organizations should develop policies regarding self- and peer-reporting, and protocols for removal of an individual's authorization to access parts of the facility or assets, or for the

immediate removal of an individual who is deemed to pose an unacceptable safety or security risk. All individuals should be clearly instructed on all policies and protocols. In some instances, methods for anonymous reporting may encourage reporting, and should be considered when developing reporting policies and procedures. These processes and procedures should be developed in consultation with the institutional human resources department.

4.3 HPTA Security Clearances

The increased biosecurity risks associated with SSBAs necessitates additional biosecurity measures, such as security screening for personnel with access to SSBAs, to mitigate the risk of potential insider threats. As such, the security screening process includes an additional requirement for individuals working in parts of a facility where SSBAs are handled or otherwise accessible; these individuals are required to obtain an HPTA Security Clearance in accordance with section 33 of the HPTA.[2] The HPTA Security Clearance process is conducted by the Royal Canadian Mounted Police (RCMP) and Canadian Security Intelligence Service (CSIS) on behalf of the PHAC, and is a key biosecurity element of the regulatory framework under the HPTA to verify the credibility and suitability of all individuals who access SSBAs. Figure 4-1 describes situations where an HPTA Security Clearance is required and where it is not required.

Further information on the validity period and the portability of HPTA Security Clearances can be found in Section 6.3.3 of the CBH. Information regarding suspension and revocation of an HPTA Security Clearance and the obligation to notify the PHAC of a criminal offense can be found in Sections 6.3.4 and 6.3.5, respectively, of the CBH.[3]

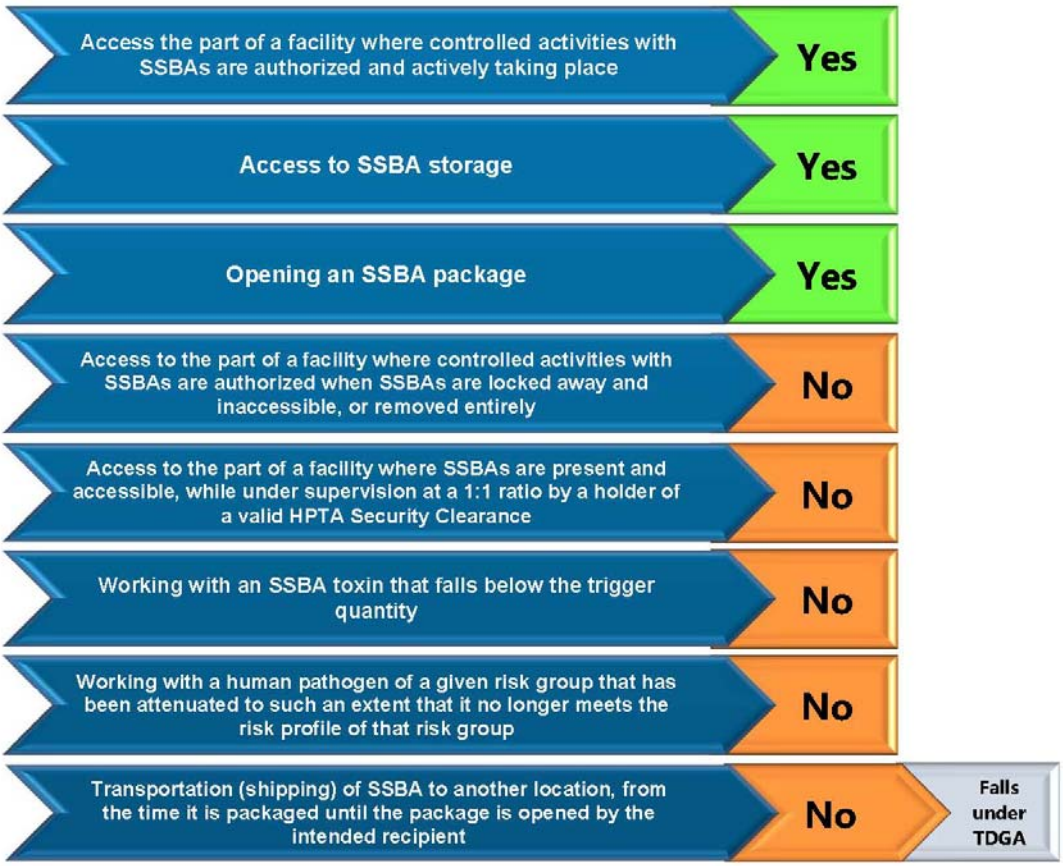

Figure 4-1: Situations where an HPTA Security Clearance issued by the PHAC is required.

The *Transportation of Dangerous Goods Act* (TDGA) governs dangerous goods while in transit.[4]

References

1 United States National Institutes of Health), National Science Advisory Board for Biosecurity. (2011). *Guidance for Enhancing Personnel Reliability and Strengthening the Culture of Responsibility.* Retrieved 2/8, 2016 from http://osp.od.nih.gov/sites/default/files/resources/CRWG_Report_final.pdf

2 *Human Pathogens and Toxins Act* (S.C. 2009, c. 24). (2015).

3 Government of Canada. (2016). *Canadian Biosafety Handbook* (2nd ed.). Ottawa, ON, Canada: Government of Canada.

4 *Transportation of Dangerous Goods Act, 1992* (S.C. 1992, c. 34). (2015).

CHAPTER 5

PATHOGEN AND TOXIN ACCOUNTABILITY AND INVENTORY CONTROL

CHAPTER 5 - PATHOGEN AND TOXIN ACCOUNTABILITY AND INVENTORY CONTROL

Pathogen and toxin accountability and inventory control procedures are established in order to track and document all pathogens, toxins, and other regulated infectious material in **long-term storage** within the organization, to protect and secure these assets against loss, theft, misuse, diversion, and release. Material control also includes procedures to account for and safely move a pathogen or toxin within the facility, or to transport it to a different building within the organization or to a different organization. The level of accountability and control measures are identified by the biosecurity risk assessment.

5.1 Pathogen and Toxin Accountability

Accountability is a means of establishing ownership of pathogens and toxins and defining the responsibilities of each authorized individual for the oversight of pathogens and toxins within the facility. Under the HPTA, HPTR, HAA and HAR, all authorized individuals are accountable for their actions and decisions involving pathogens, toxins, and other regulated infectious material.[1,2,3,4] These individuals are also answerable to their supervisors, containment zone or facility managers, the licence holder or animal pathogen import permit holder, and also accountable to the PHAC and the CFIA.

For higher risk pathogens and toxins (i.e., SSBAs, RG3, and RG4), accountability measures should include regular inventory audits to verify the accuracy of the inventory and, where applicable, that inventoried materials or the inventory itself have not been tampered with. This may be accomplished through physical verification that the material listed in the inventory is in place, verification during onsite **movement** or transfer, remote observation through CCTV, or verification of seals or other tamper-evident devices on storage containers and equipment. A robust inventory control process may include conducting periodic analysis to confirm the contents of containers.[5] Maintaining records of the entry and exit of all individuals confirms who was present in the containment zone at any point in time. This information may be used in investigations of missing pathogens or toxins from the inventory.

Examples of possible measures that may be implemented to mitigate biosecurity risks related to pathogen and toxin accountability are provided in Table 5-1. Further guidance on pathogen and toxin accountability is provided in Chapter 19 of the CBH.

Table 5-1: Possible measures that may be implemented to mitigate biosecurity risks related to pathogen and toxin accountability in a CL2, a CL3, and an SSBA area

Biosecurity plan element	Risk	Possible Mitigation Measures		
		CL2	CL3	SSBA area
Pathogen and Toxins Accountability	Shipment of pathogens or toxins is lost in transit.	• Procedure requiring the tracking of parcels during shipping. • Procedure outlining reporting structure and timelines for pathogens and toxins lost in transit. • Procedure for notifying the PHAC or the CFIA of a missing pathogen or toxin.	• Procedure requiring the tracking of parcels during shipping. • Procedure outlining reporting structure and timelines for pathogens and toxins lost in transit. • Procedure for notifying the PHAC or the CFIA of a missing pathogen or toxin. • Procedure requiring the shipper to confirm receipt of the material by the consignee.	• Procedure requiring the tracking of parcels during shipping. • Procedure outlining reporting structure for an SSBA pathogen or toxin not received within 24 hours of when it was expected, including mandatory notification of the PHAC. • Procedure requiring the shipper to confirm receipt of the material by the consignee.

5.2 Inventories and Inventory Control

An inventory of pathogens, toxins, and other regulated infectious material in long-term storage (i.e., greater than 30 days) within the containment zone is required as per CBS Matrix 4.10, and is also an important component of the biosecurity plan. This requirement does not apply to material that is in use for less than 30 days (e.g., ongoing culture of infectious material, long-term animal infection studies). The inventory requirements and the level of detail of information in an inventory will be proportional to the risk associated with the material stored and other needs of the containment zone or facility (e.g., compliance with quality management standards such as the International Organization for Standardization [ISO] 9001)[6]). The inventory can be in any format (e.g., written ledger, electronic database or spreadsheet) as long as it accurately reflects the presence of the pathogens and toxins in long-term storage within the facility.

For RG2 pathogens and toxins in long-term storage, it is sufficient to document the location and risk group. In the case of RG3, RG4, and SSBA pathogens and toxins in long-term storage, the inventory must include specific identification of the pathogens and toxins, as well as a means to detect a missing or stolen sample in a timely manner (e.g., building, room, and exact location in freezer, log of number of vials).

While it is not a requirement to maintain an inventory of pathogens and toxins stored for less than 30 days, such as recently received material or material in ongoing use (e.g., cultures), it is best practice to maintain a record of all material entering or leaving the containment zone.

Even laboratory notes or records of diagnostic activities (e.g., cultures) can prove valuable should pathogens or toxins go missing.

It is recommended that facilities conduct a review of their inventory and access records to verify the accuracy of the inventory following any suspicious activity or incident during which they may have been accessed.

Effective inventory measures for pathogens and toxins in long-term storage can be a suitable way to deter and detect insider threats. Considerations for implementing a robust pathogen and toxin inventory and accountability system include:

- designating a single qualified individual to be responsible for the maintenance of the inventory;
- updating the inventory as materials are added and removed;
- documenting all transfers, inactivation, and disposal of material;
- capturing all pathogens, toxins, and other regulated infectious material in the inventory, including material stored outside of the containment zone;
- defining and documenting all persons who have access to the materials and to the area where the materials are handled or stored;
- referencing relevant documentation (e.g., animal pathogen transfer authorization, import permits);
- labelling all pathogens, toxins, and other regulated infectious material in long-term storage appropriately; and
- labelling items in sequential order (e.g., a vial out of sequence can be easily detected).

The level of information security associated with the inventory list should correlate with the risk group of the pathogens or toxins used (e.g., RG2 pathogen versus SSBA) and, at the very least, meet the requirements outlined in the CBS. Examples of possible measures that may be implemented to mitigate biosecurity risks related to inventory control are provided in Table 5-2. Further details on information security can be found in Chapter 7.

Table 5-2: Possible measures that may be implemented to mitigate biosecurity risks related to inventory control in a CL2, a CL3, and an SSBA area

Biosecurity plan element	Risk	Possible Mitigation Measures		
		CL2	CL3	SSBA area
Inventory control	Missing pathogen or toxin is not detected.	• Procedure requiring biannual inventory audit by laboratory manager and ad hoc audits by the BSO.	• Procedure requiring biannual audit by the BSO and quarterly audits by the laboratory manager.	• Procedure requiring biannual audit by the BSO and quarterly audits by the laboratory manager, with increased sample size.

5.3 Security during Movement and Transportation

The biosecurity plan should contain policies and procedures describing accountability measures to protect pathogens and toxins from insider and outsider threats when the materials are moved or transported from one location to another. This includes shipping pathogens and toxins to another facility, as well as moving them from one location to another within the same building.

Procedural controls may also be established to reduce the biosecurity risk associated with received packages. This includes personnel training and the development of protocols for unexpected shipments of pathogens or toxins. All packages and items should be inspected before they are brought into or removed from the part of the facility licensed for controlled activities.

Some facilities may have a centralized receiving area from which all parcels are brought unopened to the consignee (receiver) by facility personnel. Other facilities may designate a "specimen receiving area" where parcels containing pathogens, toxins, and other infectious material are opened, receipt of the parcel documented, and the specimens sorted for movement (or **transportation**) to the appropriate individual or area for further handling or storage. If SSBAs are received in a specimen receiving area (i.e., the SSBA parcel is opened), the receiving area is considered part of the facility where SSBAs are handled or stored, and access to the area must be restricted to authorized persons with a valid HPTA Security Clearance when SSBAs are present and accessible.

All transfers between licence holders, whether internal or external, require notification of the BSO before the transfer occurs, even in situations where reporting to the PHAC or the CFIA is not required.

5.3.1 Internal Transfers

Facilities that transfer pathogens or toxins within the organization should include in the biosecurity plan policies and procedures describing how the transfers will take place, including provisions for safeguarding the pathogens and toxins against theft, loss, or release (e.g., a policy against leaving pathogens and toxins unattended in public areas).

Facilities transferring an **animal pathogen** that has been imported under an animal pathogen import permit issued by the CFIA require authorization from the CFIA prior to the transfer from the location specified on the import permit, whether the transfer is within or between facilities. If transferring is an authorized activity under a Pathogen and Toxin Licence issued by the PHAC, transfers of human and animal pathogens are permitted and do not need to be reported to the PHAC; however, the BSO must be notified.

A material transfer agreement or similar record may be used to document who has control of the material and is accountable at each point in the movement or transfer.[1] This documentation protects against pathogens and toxins being left unattended, and can serve to confirm that everyone who had possession of the package had the appropriate training to handle the material. For higher risk material such as SSBAs, a signature or chain-of-custody sheet would

provide a record of all individuals who had possession during the transfer and confirm they had the appropriate HPTA Security Clearance.

5.3.2 External Transfers and Exports

Under the HPTR, persons transferring human pathogens or toxins within Canada must take reasonable care to satisfy themselves that the intended recipient is licensed to work with the agent or otherwise exempted from the requirement to hold a licence. In a similar manner, the sender **exporting** human pathogens and toxins outside of Canada must take reasonable care to satisfy themselves that the intended recipient will follow the applicable biosafety and biosecurity standards and policies in the foreign jurisdiction. The same applies to animal pathogens imported under a Pathogen and Toxin Licence issued by the PHAC. Transfers of animal pathogens, including zoonotic pathogens, that have been imported under an animal pathogen import permit issued by the CFIA can only occur after obtaining authorization from the CFIA.

The *Transportation of Dangerous Goods Act* and *Regulations* (TDGA, TDGR) apply to shipments of infectious material and toxins from consignment to receipt.[7,8] While there is a limit to the oversight that the organization can provide once the pathogens and toxins are in transit, there are measures that can be taken prior to consignment to mitigate biosecurity risks. For example, a reputable courier can be selected to transport the material, or authorized facility personnel who are TDG certified can be used.

It is a requirement that the BSO be notified before arrangements are made to import or receive a human pathogen or toxin (HPTR 4[1]). This allows for attempts to be made to locate the package if it is not received within a reasonable time of when it was expected. Depending on the courier service, the shipper and receiver may also be able to track the parcel using the courier's online tool. In addition, the BSOs of both institutions are to be informed of the transfer prior to making any shipping plans. Under the HPTR, the BSO must also be informed of any SSBA shipment that is not received within 24 hours of when it was expected. Subsequently, the BSO must notify the PHAC, which can be submitted electronically to the PHAC through the online Biosecurity Portal, accessible through the PHAC website (www.publichealth.gc.ca/pathogens), by telephone, fax, or email (PHAC.LINC-DILC.ASPC@canada.ca).

References

1 *Human Pathogens and Toxins Act* (S.C. 2009, c. 24). (2015).

2 *Human Pathogens and Toxins Regulations* (SOR/2015-44) (2015).

3 *Health of Animals Act* (S.C. 1990, c. 21). (2015).

4 *Health of Animals Regulations* (C.R.C., c. 296). (2015).

5 Salerno, R. M., & J. Gaudioso. (2007). *Laboratory Biosecurity Handbook*. Boca Raton, FL, USA: CRC Press.

6 *ISO 9001:2008, Quality Management Systems - Requirements*. (2008). Geneva, Switzerland: International Organization for Standardization.

7 *Transportation of Dangerous Goods Act, 1992* (S.C. 1992, c. 34). (2015).

8 *Transportation of Dangerous Goods Regulations* (SOR/2001-286). (2015).

CHAPTER 6

INCIDENT AND EMERGENCY RESPONSE

CHAPTER 6 - INCIDENT AND EMERGENCY RESPONSE

An incident is an event that has the potential to cause harm to personnel, the community, or the environment. The ERP should include procedures to respond in a timely and effective manner to situations that could impact biosecurity of the containment zone, which may include events such as inadvertent or intentional release of pathogens or toxins, natural disasters, workplace violence, bomb threats, security breaches (e.g., unauthorized entry, unauthorized access to sensitive information), and emergencies (e.g., fire, medical emergencies). Examples of possible measures that may be implemented to mitigate biosecurity risks related to incident and emergency response are provided in Table 6-2. Emergency response is discussed in Chapter 17 of the CBH, and further details on incident reporting and investigation can be found in Chapter 18 of the CBH.[1]

6.1 Incident Reporting

The procedures developed to report incidents should comply with applicable regulations, as well as the organization's internal incident reporting and investigation procedures. SOPs for incident reporting and investigation are an integral component of a facility's ERP, and should be developed to complement or align with existing facility-wide programs (e.g., occupational health and safety).

It is a requirement in the CBS that incidents involving pathogens, toxins, other regulated infectious material, infected animals, or failure of **containment systems** or control systems be immediately reported to the appropriate internal authority, and in some cases, to the PHAC (CBS Matrix 4.9).[2] For example, the PHAC is to be notified if there is reason to believe that a pathogen or toxin has been stolen or is otherwise missing.

In particular, the following biosecurity incidents should be reported immediately to the appropriate personnel or authority within the organization:

- any loss or compromise of keys, passwords, combinations, remote access equipment (e.g., laptops, personal computers, and tablets) or other critical security information;
- unauthorized access or attempts to access restricted access areas, such as those with SSBAs, or CL3 or CL4 zones, or areas with sensitive information;
- any suspicious persons or activities;
- any missing equipment with dual-use potential; and
- any discrepancy in the inventory, or indications that the inventory has been tampered with or otherwise compromised.

The facility should identify and document situations for which early involvement of the institutional security service or local law enforcement may be needed.

6.2 Incident Response Planning

Timely, coordinated, and effective responses to specific situations that are serious and unexpected may require an immediate and planned response to reduce the harmful impacts on personnel, the community, and the environment. As such, biosecurity-related incident response plans specifically tailored to the organization, facility, and containment zone can be included in the ERP. Table 6-1 lists five key items for a successful incidence response plan.

Table 6-1: Five keys to a successful incident response plan.

1. It is focused on protecting human life before property.
2. Personnel are trained to respond quickly and effectively to the incident.
3. It is the result of collaboration between facility personnel and first responders.
4. First responders are involved in incident preparedness training.
5. It addresses the immediate danger, and the secondary effects on people who work at the facility.

Depending on the nature of the incident, responses may include evacuation or lockdown of the affected area, notifying first responders, such as law enforcement or emergency services, assessing the severity of the incident (e.g., potential for loss of containment, **exposure**, or release), preventing secondary incidents, and identifying and preserving the chain of evidence. Every incident should be documented including false alarms. While an ERP is included in the Biosafety Manual, the biosecurity aspects need to be described in the incident and emergency response element of the biosecurity plan, or a reference to the ERP included in the plan.

Table 6-2: Possible measures that may be implemented to mitigate biosecurity risks related to incident and emergency response in a CL2, a CL3, and an SSBA area

Biosecurity plan element	Risk	Possible Mitigation Measures		
		CL2	CL3	SSBA area
Incident and Emergency Response	Stolen pathogens are not reported.	• Procedure requiring that personnel investigate any missing pathogen or toxin. • Notification of the BSO if the pathogen or toxin is not found within a reasonable time. • BSO to notify the PHAC or the CFIA of the missing pathogen or toxin.	• Procedure requiring immediate notification of the BSO. • BSO to notify the PHAC or the CFIA of the missing pathogen or toxin without delay. • BSO to investigate any missing pathogen or toxin and to preserve evidence.	• Procedure requiring immediate notification of the BSO. • BSO to notify the PHAC of the missing pathogen or toxin without delay • BSO to investigate any missing pathogen or toxin and to preserve evidence. • BSO to inform law enforcement agency for suspected cases of theft.
	Lost or stolen key or keycard to containment zone is not reported.	• Procedure requires lost or stolen keys to be reported to laboratory supervisor within a reasonable time. • Lock is replaced or rekeyed within a reasonable timeframe.	• Procedure requires lost or stolen keys to be reported immediately to supervisor and security. • Lock is replaced or rekeyed without delay. • Stolen or lost keycard is deactivated upon reporting.	• Procedure requires lost or stolen keys to be reported immediately to supervisor, BSO and security. • Lock is replaced or rekeyed without delay. • Alternative temporary security measures are implemented until lock is replaced/rekeyed (e.g., SSBA moved to another secure location or placed into locked storage equipment). • Stolen or lost keycard is deactivated upon reporting.

6.3 Incident Investigation

Biosecurity incidents may be indicative of failures in biosecurity systems, or a result of human error. The investigation and report are necessary to enable facilities to accurately define the situation, determine why an incident took place (i.e., identify the root cause[s]), if it was intentional or accidental, if it was an isolated event, and to take corrective actions to prevent similar incidents in the future.

Following an incident, it may not be known or be clear if it is a biosecurity incident, and this may be purposefully hidden if the incident is intentional. As such, biosecurity elements should be considered in the all hazards approach to incident investigation so that important evidence is not overlooked. The investigation of any incident should consider the possibility that evidence of intentional acts may be deliberately concealed. Until the evidence shows otherwise, biosecurity factors should not be ruled out. If there is a possibility that the incident was the result of a criminal act, it may be prudent to obtain assistance from law enforcement at the early stages.

The incident investigation process is systematic and generally includes the stages outlined below, which are described in detail in Chapter 18 of the CBH.

- Initial Response;
- Collection of Evidence and Information;
- Analysis and Identification of Root Causes;
- Development of Corrective and Preventative Action Plans; and,
- Evaluation and Continual Improvement.

The investigation of biosecurity-related incidents may already be captured in investigation SOPs for biosafety-related incidents, which are included in the Biosafety Manual, or they can be developed as separate SOPs specific to biosecurity. As with other SOPs, they should be reviewed and updated regularly to ensure they are current and accurate, and an individual responsible for this duty should be selected.

Depending on the nature and severity of the incident, one individual may be assigned to conduct the investigation or a team may be assembled for more complex scenarios. The investigator(s) should conduct the investigation with an open mind and no pre-conceived notions or opinions regarding the incident. The extent and depth of the incident investigation may vary, depending on the severity of the incident.

References

1 Government of Canada. (2016). *Canadian Biosafety Handbook* (2nd ed.). Ottawa, ON, Canada: Government of Canada.

2 Government of Canada. (2015). *Canadian Biosafety Standard* (2nd ed.). Ottawa, ON, Canada: Government of Canada.

CHAPTER 7

INFORMATION MANAGEMENT AND SECURITY

CHAPTER 7 - INFORMATION MANAGEMENT AND SECURITY

An integral element of a biosecurity plan is addressing how information assets related to pathogens and toxins are protected and secured. There are many different types of information possessed by a facility that may be considered to be assets requiring protection against loss, theft, damage, or release. Information security is directed at protecting information – keeping sensitive information confidential (e.g., information about SSBA pathogens and toxins in the facility), maintaining the integrity of all information, and making it accessible only to those who need it.

Information security aims to protect information assets in all formats, whether it is hard-copy, electronic, or knowledge retained by personnel, while allowing authorized access only to those who need it. An information security assessment takes into account who needs access to what information and the methods used to protect the information that are commensurate with the biosecurity risk. Examples of possible measures that may be implemented to mitigate biosecurity risks related to information security are provided in Table 7-1

7.1 Information Assets

Information assets may provide information related to human and animal pathogens, toxins, and other regulated infectious material that needs to be protected. As with other assets, this information needs to be identified and classified according to its value (including criticality and its sensitivity to being compromised or released) through the biosecurity risk assessment process described in Chapter 6 of the CBH.

Knowing what information is to be protected and to what level helps maintain employee awareness about the information they have a responsibility to protect. In terms of biosecurity, information assets may include the following:

- inventories;
- biosafety and biosecurity risk assessments;
- experimental protocols and results;
- proprietary scientific information (e.g., processes, techniques, gene sequences)
- access authorizations and logs;
- building plans;
- personnel records and financial records; and,
- biological material inventories and storage locations.

While it is a requirement of the CBS that a description of the biosecurity plan appear in the Biosafety Manual, the complete detailed biosecurity plan and biosecurity risk assessments may need to be kept confidential as they may contain confidential information (e.g., about security systems, personnel, pathogens, procedures).

7.2 Classifying Information

Classifying information will help determine the level of security required. The following categories are provided as examples only, and organizations may already have a classification system in place or opt to modify the suggested categories. Also note that certain information may be regulated by federal or provincial/territorial privacy laws (e.g., personal information).

- Public – information intended for the general public, upon appropriate approval;
- Internal – information not intended for general population. Examples include data analysis and draft documents circulated to other personnel for review;
- Limited or restricted access – information only intended for authorized individuals. Release of information may negatively impact the organization. Examples may include SOPs and study data; and,
- Confidential – information only intended for a small number of authorized individuals with a need to know. Release of information may compromise facility security or critical containment systems. Examples may include dual-use gain of function research, critical proprietary information, and details of security systems.

Classification of information can vary from one organization to another. How it is accomplished is left to the organization as it will depend on the type of information held. Data deemed restricted by one organization may be considered confidential by another. Information needing higher security can lead to significant costs (e.g., hardware, software, ease of access). The damage resulting from the compromise of information should be weighed against the cost of implementing mitigation strategies.

7.3 Information Security

Effective information security measures should protect electronic and non-electronic forms of information assets from the time of their creation until their transfer, destruction, deletion, or disposal, including while the information is being stored or transferred. Some facilities may prefer to maintain information security as a separate plan, but a description of the information security measures in place is to be included in the biosecurity plan. The success of an information security plan relies heavily on management support. Developing, implementing, and maintaining information security requires resources (personnel, funding) as well as buy-in from all personnel.

In either case, one individual or team should be tasked with information security so that potential threats and security options can be reviewed on a regular basis (e.g., monthly, semi-annually, annually). This includes keeping up-to-date on the latest threats (e.g., social engineering, malware, spam, phishing, hacking) and implementing the most up-to-date countermeasures (e.g., installation of antivirus software and firewalls, notifying personnel of phishing attempts, requiring frequent password changes if there has been a recent security breach or multiple security breaches in the past).

Table 7-1: Possible measures that may be implemented to mitigate biosecurity risks related to information security in a CL2, a CL3, and an SSBA area

Biosecurity plan element	Risk	Possible Mitigation Measures		
		CL2	CL3	SSBA area
Information security	Breach of laboratory data stored on a shared network drive.	• Laboratory information stored on shared network drive is saved in access controlled folders only accessible by laboratory personnel (e.g., via a facility generic user account).	• Access to shared network only possible through individual username and password. • Laboratory information stored on shared network drive is saved in restricted access folders only accessible by authorized personnel.	• Access to shared network requires two-factor authentication (e.g., individual username and password in combination with key, grid card, fingerprint). • Highly sensitive restricted files are encrypted or stored outside of the shared network. • Laboratory information stored on shared network drive is saved in restricted access folders only accessible by authorized personnel who hold a valid HPTA Security Clearance. • Remote access to shared network folders containing SSBA records is blocked • Access and changes to restricted folders are recorded through electronic audit logs.
	Loss of USB flash drive containing laboratory data.	• Policy and procedure limiting the use of USB flash drives.	• Policy and procedure limiting the use of USB flash drives and requiring the use of passwords to protect documents. • Loss must be reported to the BSO.	• Policy and procedure limiting the use of USB flash drives and requiring approval for each use. • Use of encrypted USB flash drives. • Loss must be reported to the BSO and to security.

7.3.1 Policies and Standards

Policies can be developed to govern the identification, classification (e.g., proprietary, confidential, restricted), and handling of sensitive information and address how the information is collected, documented, transmitted, stored, accessed, and destroyed. Policies on internet use and use of removable storage media (e.g., USB flash drives) can provide personnel with clear information on expectations on their use. Good policies are simple and straightforward. For example, remote login (e.g., from home) to the facility network is only to be done using a facility laptop with updated antivirus software, the use of strong passwords is required, and passwords are not to be written down where they are readily accessible. Non-disclosure agreements may be used to prohibit personnel from discussing or releasing proprietary or security sensitive information.

7.3.2 Hardcopy Information

The implementation of a "clear desk" policy requiring staff to file or appropriately secure (i.e., in a locked desk drawer, office filing cabinet, security cabinet, safe, or other secure furniture, as appropriate) sensitive documents, which could include lab notebook, password information, data, and SOPs, will prevent access from unauthorized individuals. Also, developing policies or procedures for situations where personnel need to transport sensitive documents, and on the use of reproduction technology (e.g., copiers, scanners, cameras, mobile phones and devices) will also help protect the information present in hard copy. Sensitive information should be printed at the workstation and removed from the printer immediately after printing, or printed using a lock-print option if a centralized printer is used.

7.3.3 SSBA Information

It is a requirement to restrict access to records and documentation pertaining to controlled activities with RG3 and RG4 human pathogens and SSBA toxins to authorized personnel (CBS Matrix 4.10). This extends to anyone who may have access to electronic information. While personnel accessing or controlling SSBA information, such as IT administrators, do not require an HPTA Security Clearance, facilities should consider implementing a policy so that only those who are authorized have access to the information. Facilities wishing to apply for an HPTA Security Clearance for such individuals on a voluntary basis may submit their applications to the PHAC.

The sensitivity of dual-use applications and information should be considered when presenting SSBA-related research in scientific publications (e.g., cloning procedure to reconstitute an extinct virus); however, such issues are beyond the scope of this guideline.[1]

7.3.4 Security of Electronic Information

IT security refers specifically to the protection of electronic information, such as information stored on personal computers, servers, or removable media, or that which is transferred

electronically. This includes cloud computing, which may necessitate additional security precautions.[2] Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) provides a range of guidance documents, security bulletins, and technical reports related to cyber security issues, including alerts and advisories to communicate information about potential, imminent or actual threats, vulnerabilities or incidents affecting Canada's critical infrastructure.[3]

Depending on the security requirements of the information, it may be acceptable to store the information on a secure network; however, sensitive information is more secure if stored encrypted on a removable medium (e.g., CD-ROM or USB flash drive) or in paper format only, and kept in a secure location that is accessible only to authorized individuals. Such information should never be stored on an open or shared network without proper protection. The location selected to store documents should be accessible only to the authorized individuals who need access (i.e., "need-to-know") as determined by the organization (e.g., BSO, director, supervisor). The storage area should be sufficiently secured to protect against damage or loss of information. Documents containing sensitive information that is obsolete or no longer relevant should be shredded or destroyed in accordance with the security rating of the material designated for destruction.[4]

In addition to the information itself, other aspects of information security need to be considered. Removable media such as USB flash drives are easily misplaced, and laptops can be easy prey for thieves. While the information they contain may be difficult to access by unauthorized individuals, it may still be irreplaceable and its loss can impact the organization (e.g., inventories, list of individuals authorized to access a containment zone).

Commonly used devices that can be easily hidden from sight or are considered innocuous (e.g., smart cellular phones, personal digital assistants [PDAs], USB flash drives, SD memory cards) pose a **vulnerability** to information security. The concern with these devices is their capability to store a large amount of information on minuscule, removable media that can easily be carried out of a facility undetected. In addition, the transfer of files from a home computer to a work computer has the potential to introduce malware. The facility should consider including these types of devices in their information security policies, recognizing that they may be misused, and with a view to mitigate this risk with an appropriate compromise.

The following considerations on the use of electronic information can be used to develop policies or standards.

7.3.4.1 General electronic information security

- Implement a clear monitor policy, to lock the monitor or log off the computer or terminal when it is unattended, to prevent unauthorized individuals from accessing the computer.
- Use of privacy screens for computer or terminal monitor to prevent viewing by colleagues, or outsiders through a window.
- Lock sensitive electronic documents to make them "Read Only" to prevent editing.
- Understand the type of information that can be shared to prevent the inadvertent transfer of such information to unauthorized individuals.

- Implement a policy on the acceptable use of computers, the internet, and installation of software to prevent the inadvertent installation of malicious software, viruses, and spyware.
- Restrict the use of laptop computers and teleworking, for example, avoid the use of unsecured Wi-Fi networks, and only using antivirus-protected devices for remote access to help protect the computer and the local area network (LAN).
- Use methods of secure information transfer, for example, the use of password protected files or encryption via email, or use of fax, to protect against files being sent to the wrong address.
- Locate computers and servers in a secured zone, such as a locked LAN closet or locked computer or server room. Authenticate the user before granting access. Depending on the security requirements, this can be one-factor authentication that requires a username and strong password, or two-factor authentication that also requires the use of a physical object in possession of the user (e.g., key, grid card, USB token), or a physical characteristic of the user (e.g., fingerprint, voice, eye).
- Use secure networks, including reputable bonded third party providers.
- Use a Virtual Private Network (VPN) to communicate between offices or similar, if available.

7.3.4.2 LAN Security

- Implement a policy on passwords (i.e., to create a strong password, protect passwords, and define frequency of change).
- Install a network firewall to protect against spam and malware.
- Regularly update antivirus software to protect against viruses.
- Restrict access to network drives and folders to those who need it to add to the security of sensitive files.

7.3.4.3 The Internet

- Only visit legitimate, trusted websites. While specific websites can be blocked by a firewall, administrators would need to continually add new websites to the list in order for it to be effective.
- Develop policies for use of online storage (e.g., cloud storage) and applications.
- Verify the web page address, or copy and paste the link into the browser search engine, rather than simply clicking on it.
- Use an internet security software package.
- Do not modify or disable security safeguards such as antivirus software.
- Only provide personal or sensitive information to a trusted secure source (e.g., completing a credit card purchase only on the secure vendor's web page).
- Update software as required so that all security fixes and antivirus definitions are up to date.
- Install a firewall.
- Use administrative options to incorporate filters to restrict access to external websites (filtered versus unfiltered access with access granted to authorized personnel only).

7.3.4.4 Email

- Develop policies on email management.
- Install a spam filter.
- Do not click on links from an email.
- Implement strict password standards for all email accounts.
- Do not forward potentially harmful emails to other personnel.
- Keep employees aware of what information they are authorized to send by email.
- If sensitive files are to be sent via email, use encryption.

7.3.4.5 Data

- Back up data to a secure external drive or remote server to avoid potential losses. This also protects from accidental disruptions (e.g., hardware failure). The frequency of the back-up will depend on how often documents are modified.
- Incorporate an automatic back-up feature into software.

7.3.4.6 Remote access

- Ideally, personnel accessing the facility network from a remote location should use a direct connection to the router (i.e., Ethernet cable). If wireless access will be used, only use secure Wi-Fi, and turn on encryption.
- Access to the computer used for remote access should be limited (e.g., children and visitors should not be permitted to use the computer).

7.3.4.7 Mobile phones and devices

- Treat mobile devices and phones with the same security precautions as a desktop or laptop computer.
- Use the system access password option, and leave the device locked when not in use.
- Use the security features on the device, and install anti-malware software if it is available.
- Regularly back up information stored on the device.

7.3.4.8 Data storage devices

- Implement policies on the use and transportation of removable electronic storage devices such as USB flash drives, SD memory cards, and removable hard drives.

7.3.4.9 Cameras and video recording devices

- Implement clear policies on the use of cameras and video recording devices (including smart cellular phones) and the dissemination and publication of such information.

References

1 Tumpey T, Basler C, Aguilar P, Zeng H, Solórzano A, Swayne D, Cox N, Katz J, Taubenberger J, Palese P, García-Sastre A. (2005). Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus. *Science*, 310(5745):77-80.

2 Public Safety Canada. (2013). *Get Cyber Safe Guide for Small and Medium Businesses*. Ottawa, ON, Canada: Public Safety Canada. Retrieved 2/8, 2016 from http://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/

3 Public Safety Canada. (2015). Canadian Cyber Incident Response Centre. Retrieved 2/8, 2016 from http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx

4 Royal Canadian Mounted Police. (2014). *Destruction Equipment Selection - Section 2*. Retrieved 2/8, 2016 from http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/page_0068_e.htm

CHAPTER 8

IMPLEMENTATION, EVALUATION, AND IMPROVEMENT OF THE BIOSECURITY PLAN

CHAPTER 8 - IMPLEMENTATION, EVALUATION, AND IMPROVEMENT OF THE BIOSECURITY PLAN

A biosecurity plan is to be developed, implemented, reviewed and improved as necessary, and kept up to date. Implementation will involve the installation and testing of physical security components, but also the initial training of personnel on security policies and procedures, and ongoing biosecurity awareness.

Evaluating the effectiveness of the biosecurity plan on a routine basis, when changes are made that may affect biosecurity, and in response to biosecurity incidents, will help identify any vulnerabilities and areas for improvement.

8.1 Training

Training is a core element of biosafety and biosecurity, and is essential to the success of the biosafety program. Personnel need to be knowledgeable about the hazards, including any relevant biosecurity threats, associated with the pathogens and toxins present in their work environment, the practices and tools that can prevent accidental exposure to, or release of, pathogens and toxins, and maintain the security of assets. Training can address the particular needs of the individual, the specific work they will do, and the risks posed by the pathogens and toxins handled or stored in the facility. Biosafety training is described in Chapter 8 of the CBH.

Before an individual has been granted access to pathogens and toxins, it is important that the individual understands and follows all the biosecurity protocols (including information security) established by the facility. Biosecurity elements should be incorporated into the existing training program and be delivered to all individuals authorized to access a containment zone. It is recommended that biosecurity training include modules on specific security processes and procedures that control access and prevent the loss, theft, or compromise of pathogens, toxins, and other assets. Refresher training should be offered at a frequency determined by the training needs assessment or when changes to the processes and procedures are implemented.

8.1.1 Biosecurity Awareness

Biosecurity awareness training for personnel provides employees with a clear understanding of roles and responsibilities and establishes clear expectations regarding ways to protect the assets within the facility. This training is an important component of the ongoing reliability assessment program serving to detect and deter other internal and external threats. Biosecurity awareness should:

- provide staff with training to recognize, understand potential implications, and report suspicious activity, such as:
  - use of false identification;

- suspicious behaviour;
- lost or stolen keys, keycards, or material;
- unsafe behaviour;

- outline the organization's policies and procedures to protect sensitive information;
- include training on techniques and indicators to identify suspicious activity and behavioural changes in personnel or visitors;
- inform personnel of the consequences of inappropriate conduct; and
- provide instruction on security practices and procedures, and on reporting suspicious events and security incidents.

Recommended topics for biosecurity awareness refresher training include:[1]

- identifying suspicious persons and response (i.e., reporting, removal);
- recognizing insider threats;
- accompaniment and supervision procedures;
- refresher training on emergency response procedure (CBS Matrix 4.3); and
- review of incident reports within the institution or incidents published in the press, in order to conduct lessons learned.

Ongoing biosecurity awareness activities can inform personnel of recent threats, such as attempts at unauthorized access, or about a new computer virus, while providing a reminder of their responsibilities.

8.1.1.1 Social engineering

Social engineering is often just one of many steps in a complex fraud. Criminals use social engineering to gain information (e.g., personal information, passwords) that can be used to access assets or confidential information. It is used because it is effective. Training should inform personnel to:

- be suspicious of an individual asking about personnel, their families, or sensitive information;
- require the identity of anyone making unusual inquiries to be verified; and
- report any suspicious activity to management.

8.1.1.2 Information Security Awareness

A security awareness program will keep personnel informed about the facility security practices, policies, and standards. Information security should be included in training, but information security awareness requires more than just training. While the topic of information security can be introduced at a basic level in initial security awareness training, it should be

expanded upon over time to include more in depth training. Personnel should receive regular updates and reminders to maintain awareness, and for increased awareness when warranted.

8.2 Maintenance and Testing of Security Systems

It is essential that any equipment and procedures related to maintaining a physical security barrier, including the physical barrier itself, be inspected on a regular basis to verify it is performing its function effectively. All access control systems, intrusion detection systems, and locking devices should be installed, operated, and maintained in accordance with the manufacturer's specifications. The performance of intrusion detection devices should be verified on a regular basis (e.g., monthly, semi-annually, annually), based on a risk assessment, to confirm their continued effective operation, and a record of these performance tests should be kept on file. Verification of electronic systems should also be performed during a power failure, or the emergency protocol for such a situation reviewed.

8.3 Evaluation and Continual Improvement of the Biosecurity Plan

The biosecurity plan should be regularly reviewed and continually improved by the individual with delegated authority over biosecurity to verify that it remains relevant, applicable, and effective. The review period will depend on biosecurity risks. For example, for lower containment (i.e., CL2), the review may simply be confirmation that the biosecurity risk remains unchanged (e.g., there has been no change to the pathogens and toxins being handled or stored), and that no biosecurity-related incidents have occurred during the review period, where an in-depth biosecurity plan review is required every time the biosecurity risk assessment is reviewed. In addition, the biosecurity plan should be reviewed following any incident, and updated based on the root causes identified.

Senior management may also review the biosecurity plan at regular intervals to confirm that the existing plan meets the needs of the institution or organization and continues to reflect the long-term goals and objectives.

The review will help address broad questions related to biosecurity, such as:

- Does the current plan meet the needs of the facility?
- Are all six biosecurity elements appropriately addressed?
- Are all of the appropriate biosecurity procedures and processes in place?
- Is the personnel adequately trained in biosecurity?
- Does the plan need to be updated (e.g., in response to change or events)?
- Are adequate resources available to maintain biosecurity?

Any biosecurity issues identified during the review may need to be addressed by updating the plan or implementing new procedures.

References

1 United States Centers for Disease Control and Prevention and Division of Select Agents and Toxins and Animal and Plant Health Inspection Service Agricultures Select Agent Program. (2013). *Security Guidance for Select Agent or Toxin Facilities* (2nd Revision). Retrieved 2/8, 2016 from http://www.selectagents.gov/resources/Security_Guidance_v3-English.pdf

CHAPTER 9

GLOSSARY

CHAPTER 9 - GLOSSARY

It is important to note that while some of the definitions provided in the glossary are universally accepted, many of them were developed specifically for the CBS, the CBH, or the *Canadian Biosafety Guideline: Developing a Comprehensive Biosecurity Plan*; therefore, some definitions may not be applicable to facilities that fall outside of the scope of the CBS.

Accident	An unplanned event that results in injury, harm, or damage.
Animal pathogen	Any pathogen that causes disease in animals; including those derived from biotechnology. In the context of the *Canadian Biosafety Standard*, the *Canadian Biosafety Handbook,* and the *Canadian Biosafety Guidelines,* "animal pathogen" refers only to pathogens that cause disease in terrestrial animals; including those that infect avian and amphibian animals, but excluding those that cause disease in aquatic animals and invertebrates.
Animal room	A room designed to house animals in primary containment caging. These spaces are used to house only small-sized animals (e.g., mice, rats, rabbits).
Assets	All of the pathogens, infectious material, and toxins in the possession of a facility. Other assets include materials, equipment, non-infectious material, animals, knowledge and information (e.g., protocols, research findings), and personnel in a facility.
Authorized personnel	Individuals who have been granted unsupervised access to the containment zone by the containment zone director, biological safety officer, or another individual to whom this responsibility has been assigned. This is dependent on completing training requirements and demonstrating proficiency in the standard operating procedures, as determined to be necessary by the facility.
Biological material	Pathogenic and non-pathogenic microorganisms, proteins, and nucleic acids, as well as any biological matter that may contain microorganisms, proteins, nucleic acids, or parts thereof. Examples include, but are not limited to, bacteria, viruses, fungi, prions, toxins, genetically modified organisms, nucleic acids, tissue samples, diagnostic specimens, live vaccines, and isolates of a pathogen (e.g., pure culture, suspension, purified spores).
Biological safety officer (BSO)	An individual designated for overseeing the facility's biosafety and biosecurity practices.
Biosafety	Containment principles, technologies, and practices that are implemented to prevent unintentional exposure to infectious material and toxins, or their accidental release.
Biosafety Manual	A facility-specific manual that describes the core elements of a biosafety program (e.g., biosecurity plan, training, personal protective equipment).

Biosecurity	Security measures designed to prevent the loss, theft, misuse, diversion, or intentional release of pathogens, toxins, and other related assets (e.g., personnel, equipment, non-infectious material, and animals).
Biosecurity risk assessment	A risk assessment in which the pathogens, toxins, infectious material, and other related assets (e.g., equipment, animals, information) in possession are identified and prioritized, threats and vulnerabilities are identified and defined, and appropriate mitigation strategies are determined to protect these materials against potential theft, misuse, diversion, or intentional release.
Community	Encompasses both human (i.e., the public) and animal populations.
Containment	The combination of physical design parameters and operational practices that protect personnel, the immediate work environment, and the community from exposure to biological material. The term "biocontainment" is also used in this context.
Containment level (CL)	Minimum physical containment and operational practice requirements for handling infectious material or toxins safely in laboratory, large scale production, and animal work environments. There are four containment levels ranging from a basic laboratory (containment level 1 [CL1]) to the highest level of containment (containment level 4 [CL4]).
Containment system	Dedicated equipment that functions to provide and maintain containment. This includes, but is not limited to, primary containment devices (e.g., biological safety cabinets), heating, ventilation, and air conditioning (HVAC) and control systems, and decontamination systems (e.g., autoclaves).
Containment zone	A physical area that meets the requirements for a specified containment level. A containment zone can be a single room (e.g., containment level 2 [CL2] laboratory), a series of co-located rooms (e.g., several non-adjoining but lockable CL2 laboratory work areas), or it can be comprised of several adjoining rooms (e.g., containment level 3 [CL3] suite with dedicated laboratory areas and separate animal rooms, or animal cubicles). Dedicated support areas, including anterooms (with showers and "clean" and "dirty" change areas, where required), are considered to be part of the containment zone.
Controlled access system	A physical or electronic system designed to restrict access to authorized personnel only.

Controlled activities	Any of the following activities referred to in Section 7(1) of the *Human Pathogens and Toxins Act*: possessing, handling or using a human pathogen or toxin; producing a human pathogen or toxin; storing a human pathogen or toxin; permitting any person access to a human pathogen or toxin; transferring a human pathogen or toxin; importing or exporting a human pathogen or toxin; releasing or otherwise abandoning a human pathogen or toxin; or disposing of a human pathogen or toxin.
Disease	A disorder of structure or function in a living human or animal, or one of its parts, resulting from infection or intoxication. It is typically manifested by distinguishing signs and symptoms.
Dual-use potential	Qualities of a pathogen or toxin that allow it to be either used for legitimate scientific applications (e.g., commercial, medical, or research purposes), or intentionally misused as a biological weapon to cause disease (e.g., bioterrorism).
Emergency Response Plan (ERP)	A document outlining the actions to be taken and the parties responsible in emergency situations such as a spill, exposure, release of infectious material or toxins, animal escape, personnel injury or illness, power failure, fire, explosion, or other emergency situations (e.g., flood, earthquake, hurricane).
Exporting	The activity of shipping (e.g., transferring or transporting) pathogens, toxins, or other regulated infectious material from Canada to another country.
Exposure	Contact with, or close proximity to, infectious material or toxins that may result in infection or intoxication, respectively. Routes of exposure include inhalation, ingestion, inoculation, and absorption.
Facility (plural: facilities)	Structures or buildings, or defined areas within structures or buildings, where infectious material or toxins are handled or stored. This could include individual research and diagnostic laboratories, large scale production areas, or animal housing zones. A facility could also be a suite or building containing more than one of these areas.
Handling or storing	"Handling or storing" pathogens, toxins, or infectious material includes possessing, handling, using, producing, storing, permitting access to, transferring, importing, exporting, releasing, disposing of, or abandoning such material. This includes all controlled activities involving human pathogens and toxins specified in Section 7(1) of the *Human Pathogens and Toxins Act*.
Human Pathogens and Toxins Act Security Clearance (HPTA Security Clearance)	An authorization following verification of an individual's background and reliability status issued by the Public Health Agency of Canada under Section 34 of the *Human Pathogens and Toxins Act.*

Importing	The activity of bringing (e.g., transferring or transporting) pathogens, toxins, or other regulated infectious material into Canada from another country.
Incident	An event or occurrence with the potential of causing injury, harm, infection, intoxication, disease, or damage. Incidents can involve infectious material, infected animals, or toxins, including a spill, exposure, release of infectious material or toxins, animal escape, personnel injury or illness, missing infectious material or toxins, unauthorized entry into the containment zone, power failure, fire, explosion, flood, or other crisis situations (e.g., earthquake, hurricane). Incidents include accidents and near misses.
Infectious material	Any isolate of a pathogen or any biological material that contains human or animal pathogens and, therefore, poses a risk to human or animal health.
Insider threat	An authorized individual with access to secured assets, containment zones, or facilities as part of his/ her job that may pose a biosecurity risk.
Intoxication	A substance-induced disorder or disease resulting in a symptomatic or asymptomatic condition or other physiological change resulting from an exposure (i.e., ingestion, inhalation, inoculation, or absorption) to a toxin produced by or isolated from a microorganism. This includes a similar response from exposure to a synthetically produced microbial toxin.
Inventory	A list of (biological) assets associated with a containment zone identifying pathogens, toxins, and infectious material in storage both inside and outside of the containment zone.
Laboratory	An area within a facility or the facility itself where biological material is handled for scientific or medical purposes.
Laboratory acquired infection/intoxication (LAI)	Infection or intoxication resulting from exposure to infectious material, infected animals, or toxins being handled or stored in the containment zone.
Laboratory work area	Area inside a containment zone designed and equipped for *in vitro* research, diagnostics, and teaching purposes.
Licence	An authorization to conduct one or more controlled activities with human pathogens or toxins issued by the Public Health Agency of Canada under Section 18 of the *Human Pathogens and Toxins Act*.
Limited access	Access that is only permitted to authorized personnel and other authorized visitors through either operational means (e.g., having authorized personnel actively monitor and check all individuals entering a designated area) or through the use of a physical barrier (e.g., a controlled access system, such as, key-locks or electronic access card).

Local risk assessment (LRA)	Site-specific risk assessment used to identify hazards based on the infectious material or toxins in use and the activities being performed. This analysis provides risk mitigation and risk management strategies to be incorporated into the physical containment design and operational practices of the facility.
Long-term storage	In the context of the *Canadian Biosafety Standard*, the *Canadian Biosafety Handbook,* and the *Canadian Biosafety Guidelines*, the possession of material (i.e., pathogens, toxins, and other regulated infectious material) beyond 30 days of receipt or creation.
Movement	The action of moving (e.g., bringing, carrying, leading, relocating) people, material (including infectious material or toxins), or animals from one physical location to another physical location in the same building. This can include movement within the same containment zone, to a different containment zone, or to another location within the same building.
Operational practice requirements	Administrative controls and procedures followed in a containment zone to protect personnel, the environment, and ultimately the community from infectious material or toxins, as outlined in Chapter 4 of the *Canadian Biosafety Standard*.
Outsider threat	An individual without authorization or access to secured assets, containment zones, or facilities who may not have a formal relationship with the facility and may pose a biosecurity risk.
Pass-through chamber	Interlocked double-door compartments situated on a containment barrier that allow the safe transfer of materials into and out of containment zones.
Pathogen	A microorganism, nucleic acid, or protein capable of causing disease or infection in humans or animals. Examples of human pathogens are listed in Schedules 2 to 4 and in Part 2 of Schedule 5 of the *Human Pathogens and Toxins Act* but these are not exhaustive lists. Examples of animal pathogens can be found through the Automated Import Reference System on the Canadian Food Inspection Agency website.
Pathogenicity	The ability of a pathogen to cause disease in a human or animal host.
Release	The discharge of infectious material or toxins from a containment system.
Restricted access	Access that is strictly controlled to authorized personnel only by means of a physical barrier (i.e., a controlled access device or system, such as an electronic access card, access code, etc.).
Risk	The probability of an undesirable event (e.g., accident, incident, breach of containment) occurring and the consequences of that event.

Risk group (RG)	The classification of biological material based on its inherent characteristics, including pathogenicity, virulence, risk of spread, and availability of effective prophylactic or therapeutic treatments, that describes the risk to the health of individuals and the public as well as the health of animals and the animal population.
Scientific research	As defined in Section 1 of the *Human Pathogens and Toxins Regulations*: the following types of systematic investigation or research that are carried out in a field of science or technology by means of controlled activities: a. basic research, when the controlled activities are conducted for the advancement of scientific knowledge without a specific practical application; b. applied research, when the controlled activities are conducted for the advancement of scientific knowledge with a specific practical application; c. experimental development, when the controlled activities are conducted to achieve scientific or technological advancement for the purpose of creating new or improving existing materials, products, processes, or devices.
Security barrier	A physical obstruction designed to prevent access to pathogens, infectious material, toxins, or other related assets by unauthorized personnel (e.g., locked doors, controlled access systems, or padlocked storage equipment) that increases the security of a containment zone by restricting access to authorized personnel only.
Security sensitive biological agents (SSBAs)	The subset of human pathogens and toxins that have been determined to pose an increased biosecurity risk due to their potential for use as a biological weapon. SSBAs are identified as prescribed human pathogens and toxins by Section 10 of the *Human Pathogens and Toxins Regulations*. This means all Risk Group 3 and Risk Group 4 human pathogens that are in the *List of Human and Animal Pathogens for Export Control*, published by the Australia Group, as amended from time to time, with the exception of Duvenhage virus, Rabies virus and all other members of the Lyssavirus genus, Vesicular stomatitis virus, and Lymphocytic Choriomeningitis Virus; as well as all toxins listed in Schedule 1 of the *Human Pathogens and Toxins Act* that are listed on the *List of Human and Animal Pathogens for Export Control* when in a quantity greater than that specified in Section 10(2) of the *Human Pathogens and Toxins Regulations*.
Senior management	The ultimate authority responsible for delegating appropriate biosafety authority. Senior management is responsible for ensuring that adequate resources are available to support the biosafety program, to meet legal requirements, and that biosafety concerns are appropriately prioritized and addressed.

Standard operating procedure (SOP)	A document that standardizes safe work practices and procedures for activities with infectious material and toxins in a containment zone, as determined by a local risk assessment.
Tailgating	Gaining unauthorized access to a controlled access area by following an authorized person across the access point with or without their consent.
(Microbial) Toxin	A poisonous substance that is produced or derived from a microorganism and can lead to adverse health effects in humans or animals. Human toxins are listed in Schedule 1 and Part 1 of Schedule 5 in the *Human Pathogens and Toxins Act.*
Transfer	A change in possession of pathogens, toxins, or other regulated infectious material between individuals from the same or different facilities (i.e., the movement or transportation from the place or places specified in the licence or animal pathogen import permit to any other place).
Transportation	The act of transporting (e.g., shipping or conveyance) infectious material or toxins to another building or location (i.e., different address), within Canada or abroad, in accordance with the *Transportation of Dangerous Goods Act* and *Regulations*.
Trigger quantity	The minimum quantity above which a toxin regulated by the *Human Pathogens and Toxins Act* is considered a "prescribed toxin" and, therefore, a security sensitive biological agent, as described by Section 10(2) of the *Human Pathogens and Toxins Regulations*.
Vulnerability	A component of a biosecurity risk assessment that identifies weaknesses in a facility's physical security barriers, operational practices (e.g., biosecurity training), personnel security, transport security, information security, and program management.

CHAPTER 10

RESOURCES

CHAPTER 10 - RESOURCES

10.1 General Resources

CEN Workshop 55 – CEN Workshop Agreement (CWA) 16393:2012, *Laboratory biorisk management – Guidelines for the implementation of CWA 15793:2008.* (2012). Brussels, Belgium: European Committee for Standardization.

Fennelly, L. (2013). *Effective Physical Security* (4th ed.). Waltham, MA, USA: Elsevier Inc.

Government of Canada. (2015). *Canadian Biosafety Standard* (2nd ed.). Ottawa, ON, Canada: Government of Canada.

Government of Canada. (2016). *Canadian Biosafety Handbook* (2nd ed). Ottawa, ON, Canada: Government of Canada.

Government of Canada (2012). *Guide to Integrated Risk Management: A recommended approach for developing a Corporate Risk Profile.* Retrieved 2/9, 2016 from https://www.tbs-sct.gc.ca/tbs-sct/rm-gr/guides/girm-ggir01-eng.asp

ISO 9001:2008, Quality Management Systems - Requirements. (2008). Geneva, Switzerland: International Organization for Standardization.

Public Safety Canada. *Cyber Security Technical Advice and Guideline*. Retrieved 2/8, 2016 from http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/tchncl-dvc-gdnc-eng.aspx

Public Safety Canada. (2013). *Get Cyber Safe Guide for Small and Medium Businesses*. Retrieved 2/8, 2016 from http://www.getcybersafe.gc.ca/cnt/rsrcs/pblctns/smll-bsnss-gd/index-eng.aspx

Public Safety Canada. (2015). Canadian Cyber Incident Response Centre. Retrieved 2/8, 2016 from http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-eng.aspx

Royal Canadian Mounted Police. (2014). *Destruction Equipment Selection - Section 2*. Retrieved 2/8, 2016 from http://www.rcmp-grc.gc.ca/physec-secmat/res-lim/pubs/seg/html/page_0068_e.htm

Salerno, R. M., & J. Gaudioso. (2007). *Laboratory Biosecurity Handbook*. Boca Raton, FL, USA: CRC Press.

Tumpey T, Basler C, Aguilar P, Zeng H, Solórzano A, Swayne D, Cox N, Katz J, Taubenberger J, Palese P, García-Sastre A. (2005). Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus. *Science*, 310(5745):77-80.

United States Centers for Disease Control and Prevention Division of Select Agents and Toxins and Animal and Plant Health Inspection Service Agricultures Select Agent Program.

(2013). *Security Guidance for Select Agent or Toxin Facilities* (2nd Revision). Retrieved 2/8, 2016 from http://www.selectagents.gov/resources/Security_Guidance_v3-English.pdf

United States Geological Survey, United States Department of Interior. (2005). *Physical Security Handbook, 440-2-H*. Retrieved 15/03, 2016 from http://www.usgs.gov/usgs-manual/handbook/hb/440-2-h/440-2-h.html

United States National Institutes of Health, National Science Advisory Board for Biosecurity. (2011). *Guidance for Enhancing Personnel Reliability and Strengthening the Culture of Responsibility*. Retrieved 2/8, 2016 from http://osp.od.nih.gov/sites/default/files/resources/CRWG_Report_final.pdf

10.2 Government of Canada Legislation

Health of Animals Act (S.C. 1990, c. 21). (2015).

Health of Animals Regulations (C.R.C., c. 296). (2015).

Human Pathogens and Toxins Act (S.C. 2009, c. 24). (2015).

Human Pathogens and Toxins Regulations (SOR/2015-44). (2015).

Transportation of Dangerous Goods Act, 1992 (S.C. 1992, c. 34). (2015).

Transportation of Dangerous Goods Regulations (SOR/2001-286). (2015).