sipri

# HANDBOOK OF APPLIED BIOSECURITY FOR LIFE SCIENCE LABORATORIES

PETER CLEVESTIG

## STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE

Stockholm International Peace Research Institute (SIPRI) is an independent international institute for research into problems of peace and conflict, especially those of arms control and disarmament. SIPRI was established in 1966 to commemorate 150 years of unbroken peace in Sweden.

## GOVERNING BOARD

Ambassador Rolf Ekéus, Chairman (Sweden)
Dr Alexei G. Arbatov (Russia)
Ambassador Lakhdar Brahimi (Algeria)
Jayantha Dhanapala (Sri Lanka)
Dr Nabil Elaraby (Egypt)
Professor Mary Kaldor (United Kingdom)
Ambassador Wolfgang Ischinger (Germany)
The Director

## DIRECTOR

Dr Bates Gill (United States)


**STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE**
Signalistgatan 9
SE-169 70 Solna, Sweden
Telephone: +46 8 655 97 00
Fax: +46 8 655 97 33
Email: sipri@sipri.org
Internet: www.sipri.org

# HANDBOOK OF APPLIED BIOSECURITY FOR LIFE SCIENCE LABORATORIES

PETER CLEVESTIG


STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE

2009

© SIPRI 2009

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, without the prior permission in writing of SIPRI or as expressly permitted by law.

All photographs are courtesy of the Swedish Institute for Infectious Disease Control (Smittskyddsinstitutet, SMI): pp. 3, 7, 18, 21, 23 © SMI/Karl-Erik Sundqvist; p. 5 © SMI/Marianne Lebbad; p. 6 © SMI press archive; pp. 9, 11, 14, 17, 19 © SIPRI.

Printed in Sweden by Elanders

ISBN 978–91–85114–61–0

## CONTENTS

## PREFACE

Biosecurity aims to minimize the risk of theft, loss, intentional exposures and releases of pathogens or toxins. While biosafety is already well established in the research community to protect the environment and workplace, awareness of how the life sciences can be maliciously misused is not as widespread. The anonymous mailing of anthrax spores to politicians and members of the media through the US post in 2001 focused attention on how access to advanced scientific facilities can be abused.

This handbook is a timely and important contribution. It presents the basic components of applied biosecurity that are relevant to all laboratory employees. It fills a gap while governments and various international institutions continue to develop measures to raise barriers against possible bioterrorism.

The author, Dr Peter Clevestig of the SIPRI Arms Control and Non-proliferation Programme, is a virologist whose work in the laboratories of Karolinska Institute (KI), Stockholm, and with its Biosafety Committee make him ideally suited to write on this topic. I thank him for his professional and timely work.

On behalf of SIPRI, I thank the Swedish Civil Contingencies Agency (MSB, formerly the Swedish Emergency Management Agency, KBM), which kindly provided the financial support for the work that resulted in this publication. I would also like to thank Dr Marika Hellqvist Greberg and Dr Jan Byman, the research coordinators of this initiative. Thanks are also due to Dr Åsa Szekely Björndal, institutional biosafety officer at the Swedish Institute for Infectious Disease Control (SMI); Dr Britta Häggström and Dr Åke Forsberg of the Swedish Defence Research Agency (FOI); Professor Roland Möllby, chairman of the Karolinska Institute Biosafely Committee; Frida Kuhlau of the Centre for Research Ethics & Bioethics, Uppsala University; Dr Ian Anthony, SIPRI's Research Coordinator; and John Hart, Head of SIPRI's Chemical and Biological Security Project, for their support and expert advice. I also thank Jetta Gilligan Borg and Joey Fox for the editing.

Dr Bates Gill
Director, SIPRI
June 2009

## 1. THE PURPOSE OF THIS HANDBOOK

***Biosecurity or applied biosecurity refers to the principles, technologies and practices that are implemented to secure pathogens, toxins and sensitive technologies from unauthorized access, loss, theft, misuse, diversion or intentional release***[1]

This handbook is primarily for personnel who work with infectious pathogens and toxins that may affect the health of humans, animals and plants. Such work may be carried out in the public sector (at universities, medical or veterinary schools, and in public health laboratories) or in the private sector (in the biotechnological and pharmaceutical industries). The handbook aims:

- to engage scientists, laboratory employees and students in laboratory biosecurity, and
- to provide practical advice that will ensure the secure handling, management and storage of biological materials.

The regulations that govern work with infectious agents relate mainly to personnel safety. They are commonly integrated into national laws that cover the work environment and occupational health.[2] Security issues related to laboratory work involving infectious agents have often been overlooked unless they have coincided with biosafety. A number of international guidelines, best practices and codes of conduct have recently been published that together provide a framework for international standardization and implementation of biosecurity.[3] However, little documentation is available on applied biosecurity for the laboratory employee. The European Union (EU) is developing new directives to address biosecurity and security issues related to activities with infectious pathogens and toxins. Sometime after 2010 these directives will serve as the basis for national legislation to oversee laboratories. This handbook aims to facilitate the transition to such legislation by encouraging scientists, laboratory staff, students and management to acknowledge security as an important component of laboratory work.

Biosecurity requires that each employee understands that any activity related to infectious pathogens and toxins also involves an inherent security risk: the individual employee is both the most important asset and potential liability. Acknowledging biosecurity risks and the important role of the employee is crucial to keeping the workplace safe and secure. Safeguarding infectious agents is also a national legal obligation under the 1972 Biological and Toxin Weapons Convention (BTWC) and United Nations Security Council Resolution 1540.[4]

Section 2 of this handbook introduces the basic components of laboratory biosecurity that are relevant to all laboratory employees. Section 3 is primarily intended for laboratory managers and principal investigators in positions of authority, with responsibility for staff and their roles in the laboratory. It focuses on their role in safeguarding laboratory assets, including human resources. The glossary presents definitions of selected terms used in this handbook.

## 2. THE COMPONENTS OF APPLIED BIOSECURITY

### 2.1. What is applied biosecurity?

Biosecurity covers a broad spectrum of potential risks and threats ranging from criminal activities, such as sabotage and isolated acts of aggression, to bioterrorism and espionage. The term 'biosecurity' has been used in discussions of the risks associated with dual uses of the life sciences, where legitimate research may have malicious applications and implications beyond its intended use. The term is also used to describe environmental risks in the areas of agriculture and food safety. Discussions of the effect on biodiversity of the introduction and release of genetically modified organisms or foreign invasive species use the term as well.[5]

This handbook focuses on laboratory-related activities. Here laboratory biosecurity describes the principles, technologies and practices that are implemented to secure pathogens, toxins and sensitive information technology from unauthorized access, loss, theft, misuse, diversion or intentional release.

The objective of laboratory biosecurity is to safeguard materials, employees, information and other laboratory assets. This is true regardless of whether the laboratory's activities relate to research, diagnostics, the production of pharmaceuticals or to other life science areas. Applied biosecurity addresses laboratory risks and threats that fall outside the realm of accidental exposure or release. It builds on and shares many components with biosafety practices (figure 1).

*View into the decontamination chamber of a BSL4 laboratory*

Laboratory biosecurity risks can be effectively minimized by identifying assets, such as biological materials, sensitive data and equipment; ensuring that these assets are secure and accounted for at all times; and by adopting an awareness of security. Such an approach benefits the laboratory staff and assures the general public that biological materials and the activities related to them are both safe and secure.

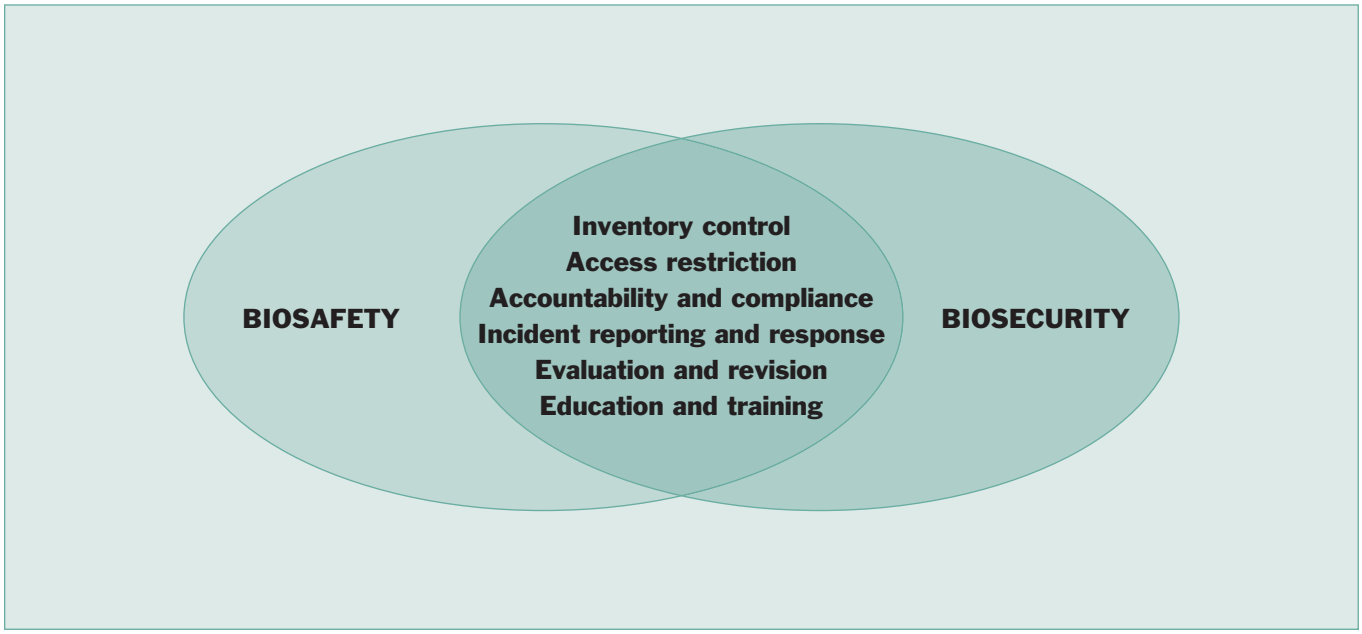



**Figure 1.** The relationship between biosafety and biosecurity

Biosafety and biosecurity are both different approaches to ensure containment, and they both share an end goal of minimizing the risk of accidental or intentional exposures and releases of pathogens or toxins. They also share a number of elements such as inventory control, access restriction, accountability and compliance, incident reporting, evaluation and revision, and education and training.

### 2.2. Biosecurity risk assessment

Risk assessment can evaluate the threat posed by any laboratory activity. Risk is relative to the probability that an event will occur and the consequences of its occurrence (see figure 2).[6] Work with any pathogen or toxin carries biosafety risks, but the severity of the harm that a pathogen or toxin may cause varies. Appropriate biosafety procedures aim to keep risks at a safe level. Such biosafety procedures include good laboratory practice and the use of safety equipment and procedures, including safety cabinets, personal protective equipment and good post-work decontamination techniques.[7] Some countries use work environment regulations to decrease the risk of work with pathogens and toxins.[8]

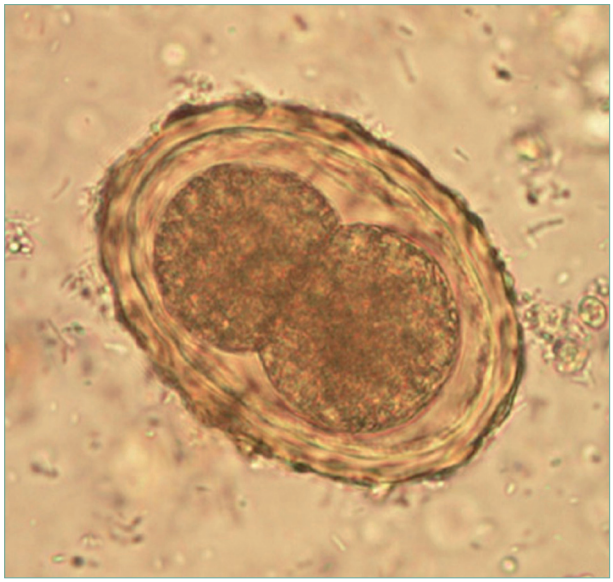
In addition to the risks of accidental exposure and laboratory-acquired infections (biosafety risks), working with infectious pathogens and toxins carries a biosecurity risk. Infectious pathogens and toxins can be stolen, lost or used for malicious purposes by intentionally exposing co-workers to them or carrying out acts of sabotage or bioterrorism (see cases 1 and 2). Biosecurity risks are difficult to identify because they are potential and dynamic, not concrete, and are posed by an individual who is interested in attaining laboratory materials, disrupting laboratory activities or endangering those who work there.[9]

| NATURAL | ACCIDENTAL | INTENTIONAL |
|---|---|---|
| Outbreaks | Laboratory acquired infections | Sabotage |
| Epidemics | Containment failures | Biocrimes |
| Pandemics | Negligence | Bioterrorism |

**Figure 2.** The spectrum of biological risks and their causes

Although many of the pathogens that are studied by scientists are readily available in nature, natural pathogens with the characteristics needed to inflict harm on human, animal or plant populations are rare. (Exceptions are those that occur during local outbreaks or epidemics). Thus, individuals who wish to acquire materials and knowledge may seek them from facilities where a large variety of pathogens and toxins with specific traits are located and stored, perhaps in abundance.

Patient material (e.g. blood and tissue samples) stored at hospitals or diagnostic laboratories is another identifiable source of potentially dangerous pathogens. Diagnostic laboratories commonly do not store the materials that they receive for processing. Nonetheless, such facilities may need to revise and increase the safety of their procedures for the disposal of spent materials and associated information.



*Ascaris egg*

The consequences of the malicious use of a pathogen or toxin primarily depend on its specific characteristics and ability to affect health, but the economic and psychological effects are also significant considerations. It is therefore also important to pay attention to the more benign pathogens. While they may not cause death, they have the capacity to cause economic damage and create harm and discomfort. This was illustrated in 1984 when the Rajneeshee cult used *Salmonella enterica typhimurium* to poison people in Oregon in the United States.[10] It is imperative that all infectious biological materials are handled safely and securely, using standardized procedures.

The suitability of a pathogen or toxin for malicious purposes determines its biosecurity risk. The assessment of such a risk must be broad in order to take into account potential adversaries and their capabilities as well as the vulnerabilities of a specific facility. A scenario-driven (risk-based) approach can successfully assess the risk by identifying weaknesses in existing and planned biosecurity measures. Resources can then be focused on appropriate security measures.

Assessing and managing biosecurity risks is primarily the responsibility of facility management. Laboratory managers or principal investigators can

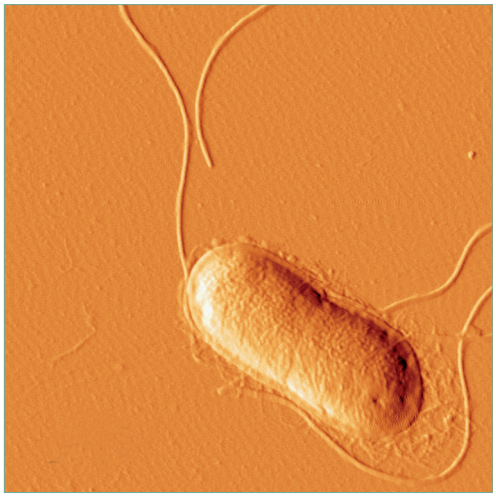
**Case 1.** Employee intentionally infects co-workers

In 1996 a laboratory technician at St Paul's Medical Center in Dallas, Texas, USA, laced pastries with *Shigella dysenteriae* type 2, causing 12 of her co-workers to become ill. Premeditation was apparent: she had sent an email to her colleagues saying that pastries were available in the coffee room.

**Case 2.** Student deliberately infects room-mates

In 1970 a postgraduate student of parasitology at the Macdonald campus of McGill University near Montreal, Canada, contaminated his room-mates' food with stolen *Ascaris suum* eggs. Two of the four room-mates developed acute respiratory failure before parasitic worms were identified as the cause. Prior to the incident, there had been numerous disputes about the rent for the apartment where the student lived with his room-mates.

*Source*: Carus, S. W., 'Bioterrorism and biocrimes: the illicit use of biological agents since 1900', Working paper, Center for Counterproliferation Research, National Defence University, Washington, DC, Feb. 2001, pp. 43–45, 61.



*A salmonella bacterium*

assist in making risk assessments, but these should be coordinated and handled by an appointed facility biosafety and biosecurity officer. An inventory must be made of all viable pathogens and active toxins within a facility under the coordination of management. In some cases such an inventory will already have been created to meet biosafety regulations or best practices. Management must coordinate the assessments and identify any potential threat to a facility in consultation with law enforcement and security specialists.

The laboratory manager and the principal investigator possess the knowledge and expertise to assess the pathogens and toxins present at a laboratory. In making their assessment, they may choose to use existing biosafety level (BSL) or risk group classifications.[11] A risk assessment provides the basis for setting up a 'tailored' biosecurity programme to addresses the security concerns that it identifies.[12]

## 2.3. Applied biosecurity in practice

Implementing biosecurity encompasses many aspects of laboratory activities and resources. It aims to ensure the integrity and security of all pathogens, toxins and sensitive information. Applied biosecurity has a number of key components:

- employee accountability;
- material control;
- development of standard operating procedures;
- compliance with biosecurity procedures;
- physical security;
- access control;
- information security;
- transport security;
- proper routines for security-incident reporting and response;
- maintaining continuous evaluation and revision; and
- providing training and education.[13]

### *2.3.1. Employee accountability*

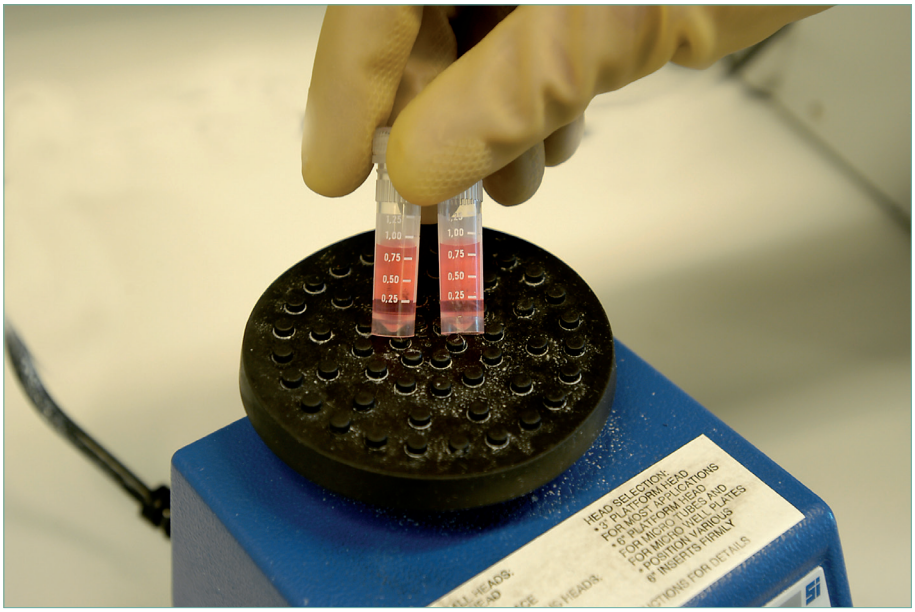
Responsibility for biosecurity is shared by the employer and the employee. However, the facility director or head of department has the ultimate responsibility and accountability for the materials, equipment and information at a facility, the activities performed within it and the actions of the staff. It is difficult for one employee to have complete overview of all activities, and thus responsibilities are commonly delegated to laboratory managers and principal investigators. In turn, they can designate employees with proper qualifications and authorization to oversee specific agents or all agents in one laboratory. These employees must:

- oversee and manage infectious pathogens, toxins, sensitive information and equipment;
- ensure that these are accounted for at all times; and
- conduct record keeping, auditing and reporting.[14]

The appropriate responsible person or persons must oversee all aspects of the agent that he or she has been chosen to supervise—from the moment of its acquisition or creation to its final destruction or transfer outside the facility. This employee is also responsible for recording any changes to an agent's status, for example by placing it on the inventory list of infectious agents. In addition, the employee must report anomalies in the inventory to the proper supervisory employee, such as the laboratory manager, the principal investigator or the biosafety and biosecurity officer. Delegating responsibility to specific employees enables full accountability for all agents under that employee's supervision and allows for the rapid detection of potential problems.

Other laboratory assets that are of potential value include:

- materials and equipment;
- laboratory notebooks, journals and raw data;
- patient data, digital or hard copy inventory lists of material, equipment and staff data (i.e. facility or security details, access lists, employee salary details, personal information etc.);
- laboratory computers; and
- shipping receipts for materials and equipment.




*Typical (Sarstedt) vials used in laboratories for storing and manipulating samples*

Every employee within a laboratory facility, regardless of the type of employment or level of access, has some degree of responsibility and accountability for maintaining biosecurity. This responsibility has been earned on the basis of the employee's qualifications and the professional evaluation of management, the laboratory manager or the principal investigator.

☛ ***Know the materials, equipment and information that are your responsibility.***
☛ ***Determine whether you are confident with the responsibility you have been given by your employer.***
☛ ***Familiarize yourself with the standard operating procedures for ensuring biosafety and biosecurity.***

### *2.3.2. Material control*

Proper inventory practices are essential for effective material control and must cover pathogens and toxins from the time that they arrive at a facility or laboratory to their final destruction or shipping.[15] Proper inventory practices must include the confirmation of receipt by the designated party. Proper biosafety practices and regulations do partially address inventory control, but this is far from common practice.

Access to areas where biological materials are used or stored must be limited to those with proper clearance. The employees who have access to and work with biological materials must be responsible for basic inventory tasks because they are familiar with the type and amount of biological materials present and their location and state. Rules and procedures for inventory control must be developed by laboratory managers or principal investigators, together with management and the biosafety and biosecurity officer.

Existing biosafety procedures for material control serve as the basis for inventory control but may conflict with security concerns. For example, lists of the pathogens or toxins in use in a laboratory are openly displayed outside it to signal the need for caution. However, from a biosecurity perspective such information must be viewed as sensitive—not to be openly displayed. Posting a 'biohazard' sign with information about the employee to contact for further details would meet this concern.

Inventories of pathogens and toxins vary in complexity, but they should include relevant information such as:

- types of material (name, strain, serotype, taxonomy etc.);
- forms of material (solution or pellet, freeze dried, paraffin embedded etc.);
- quantities of material (number of vials, amounts of liquid, post-experiment quantities);
- locations of material (in short- or long-term storage or in use);
- contact or responsible employee;
- employees who have access to the materials;
- modifications of the original biological properties of material (i.e. genetically modified microorganisms and genetically modified organisms);
- confirmation, date and method of destruction or inactivation of material; and
- dates of transfer of material (delivery and departure) and end-user or recipient receipts.

Various methods can be used to coordinate and manage material inventories.

- Local laboratory lists of material can be created and managed by those accountable for them and passed on to an employee at a higher level of authority.
- A general material list for the whole facility can be maintained, coordinated and managed by the appointed biosafety and biosecurity officer.

A general material list may reduce the numbers of material and manipulations, or replace infectious pathogens or toxins with less dangerous ones.[16]

☛ ***What specific information on materials must be recorded, and when?***
☛ ***How long must information on materials be stored?***
☛ ***How must information on materials be kept secure?***

- ***How often should such information be reviewed and updated?***
- ***Who must have access to information on materials?***
- ***How and to whom are inventory anomalies reported?***

*2.3.2.1. Additional inventory control.* Special equipment that has dual-use potential and is regulated by national and international export laws must also be controlled. The same scrutiny and security measures as those for material inventory lists must be applied. Such items include:

- biotechnological equipment, including whole-containment BSL3 and BSL4 laboratories;
- fermenters;
- centrifugal separators;
- cross (tangential) flow filtration equipment;
- freeze-drying equipment;
- aerosol inhalation chambers; and
- spraying or fogging systems.[17]

*2.3.3. Physical security*

The aim of physical security is to restrict access to those with professional qualifications and who have the immunizations that allow them to work with specific pathogens and delay, deny and detect access by unauthorized individuals. Physical security is closely associated with biosafety and facility design. However, even the most sophisticated physical security is only one component of a secure workplace. The level of security of a laboratory or facility is ultimately determined by the employee's awareness of the need for security and behaviour that reflects such an awareness.

Physical security entails:

- monitoring and managing perimeters and security boundaries;
- establishing and enforcing access restrictions;
- installing and maintaining alarm and surveillance equipment;
- determining and preserving adequate containment levels; and
- provide prompt alerts of breaches or intrusions.

A variety of equipment is used to restrict access and monitor a facility in order to detect unauthorized access (intrusions). The complexity of such equipment increases as security requirements increase. Table 1 lists the components of physical security that may be used in laboratory facilities to restrict access and provide surveillance.

The BSL designation of a facility or laboratory dictates the level of containment that is needed for safe work (table 2).[18] The biosecurity risk level corresponds to the BSL desig-


*Highly restricted area access door to BSL4 laboratory*

**Table 1.** Physical security components for control of access and surveillance

| Access control | Surveillance |
|---|---|
| • Laboratory or facility perimeter (i.e. fences, walls)<br>• Locks, keypads, electronic card readers<br>• Biometric scanners<br>• Visual identification badges<br>• Guards<br>• Facility design | • Closed circuit television cameras<br>• Night vision and infrared cameras<br>• Motion detectors (i.e. passive infrared, microwave or ultrasonic sensors)<br>• Sound recording devices<br>• Guards |

nation. As it increases, so must physical security. Higher levels of access restriction and increasingly sophisticated surveillance equipment are needed as the level of risk rises.

In most instances, 'general security' areas are accessible to all authorized employees and correspond to the physical boundary of the facility. Authorized guests and visitors may be allowed access after screening and if visual identification badges are worn. Access is controlled by locked doors that are opened with traditional keys, keypads and electronic card readers or by guards to whom identification is presented.

'Restricted' areas are BSL1 and BSL2 laboratories for microbiological work with low to moderate biosecurity restrictions. Restricted areas must be accessible only to employees who have been authorized to enter them. Most laboratories fall under this classification. They pose low risk to humans and conduct activities that only affect plants or animals.

**Table 2.** Biosafety levels and corresponding biosecurity risk and physical security levels

| Containment level | Biosecurity risk level | Level of physical security |
|---|---|---|
| Not applicable | Negligible to low | General security |
| BSL1 and BSL2 | Low to moderate | Restricted |
| BSL3 | Moderate to high | Highly restricted |
| BSL4 | High | Highly restricted |

'Highly restricted' areas have added layers of security to safeguard moderate to high-risk pathogens and toxins in BSL3 and BSL4 laboratories—the highest levels of security and restriction.

☛ ***Be aware of security areas and adopt a professional attitude towards security when in such areas and when using restricted equipment.***

☛ ***Do not rely solely on physical barriers for security. (Human behaviour is the most important component of a security system.)***

☛ ***Report negligent behaviour directly to the negligent person or to a superior.***

*2.3.3.1. Access control.* Limiting access to facilities and laboratories is a component of both biosafety and biosecurity. Management and the employees who grant access to restricted areas are responsible for ensuring that those admitted to such areas are qualified to be there or are given proper training in laboratory procedures and conduct. Most laboratory facilities employ personnel who grant or monitor access to particular areas, such as containment laboratories.

If access to facilities and laboratories by unqualified or non-immunized employees is not limited, accidental exposure or other harm may be in breach of biosafety best practices and be in violation of national work environment and occupational health laws. The degree of access permitted depends on the work performed and the materials used. While the allocation of labora-

tory workspace is usually resource driven, biosafety and biosecurity must also be taken into account.

Professional qualifications should be used as a guideline to determine who is allowed access to areas where high-risk pathogens are located, but management may wish to adopt additional screening policies, such as background checks. An employee may need also to be validated by background checks or other measures. Access to restricted areas must be re-evaluated periodically so that outdated restrictions can be removed or rights revoked if negligent behaviour has been identified.

When access to a facility or restricted areas is unsupervised, the employee must minimize the risk that access information can be obtained. For example, entering a PIN code can be observed from a distance, and key cards can easily be copied. However, when used together they provide good security because no card or code alone can be used to gain access. Entry codes should preferably be changed periodically to increase security. However, the employee plays the key role in shielding the PIN code from view and keeping the key card secure.

The employee must use good security practices when using the doors of a facility or security area. Doors must always automatically lock when closing, and the interval when they are open must be minimal in order to reduce the opportunity for unauthorized individuals to gain entry (known as tailgating).

*Electronic card reader with a scrambled numerical pad*

An unauthorized person must not be allowed to gain access by following an authorized employee through an open door. An unauthorized person may provide a false account of having misplaced or lost a key card or keys, or offer another reason for not being able to gain entry alone. The person may be persuasive or become aggressive if questioned. It is essential that the employee continues to insist on proper identification. If necessary, colleagues or security staff must be asked for assistance.

Employees must return key cards when their employment is terminated. Prompt reporting of missing key cards or keys is also important. Such key cards and keys must be rendered unusable and replaced.

- ***Be vigilant when entering PIN codes to access a facility or restricted area.***
- ***Never discuss PIN codes openly.***
- ***Avoid writing down PIN codes or storing them electronically.***
- ***Demand identification from anyone attempting to enter the facility if the person cannot gain access alone. If the person is unable to provide identification, promptly report this to the head of security or take similar action.***
- ***Return unused key cards and report losses immediately.***
- ***Make locking doors a routine, including those to offices and storage areas.***

*2.3.4. Information security*

Information that enables access to a facility or to biological materials is sensitive and must be kept secure.[19] Security measures may also be required for other sensitive information, such as:

- inventory lists of pathogens and toxins;
- sensitive equipment, including its location;
- security routines;
- access lists;
- patient sample data; and
- employee contact information.[20]

Sensitive information must be stored electronically on non-networked computers with backup hard copies kept in locked cabinets. The information must never be carried on storage peripherals such as memory USB cards. Old records must be destroyed in order to ensure that current data is accurate and that obsolete data is made unavailable.

Hardware (physical) firewalls are more reliable that software programs, and they are commonly used in large facilities. The use of software antivirus programs requires regular updating of virus definition files; keeping operating systems updated is equally important. Home computers are unlikely to offer adequate protection and the storage of sensitive information on such computers must be avoided.

Information on hard drives can also be retrieved, even after it has been deleted or the disk reformatted. One way to avoid this is by using encryption software. Such software is readily available as open source 'freeware'. Encryption software must also be used when communicating sensitive data via email. Care must be taken when decommissioning old computers to ensure that sensitive data does not remain, and the hard drive must therefore be removed.

Many facilities have an independent or shared information technology (IT) department. The IT department must be consulted to provide guidance on pertinent issues.

☛ ***Identify sensitive data and establish procedures to keep it safe and secure.***
☛ ***Use available IT security tools to ensure the integrity of electronic data.***
☛ ***Avoid maintaining sensitive data on home computers.***
☛ ***Avoid communicating sensitive information via email.***
☛ ***Keep sensitive data current and destroy data that is obsolete (including paper copies).***
☛ ***Choose complex passwords that combine upper and lower case letters with numbers.***
☛ ***Change passwords periodically.***

*2.3.5. Transfer and transport security*

Transfers of dangerous pathogens and toxins must follow national and international guidelines that are based on the UN regulations for the two most hazardous categories of material (categories A and B).[21] The UN regulations focus on the safety of the employees involved in transporting the

**Case 3.** Live *Bacillus anthracis* shipped by mistake

In May 2004 live *Bacillus anthracis* was shipped from the Southern Research Institute in Frederick, Maryland, USA, to the Oakland Children's Hospital & Research Center in Oakland, California, USA. The sender had verified that the samples were not viable. However, the death of 49 mice that were infected using the *Bacillus anthracis* samples revealed the viability of the samples.

*Source*: Vesely, R., 'Anthrax incident spurs concern', *Oakland Tribune*, 12 June 2004.

**Case 4.** British journalists order a sequence of modified smallpox DNA

On 14 June 2006, *The Guardian* reported that journalists had successfully ordered online and received a plastic vial containing the 78bp sequence of DNA coding for the smallpox virus coat protein modified with three mutations from VH Bio Ltd. The vial, which arrived in an A5-size Jiffy bag, cost £33. The company was unaware that the sequence belonged to the smallpox genome.

*Source*: Randerson, J., 'Revealed: the lax laws that could allow assembly of deadly virus DNA', *The Guardian*, 14 June 2006.

**Case 5.** *Bacillus anthracis* requested from the University of Gothenburg

The University of Gothenburg, Sweden, which has one of the largest bacteria depositories in the world, has on two occasions since the 2001 mailing of the anthrax-contaminated letters in the United States received requests for *Bacillus anthracis* that were deemed suspicious. The requests were forwarded to the Swedish security police for investigation. The University of Gothenburg has stated that its depository has never held or offered *Bacillus anthracis*.

*Source*: 'Ekot', Swedish Radio, 17 May 2006.

**Case 6.** *Yersinia pestis* shipped to Tanzania

In September 2002 Thomas Butler, a professor at Texas Tech University, Lubbock, Texas, USA, knowingly transferred the human pathogen *Yersinia pestis* (bubonic plague) to Tanzania without obtaining the required US Department of Commerce licence. He described the pathogen as 'laboratory materials' on the waybill and failed to fill out relevant sections of the Shipper's Export Declaration requirement. Butler was therefore considered to have deliberately evaded provisions of the US Export Administration Regulations. On 10 March 2004 Butler was sentenced to two years imprisonment with three years supervised release. He was also required to pay criminal fines and make restitution for export violations and false statements.

*Source*: Enserink, M. and Malakoff, D., 'The trials of Thomas Butler', *Science*, vol. 302, no. 5653 (19 Dec. 2003), pp. 2054–63.

materials and the integrity of the containment (see case studies 3–6 for examples of violations of proper procedures or mistakes). Adequate containment must also be ensured for transports over shorter distances, such as between neighbouring facilities or within a facility.

When materials are transferred in a facility or between facilities the properly packaged material must not be out of sight, even for a moment. This ensures the integrity of the transfer all the way to its final destination.[22] Professional handling must be used for longer transports and there are many companies that handle dangerous goods and possess ADR (safe international transport of dangerous goods by road) certification.[23] The primary security problem in long distance transfers is that the sender cannot personally supervise the transfer but must rely on the company to do so. In such cases, the sender must establish a chain of custody that:

- identifies the individuals involved in the transfer; and
- outlines the provisions to address potential problems.

Management or the biosafety and biosecurity officer must be notified of transfers of hazardous materials. The biosafety and biosecurity officer can

also assist in arranging for safe packaging and secure transport via appropriate carriers.

A number of criteria must be met in order to ensure safe and secure transport, no matter how benign the pathogen or toxin to be transferred.

- The recipient must be known and trusted. If that is not the case, the recipient's institutional or company affiliation must be checked via the Internet and a PubMed search of scientific merits conducted to confirm the recipient's professional qualifications.[24]
- The shipping company for the transfer must have a valid licence for handling dangerous goods. The company's policy on lost or stolen goods must be known and advice provided on what to do should loss or theft occur. The response must be that law enforcement representatives are contacted as well as both the sender and the recipient.
- The sender must ensure that the correct material is being shipped and that it is properly packaged.
- On delivery, the recipient must sign a receipt confirming that the material has arrived and matches the specifications of the material that was ordered. The recipient must mail or fax the receipt to the sender, who is then no longer responsible for the material. All information must be documented to enable the material to be traced.[25]

Many countries regulate the export of biological materials, equipment and technology as part of their effort to prevent the proliferation of weapons of mass destruction, including biological weapons. Under EU Council Regulation 3381/94/EEC it is illegal for an EU member state to export items listed in the regulation's annex without authorization.[26] The items listed in the annex include human, animal and plant pathogens and toxins.

In response to decisions by the UN Security Council, countries have passed legislation to combat terrorism that introduces new criminal offences, including some related to biological materials. Under national implementing legislation, the unauthorized export of listed items is illegal.[27] If the exporter is convicted, the facility or the employee may face criminal or administrative penalties, such as fines. Thus, the sender must establish a system to verify that shipments comply with current international export laws and do not violate relevant treaties or embargoes.

*Common packaging for hazardous biological materials*

Export control authorities often organize open meetings where they explain the current laws to exporters. The national authorities are also often willing to visit facilities to provide information on export control laws.

- ☛ *Always consult with the laboratory manager or principal investigator about transfers or requests and ensure the correct state of the sample(s).*
- ☛ *When shipping pathogens and toxins, verify that the recipient is legitimate by checking credentials and affiliation.*
- ☛ *Never ship to an unknown recipient.*
- ☛ *Establish a chain of custody when transporting materials.*
- ☛ *Never leave hazardous biological materials unattended in areas of lower biosecurity during transfers.*
- ☛ *Use only qualified handlers that have proper training and use correct procedures, including a final receipt of delivery.*

*In addition*

- ☛ *Learn about and abide by the national laws regulating exports from your country, including the laws passed by the European Union. (What is the legal definition of an export? Are you an exporter?)*
- ☛ *Check that pending transfers comply with national and international export laws.*
- ☛ *Learn about opportunities to discuss export controls with your national authorities.*
- ☛ *Ask your professional handler if they have procedures for security during transport of dangerous goods.*

## 3. SUPERVISION OF APPLIED BIOSECURITY

### 3.1. Biosecurity concerns for the laboratory manager and the principal investigator

Ensuring safety and security in storing and handling infectious agents and toxins is a prerequisite for any life science activity and for keeping the trust of the public and that of decision makers. Such safeguarding is also an international obligation under the Biological and Toxin Weapons Convention, which 163 states have signed and ratified since its adoption on 26 March 1975.[28] UN Security Council Resolution 1540 also requires that UN member states implement national legislation and other measures to prohibit and prevent the proliferation of biological weapons. The resolution mandates that control must be established and maintained over related materials that could be used for the development of such weapons.[29]

The levels of security awareness and of threat perception vary widely from scientist to scientist and from country to country. In addition, the scientific community is somewhat reluctant to accept abstract threats, such as those of internal sabotage and bioterrorism. The USA, for example, has increasingly focused on 'biodefence' research and national regulations for life science facilities and activities, and this has produced new problems and restrictions, such as those related to transfers of material and knowledge.[30]

A balance must be found: fulfilling international obligations to secure infectious pathogens and toxins, sensitive equipment, technologies and information and preventing them from falling into the wrong hands or being misused must occur without hindering the scientific community. Applied biosecurity requires an approach that is both balanced and nuanced and that seriously addresses abstract threats combined with the understanding that security threats are dynamic.

### 3.2. Managing applied biosecurity

A comprehensive biosecurity risk assessment falls outside the scope of this handbook and legislation would be needed to require that such assessments be carried out at all facilities and laboratories. However, it is the responsibility of laboratory managers and principal investigators to improve biosecurity in the laboratory and safeguard the assets under their supervision. Biosecurity risks and the management of them are best identified by the use of biosecurity risk assessment scenarios and by listing the most dangerous agents. The standard biosafety level classification system can be used to make such determinations.

*3.2.1. Material management*

*A common freezer room for BSL1 or BSL2 materials or reagents*

*3.2.1.1. Inventory control.* 'Inventory control' can be summarized as having a complete overview of all pathogens or toxins (materials) in custody. Good inventory control provides the benefit of enabling full accountability at any time (see also section 2.3.2). The absence of a detailed inventory is a potential security risk, and also a threat to the safety of laboratory employees. In many laboratories samples are allowed to accumulate, creating a potential hazard. Good inventory control also enables rapid detection of discrepancies, which is of major importance in the context of security. In addition, in the event that a facility or a laboratory appears to be the source of a pathogen that has been used maliciously, inventory information can be used to defend the laboratory's practices.

*3.2.1.2. Inventory information.* A determination must be made of what information to include in an inventory list. Changes made to material amounts during experimentation must also be reflected. The suggested characteristics of a material inventory list are discussed above (see section 2.3.2). Inventory lists must be deemed sensitive and handled and stored securely by the responsible employee because of the sensitive information that they contain.

*3.2.1.3. Materials in use.* Monitoring and noting experimental parameters are good laboratory practice and provide valuable information when updating inventory lists. Materials in use may be difficult to quantify, especially during culturing or other procedures when the number of samples and volumes does not correspond to previous amounts for short periods of time. Samples must be given new identification or sample numbers following experimental use and re-entered in the inventory list. The destruction of material must also be noted.

*3.2.1.4. Materials in storage.* Whether materials are stored for a short or long period, their storage must follow the provisions of containment and adhere to the appropriate biosafety level classification and the provisions of the biosafety guidelines in use. Viable BSL4 materials must remain stored in BSL4 containment laboratories at all times, and detailed inventories of such materials must be maintained, until the viable material has been properly inactivated and is deemed safe for transfer outside the BSL4 containment area.[31] Similarly, viable BSL3 materials should be stored in a BSL3 containment laboratory under similar conditions, but this may not always be possible due to limited space. Breaches in both biosafety and biosecurity best prac-

tices must be addressed. BSL activities must be adapted to the available capacity of the containment facilities rather than altering best practices because of space limitations.

*3.2.1.5. New acquisitions.* New acquisitions must be promptly incorporated into the inventory system so that they can be managed by it. Introducing new or modified pathogens or toxins into an inventory may require permission from or notification to national authorities. The facility may also need to provide assurance that it can safely store and handle the new materials using relevant BSL containment guidelines and that a proper biosafety risk assessment has been made. The appropriate supervisor must determine which employees are authorized to access new materials and that decision must be communicated to other employees.

*3.2.1.6. Sensitive laboratory equipment.* Laboratory equipment that is controlled by international export laws and regulations can be termed 'sensitive'. Such equipment may be desirable to an adversary. The Australia Group is an informal gathering of 41 countries that focuses on the use of licensing measures for the export of certain chemicals, biological agents and related equipment, with the objective of countering the proliferation of chemical and biological agents.[32] The group's website lists select pathogens, toxins and equipment that require export licensing (see also section 2.3.2.1) Equipment in these categories must be kept secure and accounted for at all times. The loss or theft of such equipment must be reported to management.

*A fully suited researcher in a BSL4 laboratory*

### *3.2.2. Personnel management*

The laboratory manager or the principal investigator manages the employees who use materials, equipment and facility infrastructure on a daily basis. Good leadership and management is important for both biosafety and biosecurity because the laboratory manager or the principal investigator will delegate responsibility for and the right of access to dangerous materials. Responsibility is delegated on the basis of professional qualifications, security vetting and prior employment. Education and training together with proper guidance are essential to establish a well-functioning group of co-workers and to avoid conflict.

A commonly discussed threat is the 'insider' threat posed by a person with both access to materials and the technical know how to covertly appropriate and use them for malicious purposes. In order to address such threats, personnel management must include strategies to detect and manage conflicts before they become a liability to safety and security. Establishing and maintaining good professional relationships with employees may help to prevent such situations.

*Negative pressure room for suiting up before entering the BSL4 laboratory*

*3.2.2.1. Pre-employment scrutiny.* Before a potential employee is called to an interview, credentials and past work experience must be verified to establish confidence in the capabilities of the potential employee. Previous employers must be asked for recommendations and academic qualifications must be verified. An Internet search may provide additional information about a potential recruit and may suggest questions to be asked during an employment interview.

If the employee will be granted access to materials of elevated risk and high-level (BSL3 and BSL4) containment laboratories, more sophisticated background screening (security vetting) may be required. Such screening entails the use of security specialists and law enforcement personnel and must be handled by facility management in consultation with the laboratory manager or the biosafety and biosecurity officer.

*3.2.2.2. Delegation of responsibility.* Before a new employee is authorized to access restricted areas, the appropriate supervisor must thoroughly assess what level of access and autonomy to allow. Initially, access must be limited to those areas that are essential to the new employee's work and to those storage areas where the materials needed for that work are located. During an introductory period, the laboratory manager or the principal investigator may opt to personally supervise the new employee and grant access to materials and areas of the laboratory under supervision in order to establish that work is performed safely and securely. Gradually, the new employee's autonomy can be increased.

In a culture of responsibility, responsibilities are defined for each employee as part of a team and awareness of security issues is nurtured. Delegated responsibilities must match the capabilities of the team members, and this delegation must be regularly reassessed by the laboratory manager or the principal investigator.

*3.2.2.3. Access rights and employee responsibility.* Access to restricted areas must be based on need and qualifications. The laboratory manager or the principal investigator must take into account the level of autonomy needed by an employee and consider factors such as the hours the employee will be allowed access and the areas to which access will be permitted (e.g. freezer and apparatus rooms, and containment laboratories). Employees with access to BSL1 and BSL2 laboratories and materials require restricted area access. Full access to BSL3 or BSL4 laboratories necessitates highly restricted area access. A common strategy employed both for safety reasons and to address the insider threat is to use a 'two-person rule', where no one person is allowed

autonomous access to BSL3 or BSL4 areas. Restrictions may also apply to activities that fall outside the context of BSL classifications, such as production or work involving animals.

Access rights must be re-evaluated periodically and revoked when no longer needed. Negligent or careless behaviour that affects safety or security must be investigated and access rights revoked or denied when appropriate. When employment is terminated, it is good practice to have a proper procedure for revoking access rights and other work-related privileges in a timely manner, including the return of ID badges and the cancelling or return of access cards.

Special care must be taken with visitors who are allowed a basic level of access into a facility or laboratory. The security aspects of permitting a visitor to enter a laboratory must be considered beforehand, and the host must be responsible for the safety and behaviour of the visitor at all times.

*3.2.2.4. Managing conflicts*. In order to ensure a safe and secure work environment, interpersonal conflicts and other problems that may influence work must be identified and addressed (see also above). Problems may arise between colleagues, between staff and management, or may be of a personal nature. They include issues related to:

- personal relationships;
- salary or economic issues;
- competitiveness;
- social exclusion;
- mental health; and
- private life.

Regardless of the nature of the problem, it is vital that it is detected early, before it gets out of control.

Disputes among staff or personal problems outside the workplace have the potential to lead to the development of an insider threat. The potential for such a development may be difficult to detect, particularly if the source of dissatisfaction lies outside the workplace. A laboratory manager or the principal investigator must be responsive to staff, try to identify problems early and offer appropriate means of resolution, such as counselling or mediation. The employee must have access to help or counselling if necessary.

### *3.2.3. Information management*

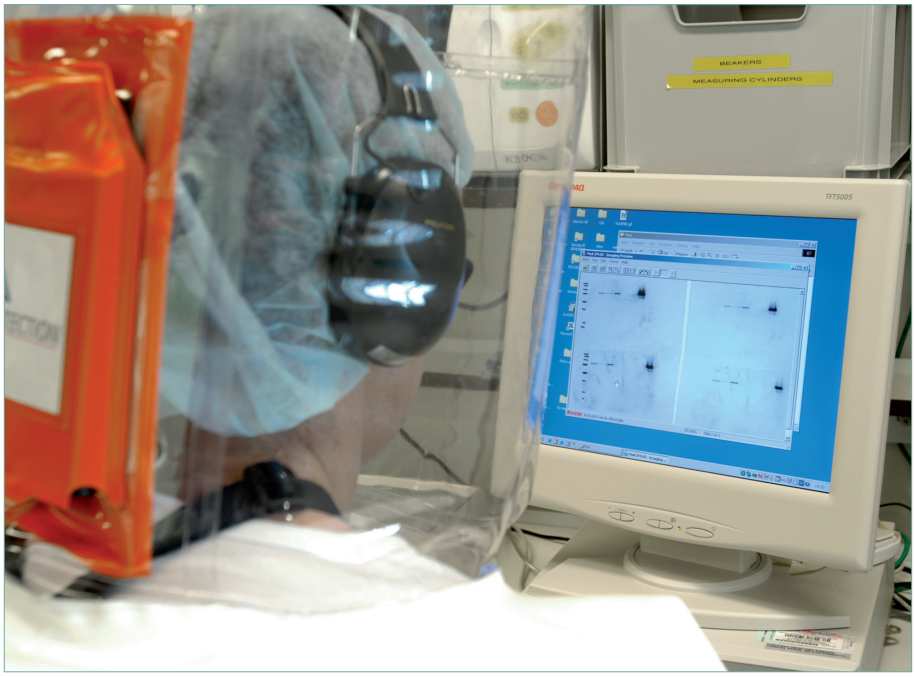
*3.2.3.1. Types of sensitive information*. Safeguarding sensitive information is as important as restricting access to hazardous materials. Access to sensitive information must be restricted to those employees who need it for their work. Sensitive information is often information that could be used by an adversary to gain access to a facility and the hazardous biological materials it contains (see also section 2.3.5). This includes information on:

- pathogens and toxins;
- storage locations;
- entry codes;

- physical security; and
- security procedures.

Other information about laboratory assets or employees may also be valuable or of interest to certain groups and must be safeguarded. An adversary could use information on an employee to coerce that employee into appropriating information or materials or into providing access to a facility. Such information includes:

- employment details;
- medical records;
- the names of employees who handle laboratory animals; and
- personal email correspondence.




*BSL4 laboratory computer*

A third type of sensitive information must be given additional protection. Such information must not be made available to other employees or to non-employees. It includes:

- unpublished experimental data;
- proprietary information;
- patent applications;
- in-house protocols; and
- patient data, which is often also protected by national legislation.

*3.2.3.2. Safeguarding sensitive information.* Determining which information to label as sensitive is a difficult challenge. The author of the information (generally the laboratory manager or the principal investigator) must make the decision on whether the information should be considered sensitive. The author must specify how to protect the information and who may have access to it. The author must also decide when it is no longer sensitive or when it can be destroyed.[33] The latter practice helps to keep the amount of restricted information at necessary and manageable levels.

Sensitive information must be safeguarded by using appropriate procedures for creating, filing, sending and destroying physical or electronic copies. Encryption must be used when deemed appropriate. Adequate backup capabilities must be used to ensure that data is not irretrievably lost or corrupted.

### 3.3. Biosecurity emergencies

Emergencies or unexpected situations may occur despite effective risk management. Contingency plans must exist to deal with such situations. Plan-

ning for emergencies or unexpected situations is an integral part of applied biosecurity. Each laboratory must develop procedures for assessing unusual situations and establish criteria for determining when outside involvement is warranted. Some security-related events may require the involvement of law enforcement personnel and result in criminal investigations.

Outside assistance may need to be sought when:

- property damage occurs;
- personal injury takes place;
- threats are made; or
- commodities are stolen.

### *3.3.1. Response planning*

The response to a biosecurity breach or incident must include procedures to deal with the various aspects of such occurrences. Contingency plans for such an emergency or unexpected situation must address:

- damage to property;
- injury to employees;
- theft or other loss of assets, including entry codes, badges and the like;
- inventory discrepancies;
- attempted or successful unauthorized access (physical and electronic);
- violence and threats; and
- suspicious or negligent behaviour.

The response plan must clearly outline the procedures to be followed. It must aim to effectively communicate important information to all employees and the relevant authorities. The plan must include:

- procedures for assessing the severity of the incident in order to determine the proper course of action;
- the name of the supervisory employee (i.e. the laboratory manager, the principal investigator or the biosafety and biosecurity officer);
- delineation of roles and responsibilities, including during non-office hours;
- a floor plan of and other relevant information about the facility, building or laboratory;
- emergency routines for safe evacuation, transport and transfer of casualties;
- methods for the safe removal of dangerous substances and proper decontamination procedures;
- information about emergency response personnel and local law enforcement; and
- other relevant contact information.

### *3.3.2. Reporting security breaches or incidents*

A reliable and easily accessible electronic or physical system must exist in order for the reporting of security breaches or incidents to function satis-

factorily. Such a system depends on willingness to report events, regardless of their severity or implications. Security breaches or incidents are often not reported because the situation was well managed and resolved. A biosecurity breach or incident may also not be reported due to embarrassment that the event occurred or because of fear of exaggerating the situation.

However, failure to report an event means that any lesson learned will be lost. The biosecurity-related incidents that have been documented in the scientific literature are mainly those that have occurred in the USA, where stringent legislation governs the use and transfer of biological materials and where biosafety and biosecurity are openly scrutinized. The lack of information on similar incidents in other countries and on the lessons learned from them weakens the case for biosecurity among the stakeholders in those countries and may be due to such events not being reported in the first place.

*Emergency access door to a BSL4 laboratory*

### 3.4. Training and evaluation

Constant evaluation and revision of procedures and protocols are significant factors in maintaining biosecurity at a high level. The procedures involved in work with pathogens and toxins may change over time. Such changes as well as alterations in material stocks, storage locations and access must be conveyed in a timely manner to the employees who are responsible for security. If accuracy of information and accountability are to be maintained employees must be kept informed. Such routines also enable the rapid reporting of incidents and assist each employee to remain aware of biosecurity and personal responsibility.

Inspections and audits to ensure that provisions are followed are important tools to achieve biosecurity. Participation in emergency response drills also helps maintain awareness of biosecurity's importance. Such drills help to define the individual employee's role while revealing deficiencies in preparedness.

## GLOSSARY

| | |
|---|---|
| **ADR** | European Agreement concerning the International Carriage of Dangerous Goods by Road (Accord européen sur le transport des marchandises dangereuses par route). It was opened for signature on 30 September 1957 and entered into force on 29 January 1968. It is intended to increase the safety of international transport of dangerous goods by road and outlines how dangerous goods may be transported internationally. |
| **Biosafety** | Principles, technologies and practices implemented to prevent the accidental or unintentional exposure or release of pathogens and toxins. |
| **Biosecurity** | Principles, technologies and practices implemented to secure pathogens, toxins and sensitive technology from unauthorized access, loss, theft, misuse, diversion or intentional release. |
| **Bioterrorism** | Act of violence or the threat of using biological agents or toxins to further a political agenda or challenge democratic values. |
| **BSL** | Biosafety levels 1 to 4, which describe the level of containment needed for safe and secure work with specific pathogens or toxins. BSL1 is the lowest level of containment, while BSL4 is the highest. |
| **BTWC** | Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction (Biological and Toxin Weapons Convention). It was opened for signature on 10 April 1972 and entered into force on 26 March 1975. It prohibits the development, production, stockpiling or acquisition by other means or retention of microbial or other biological agents or toxins whatever their origin or method of production of types and in quantities that have no justification of prophylactic, protective or other peaceful purposes, as well as weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict. |
| **Containment** | Isolation of hazardous materials to prevent their causing harm to people, animals and plants or damaging the environment. |
| **Dual use** | Materials, information or technologies that have more than one use and can be misused in a harmful way. |
| **Insider threat** | Individual with access to a facility (i.e. employee or legitimate user) who intentionally, or because of coercion, procures or uses facility assets for a malicious purpose. |

| | |
|---|---|
| **Principal investigator** | A key researcher—such as a senior scientist, group leader or laboratory manager—who is the primary custodian of biological materials, equipment and sensitive information. |
| **Risk assessment** | Process of identifying sources of potential harm associated with possible loss, theft, unauthorized access, misuse, diversion or intentional release of pathogens or toxins when stored, used for legitimate purposes, transferred and supplied. Also includes assessing the possibility that such harm will occur and the level of both short- and long-term harm. |
| **Risk management** | Implementation of procedures and practices to minimize risk to an acceptable level. |
| **Sensitive information** | Information that could be of potential use to an adversary in gaining access to a facility and the hazardous biological materials within (e.g. lists of pathogens and toxins, storage locations, access entry codes, security routines, and physical and procedural security details). |
| **Severity** | Risk assessment term for the potential hazard or damage posed by a biological agent or toxin. |
| **WHO** | World Health Organization. |

## NOTES

[1] The definition is based on World Health Organization (WHO), *Biorisk Management: Laboratory Biosecurity Guidance* (WHO: Geneva, Sep. 2006), <http://www.who.int/resources/publications/biosafety/WHO_CDS_EPR_2006_6/en/>, pp. 6–8; Organisation for Economic Co-operation and Development (OECD), Directorate for Science, Technology and Industry, *Best Practice Guidelines on Biosecurity for Biological Resource Centres* (OECD: Paris, 2007), <http://www.oecd.org/>, p. 8; and International Biorisk Standards Development Initiative Secretariat, 'Laboratory biorisk management standard, CWA biorisk public enquiry', 25 July 2007, <http://www.biorisk.eu/documents/draft_document.PDF>, pp. 7–13. CWA stands for CEN Workshop Agreement; CEN stands for Comité Européen de Normalisation (European Committee for Standardization).

[2] Council Directive 90/219/EEC of 23 April 1990 on the contained use of genetically modified micro-organisms, *Official Journal of the European Communities*, L117, 8 May 1990; Directive 2000/54/EC of the European Parliament and of the Council of 18 September 2000 on the protection of workers from risks related to exposure to biological agents at work, *Official Journal of the European Communities*, L262, 17 Oct. 2000; and Council Directive 2001/18/EC of the European Parliament and of the Council of 12 March 2001 on the deliberate release into the environment of genetically modified organisms and repealing Council Directive 90/220/EEC, *Official Journal of the European Communities*, L106, 17 Apr. 2001. See also note 1.

[3] Organisation for Economic Co-operation and Development (note 1); World Health Organization (note 1); US Department of Health and Human Services, Public Health Service, Centers for Disease Control and Prevention and National Institutes of Health, *Biosafety in Microbiological and Biomedical Laboratories*, 5th edn (US Government Printing Office: Washington, DC, 2007); Royal Netherlands Academy of Arts and Sciences, *A Code of Conduct for Biosecurity: Report by the Biosecurity Working Group* (Royal Netherlands Academy of Arts and Sciences: Amsterdam, Aug. 2008); and European Committee for Standardization, 'Laboratory biorisk management standard', CEN Workshop Agreement CWA15793, Feb. 2008, <ftp://ftp.cenorm.be/PUBLIC/CWAs/wokrshop31/CWA15793.pdf>.

[4] The text of the BTWC is available at <http://www.opbw.org/convention/documents/btwctext.pdf>. See BTWC, Article 4; and UN Security Council Resolution 1540, 28 Apr. 2004, Article 3.

[5] The definition is from World Health Organization (note 1), p. 4.

[6] World Health Organization (note 1), pp. 13–14.

[7] US Department of Health and Human Services (note 3).

[8] Directive 2000/54/EC (note 2).

[9] Salerno, R. M. and Gaudioso, J., *Laboratory Biosecurity Handbook* (CRC Press: Boca Raton, FL, 2007), p. 16.

[10] Carus, S. W., 'Bioterrorism and biocrimes: the illicit use of biological agents since 1900', Working paper, Center for Counterproliferation Research, National Defence University, Washington, DC, Feb. 2001, pp. 50–58.

[11] Biosafety levels 1 to 4 describe the level of containment needed for safe and secure work with specific pathogens or toxins.

[12] EU guidelines for laboratory biosecurity have not yet been finalized and thus a complete biosecurity assessment is not possible and falls outside the scope of this handbook.

[13] World Health Organization (note 1), p. 23.

[14] Salerno and Gaudioso (note 9), p. 51.

[15] World Health Organization (note 1), p. 19.

[16] International Biorisk Standards Development Initiative Secretariat (note 1), p. 46. 'The employer shall avoid the use of a harmful biological agent if the nature of the activity so permits, by replacing it with a biological agent which, under its conditions of use, is not dangerous or is less dangerous to workers' health, as the case may be, in the present state of knowledge.' Directive 2000/54/EC (note 2), Article 5 (replacements).

[17] Australia Group, 'Control list of dual-use biological equipment and related technology', <http://www.australiagroup.net/en/dual_biological.html>.

[18] Organisation for Economic Co-operation and Development (note 1), pp. 10–11, 16.

[19] World Health Organization (note 1), p. 27.

[20] European Committee for Standardization (note 3), p. 45.

[21] International Biorisk Standards Development Initiative Secretariat (note 1), p. 41; and World Health Organization (note 1), p. 22. See also the European Agreement concerning the International Carriage of Dangerous Goods by Road (Accord européen sur le transport des marchandises dangereuses par route, ADR). It was opened for signature on 30 Sep. 1957 and entered into force on 29 Jan. 1968. The most recent amendments entered into force on 1 Jan. 2009. A revised consolidated version was published as document ECE/TRANS/202, vols 1 and 2 (ADR 2009), <http://www.unece.org/trans/danger/publi/adr/adr2009/09ContentsE.html>.

[22] Organisation for Economic Co-operation and Development (note 1), p. 14.

[23] See ADR (note 21).

[24] See the PubMed website, <http://www.ncbi.nlm.nih.gov/PubMed/>.

[25] European Committee for Standardization (note 3), p. 29.

[26] Council Regulation 3381/94/EEC on the control of export of dual-use goods, *Official Journal of the European Communities*, L367, 31 Dec. 1994, p. 1.

[27] Council Regulation (EC) no. 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfers, brokering and transit of dual-use items, *Official Journal of the European Union*, L134, 29 May 2009.

[28] The convention text is available at <http://www.opbw.org/convention/conv.html>.

[29] UN Security Council Resolution 1540 (note 4).

[30] US Government Accountability Office (GAO), *High-Containment Biosafety Laboratories: Preliminary Observations on the Oversight of the Proliferation of BSL-3 and BSL-4 Laboratories in the United States*, GAO-08-108T (GAO: Washington, DC, 4 Oct. 2007).

[31] Public Health Agency of Canada, *Laboratory Biosafety Guidelines*, 3rd edn (Public Works and Government Services: Ottawa, 2004), p. 27.

[32] See the Australia Group website, <http://www.australiagroup.net/>. The current Australia Group participants are Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, South Korea, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom, the United States and the European Commission.

[33] Salerno and Gaudioso (note 9), p. 58.

## ABOUT THE AUTHOR

**Dr Peter Clevestig** (Sweden) is a Senior Researcher with the Chemical and Biological Security Project of the SIPRI Arms Control and Non-proliferation Programme. He is a virologist by training and, before joining SIPRI, conducted research at the Department of Microbiology, Tumor and Cell Biology of Karolinska Institute (KI), Stockholm. He also served as the administrator of the KI Biosafety Committee. He is an active member of the Nordic Biosafety Network and the European Biosafety Association (EBSA). He has authored or co-authored several scientific publications, primarily in the field of virology, and regularly lectures on biosecurity issues at European scientific research facilities.

sipri

**STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE**

**Handbook of Applied Biosecurity for Life Science Laboratories**

Biosecurity covers a broad spectrum of potential risks and threats ranging from criminal activities to bioterrorism and espionage. This handbook focuses on the laboratory-related activities and basic components of applied biosecurity that are relevant to all laboratory employees. The role played by laboratory managers and principal investigators in safeguarding laboratory assets and the employees under their supervision is also highlighted.

This handbook provides guidance for personnel who work with infectious pathogens and toxins that may affect the health of humans, animals and plants. It aims to engage scientists, laboratory employees and students in laboratory biosecurity, and to provide practical advice that will ensure the secure handling and storage of biological materials.

Acknowledging biosecurity risks and the important role of the employee in maintaining biosecurity is crucial to keeping the workplace safe and secure. Safeguarding infectious agents is also a national legal obligation under the 1972 Biological and Toxin Weapons Convention and United Nations Security Council Resolution 1540.

ISBN 978-91-85114-61-0