

An efficient and practical approach to  
**BIOSECURITY**





# PREFACE

In 2008, the Danish Parliament enacted a comprehensive Biosecurity Law; the following year, the Danish Ministry of Health issued an Executive Order describing the practical details of implementation.

A lot of research and hard work went into the preparation of this legislation, and its implementation was equally demanding. But today Denmark has a straightforward and well-functioning biosecurity system, based upon a single, dedicated law and a single executive order. And we at the Danish Centre for Biosecurity and Biopreparedness (CBB) have gained a great deal of experience that could be of value to others.

Biosecurity systems such as the one in Denmark have been required of all United Nations members since 2004. This handbook was created by the CBB – Denmark’s National Biosecurity Agency – as an aid to those countries that are still in the process of fulfilling the UN mandate. The book was supported through a collaboration between CBB and the Ministry of Defense, the Ministry of Foreign Affairs and the Ministry of Health.

Our aim is to draw upon our experiences with biosecurity to suggest an efficient and practical model that other countries can use – in whole or in part – as a blueprint for establishing or improving their own biosecurity systems. We hope you will find it helpful.



## TABLE OF CONTENTS

---

<b>PREFACE</b> .....	<b>3</b>
<b>INTRODUCTION:</b>	
<b>AN UP-TO-DATE BIOSECURITY SYSTEM</b> .....	<b>7</b>
<b>SECTION 1:</b>	
<b>SETTING UP A BIOSECURITY SYSTEM</b> .....	<b>17</b>
<b>CHAPTER 1:</b> The elements of biosecurity .....	<b>19</b>
<b>CHAPTER 2:</b> Preparing a gap analysis .....	<b>29</b>
<b>CHAPTER 3:</b> Creating a Biosecurity Law .....	<b>39</b>
<b>CHAPTER 4:</b> Creating a Biosecurity Agency and an Executive Order .....	<b>49</b>
<b>CHAPTER 5:</b> Practical implementation of biosecurity .....	<b>65</b>
<b>CHAPTER 6:</b> Enforcement activities and revision of laws .....	<b>77</b>
<b>SECTION 2:</b>	
<b>BIOSECURITY IN PRACTICE</b> .....	<b>87</b>
<b>CHAPTER 7:</b> Vulnerability assessments and security plans .....	<b>89</b>
<b>CHAPTER 8:</b> A general guide to licensing .....	<b>101</b>



---

<b>CHAPTER 9:</b>	Exceptions and special licensing cases .....	<b>113</b>
<b>CHAPTER 10:</b>	Employee security .....	<b>121</b>
<b>CHAPTER 11:</b>	The basics of physical security .....	<b>135</b>
<b>CHAPTER 12:</b>	Lock and key: choosing the right security system .....	<b>149</b>
<b>CHAPTER 13:</b>	Inventory control .....	<b>163</b>
<b>CHAPTER 14:</b>	Biopreparedness .....	<b>177</b>
<b>CHAPTER 15:</b>	The work of Biosecurity Officers .....	<b>193</b>
<b>CHAPTER 16:</b>	Preparing and conducting an inspection visit .....	<b>205</b>
 <b>SECTION 3:</b>		
	IMPORTANT BIOSECURITY ISSUES .....	<b>221</b>
<b>CHAPTER 17:</b>	Biosecurity culture and bioethics .....	<b>223</b>
<b>CHAPTER 18:</b>	Dual-use technology .....	<b>235</b>
<b>CHAPTER 19:</b>	Future challenges .....	<b>249</b>
<b>CHAPTER 20:</b>	Dilemmas for discussion .....	<b>261</b>
<b>GLOSSARY</b>	.....	<b>267</b>





INTRODUCTION:

# AN UP-TO-DATE BIOSECURITY SYSTEM

*In today's world, terrorism is probably a greater menace to biosecurity than hostile nations and governments. This book will show you how to address contemporary biosecurity threats with an up-to-date system.*



**O**n 18 September 2001, exactly one week after the terrorist attack on the World Trade Center in New York, letters containing deadly anthrax spores were mailed to several US news media. Three weeks later, another two 'anthrax letters' were sent to the offices of two United States Senators.

Twenty-two people developed anthrax infections as a result of these attacks; five of the victims died. Dozens of buildings were contaminated by the letters that circulated through the postal system and a variety of other offices. Cleanup-efforts took many months, and an FBI estimate places the total cost at around 1 billion USD.

The lengthy investigation that followed revealed a shockingly flawed biosecurity system that allowed a mentally disturbed scientist at a military research facility to work with one of the deadliest bacteria strains in the world.

**See box** on page 15-16: 'Anatomy of a failure: no questions were asked'.

It was a spectacular demonstration of the need for effective measures to prevent legitimate research material from being turned into a diabolical weapon.

### BIOSECURITY IS DESIGNED TO PREVENT THE UNTHINKABLE

---

No legitimate research facility, private company or other entity is interested in supplying the needs of a madman – or involuntarily helping to create a horrifying weapon. But as the anthrax case and



other examples from around the world have demonstrated, the danger of a facility becoming an unwilling supplier to the makers of biological weapons is very real.

It is precisely this kind of unthinkable situation that a good biosecurity system must prevent.

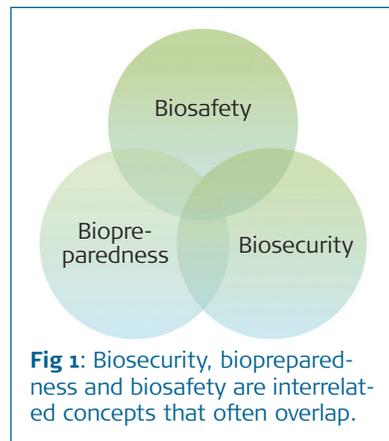
*Biosecurity*, then, is a series of measures designed to prevent the malicious abuse of 'dual use' biological materials – that is, biological substances and related materials that are intended for legal research but which could also be used to create and disseminate a dangerous biological agent.

### BIOSECURITY, BIOSAFETY AND BIOPREPAREDNESS ARE RELATED CONCEPTS

---

**Biosecurity** differs somewhat from the concepts of **biosafety** and **biopreparedness**. All three are interrelated (see fig. 1), and all of them relate in one way or another to the anthrax case. But there are also important differences.

**Biosafety** is the *prevention of accidents* that involve the release of harmful biological substances. Biosafety measures are primarily designed to protect the people who work with these substances. But it relates to biosecurity and biopreparedness in the sense that many biosecurity regulations can also improve laboratory safety.



**Biopreparedness** is likewise linked to both safety and security: it involves *knowing what to do* if a biosecurity or biosafety failure occurs. Immediate warning, containment, detection and decontamination measures are a necessary part of preparedness, regardless of whether the release of a harmful biological substance was intentional or accidental.

**Biosecurity**, as previously mentioned, is the *prevention of malicious* use of biological substances and related materials.

All three of these concepts are important. For the purposes of this book, however, our highest priority and primary focus will be on how to prevent materials intended for peaceful purposes from being used in a biological attack.

### BIOLOGICAL WEAPONS HAVE A LONG HISTORY

The use of biological weapons has a history that began long before the anthrax letters in 2001. Infected corpses have been used for hundreds of years to spread disease among enemy troops. In 1763, a colonial British captain is said to have given smallpox-infected blankets to a Native American tribe during a conflict near Fort Pitt (now Pittsburg).

More recent examples include Japanese attacks with biological weapons on 11 Chinese cities between 1932 and 1945. Many years later, Japan was itself the victim of what could have been a catastrophic biological assault: in 1993, members of the fanatical Aum Shinrikyo cult sprayed a suburb of Tokyo with a strain of anthrax bacteria cultivated in the basement of the group's headquarters.



The strain turned out to be non-virulent, but some investigators believe this was only a 'practice' exercise. The motives of the cult were certainly malicious: two years later, the same group executed a widely-publicised chemical gas attack in the Tokyo subway system that killed 12 and sickened thousands.

'Delivery systems' refers to equipment that can be used to deploy a biological weapon. In practice, this often means an unmanned spraying system.

### INTERNATIONAL LAW REQUIRES BIOSECURITY MEASURES

---

International laws and regulations have addressed the issue of biosecurity for decades.

The Biological and Toxin Weapons Convention (BTWC), for example, is an international treaty that went into effect in 1975. It bans the use of biological weapons and prohibits all development, production, acquisition, stockpiling or transfer of such weapons.

The United Nations Security Council Resolution 1540 (UNSCR 1540), enacted in 2004, legally requires all member nations to "take and enforce effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery, including by establishing appropriate controls over related materials."

The Danish biosecurity law, for example, was enacted in 2008 as a direct result of UNSCR 1540.



## BIOSECURITY INVOLVES MORE THAN TOXINS

---

Throughout this book, you will find the expression 'biological substances and related materials'. 'Biological substances', in this context, are biological pathogens and toxins that can be used in a biological weapon.

But biosecurity deals with more than pathogens and toxins. Hence the expression 'related materials' – a common term for the equipment (fermenters, spray driers, etc.) that can be used or modified to create biological weapons. Such equipment also includes the delivery systems that can be used to deploy a biological weapon. In practice, this often means an unmanned spraying system.

'Related materials' also refers to non-public *information and knowledge* that could be misused for harmful purposes. This type of material is sometimes also referred to as 'technology'.

When we use the term 'related materials' in this book, it is meant to include all the above-mentioned elements.

**You will find** more detailed definitions of these concepts in the Glossary beginning on page 267.

## YOU MAY WISH TO EXCLUDE 'RELATED MATERIALS' TO BEGIN WITH

---

Not every country will wish to include 'related materials' in its biosecurity legislation to begin with. In Denmark, we have chosen to regulate these



materials as mandated by UNSCR1540 and have therefore included it in our suggestion for a complete biosecurity system.

Regardless of how you choose to structure or time the implementation of your biosecurity system, you can use this book as a how-to for executing the aspects of the system that you find relevant.

### BIOSECURITY LAWS MUST ADDRESS A NEW KIND OF THREAT

---

Many biosecurity-related measures around the world – including the security regulations that existed in Denmark before the anthrax attacks – have been based on the assumption that the main biosecurity threat is from hostile countries and governments, and that biological weapons would be used in a war between nations.

This may sometimes still be the case. It is certainly how biological weapons have been used in the past, and biosecurity during the Cold War was based on this scenario. But the anthrax case of 2001 was painful proof that the post-Cold War era involved new kinds of threats that were not being properly addressed by countries throughout the world.

Cold War security could not protect the anthrax victims from the actions of a disturbed laboratory employee with access to a highly dangerous pathogen. Nor did it take into account modern-day terrorist activity such as the Aum Shinrikyo attack, which originated in a relatively small group that was loyal to a fanatical belief rather than to a national government.



For these reasons, even countries that have already addressed biosecurity-related issues may need to update or supplement their legislation and security systems.

### YOU CAN FIND EXACTLY WHAT YOU NEED

---

This book is intended to help you establish an efficient and practical biosecurity system that addresses modern-day threats and issues. If your country already has a biosecurity system, this book will help you to assess whether it needs to be updated or supplemented. It will also describe what you need to do.

You can read this book from cover to cover or use it as a reference tool. It is divided into sections, chapters and smaller segments with headings that make it easy to find exactly what you need to know.

To make this book even more accessible, it is illustrated throughout with case stories, diagrams, photographs and best practice tips ('Lessons learned').

**Supplementary material** can be found on the Danish Centre for Biosecurity and Biopreparedness website. You will find the website at [www.biosecurity.dk/eng](http://www.biosecurity.dk/eng). To find the material related to this book, click 'Resources', and then click 'Biosecurity Book'.

As previously mentioned, **you will also find** a Glossary of biosecurity terms at the back of this book.



## A BIOSECURITY SYSTEM MUST APPLY TO EVERYONE

Later in this book we will discuss in more detail the issues related to 'insider' threats of the type posed by employees like the scientist behind the anthrax attacks.

But we will begin with a basic review of how to set up and implement an effective, national biosecurity system that applies to every employee, and to each and every research facility, hospital, private company, diagnostic laboratory, retailer or other entity – whether military or civilian – that in any way handles biological substances and related materials.

### ANATOMY OF A FAILURE: NO QUESTIONS WERE ASKED

---

After years of inquiries, the US Federal Bureau of Investigation finally concluded that the anthrax powder letters that killed five people in 2001 were sent by a civilian scientist who had access to the deadly bacteria through his work at a US military laboratory at Fort Detrick, Maryland.

Investigations proved that the person in question had a long history of mental instability and had spent time in a psychiatric hospital just a few months before the anthrax letters were sent. In the months before these attacks, he had apparently felt that his work with a new anthrax vaccine was being threatened by funding cuts. This worsened his condition.





No screening process prevented him from being hired by the military; nothing restricted his access

to the anthrax spores. Inventory control at the facility was lax, and no one seemed to think this was an issue.

No one took any notice of the fact that, in September and October of 2001, the presumed attacker had begun to work very late hours in his laboratory. No questions were asked until it was too late.

The scientist was never tried for the anthrax crime. He committed suicide in 2008 before he could be charged or have the opportunity to defend himself.



# SECTION 1:

## SETTING UP A BIOSECURITY SYSTEM

---

This section suggests a general framework for a practical biosecurity system that addresses modern concerns. It introduces you to the basic concepts and structure of the system and explains how the various elements work to help prevent the intentional release of potentially dangerous biological agents.

Many of the concepts introduced here will require further explanation and illustration. To this end, Section 2 will provide a more detailed description of some of the most important biosecurity elements and tasks, while Section 3 will examine some biosecurity problems that require extra reflection.

But we will begin here with a general overview, making references to chapters in Section 2 or other parts of this book when appropriate.





## CHAPTER 1:

# THE ELEMENTS OF BIOSECURITY

*A good biosecurity system involves biosecurity legislation, a National Biosecurity Agency and systems for licensing, controls, etc. – plus an all-important biosecurity culture.*



**B**iosecurity is much more than locks on a door and a fence around a building. This chapter takes a look at all the basic elements of a good system – the laws, the administrators and the procedures, not to mention the biosecurity culture that will enable the laws and procedures to work.

### BIOSECURITY WORKS AT THREE LEVELS

---

There are three levels which must be addressed when creating a good biosecurity system: a political, an administrative and an institutional level.

**The political level** involves the national lawmakers who must live up to their international obligations (mandated by UNSCR 1540) by enacting national legislation. This will ensure that everyone in the country is measured by the same standards, and will make these standards mandatory for all.

**The administrative level** involves the creation of a dedicated, government-established National Biosecurity Agency whose licensing activities will ensure compliance with biosecurity laws and executive orders. Among many other things, the Agency must also be responsible for biosecurity education and awareness-raising.

**The institutional level** involves all the research institutes, universities, private companies, hospitals, diagnostic laboratories, retailers, distributors and other facilities that use or handle biological substances or related materials.

For the sake of simplicity, we will in this book consistently refer to the above entities as ‘facilities’. Different types of facilities will have different



biosecurity requirements, but all must comply with the biosecurity regulations that apply to them.

### A BIOSECURITY SYSTEM CONTAINS MANY ELEMENTS

In addition to biosecurity legislation and a National Biosecurity Agency, an effective biosecurity system should contain the following elements:

**A control list** of all biological substances and related materials that need to be regulated. This list should be incorporated into the Biosecurity Law and regularly updated by the National Biosecurity Agency.

**A system of licensing and auditing** for facilities that wish to handle, use or store biological substances and related materials.

**Trained Biosecurity Officers** who are responsible for implementing and maintaining biosecurity at the various facilities.

**Vulnerability assessments and security plans** that address sensitive areas and issues at the various facilities.

**Security procedures and physical security systems** to protect sensitive materials. Such security could include fences, cameras, alarm systems, etc. as well as procedures for employee screening, inventory control, etc.

**Reporting systems** to effectively record all relevant changes in inventory, staff, leadership, access privileges, storage facilities, building usage, etc. that relate to biological substances and related materials.



**Biopreparedness plans** to deal with biosecurity failures.

We will deal with each of the above elements in much more detail later in this book.

### THE MOST ESSENTIAL ELEMENT: BIOSECURITY CULTURE

---

No biosecurity system, laws or procedure will work if it isn't taken seriously by the people who must live with it. This is the essence of biosecurity culture: a respect for the letter and spirit of biosecurity laws and procedures, and an understanding of why they are necessary.

Every recommendation in this book depends on a good biosecurity culture to make them work. For this reason, we have devoted an entire chapter to this subject.

**See Chapter 17, 'Biosecurity culture and bioethics'.**

At this point, however, we will note that every biosecurity player – the lawmaker, the administrator and the facility – must act and interact within the framework of a good biosecurity culture. Lawmakers who do not respect the need for biosecurity will create an ineffective law, and agencies without respect for the law will not enforce it properly.

And of course facilities that do not understand or respect the law will not abide by it – especially if they sense the same lack of respect in the enforcing Agency.



## THE SCIENTIFIC COMMUNITY MUST BE COMMITTED TO BIOSECURITY

---

There is one group of players whose commitment to biosecurity is key: the scientific community. By 'community' we refer to a group that is much broader than the researchers, technicians and students who work directly with biological substances and related materials.

This community is an interconnected network that also includes the publishers and readers of scientific journals, the members of relevant scientific and industrial organisations, the funding agencies, universities and opinion leaders who in one way or another affect scientific development.

Their commitment to a responsible biosecurity culture must lead the way. Without their public example, the law has no credibility and the procedures have no strength.

At the end of the day, the community's commitment to a rational control of scientific endeavor will not hinder their work; on the contrary, it will actually ensure continued public support and protect their work. We will expand on this topic in Chapter 3, 'Creating a new Biosecurity Law'.

## BIOSECURITY EDUCATION IS ESSENTIAL

---

To ensure a good biosecurity culture, education is essential. This training begins at the administrative level with the employees of the National Biosecurity Agency, who must be properly prepared to advise biosecurity lawmakers at the political level



while also enforcing the law and explaining it to others. Agency staff must also be prepared to train Biosecurity Officers and conduct external educational activities.

At the institutional level, the Biosecurity Officer will be responsible for providing an appropriate level of biosecurity training to his or her colleagues. This training should include an explanation of applicable laws and procedures as well as the reasoning behind them.

The training should also include an explanation of how the individual employee can personally contribute to the biosecurity culture of the facility. When it comes to biosecurity, no one should be in doubt as to their roles and responsibilities.

The interplay between education and lawmaking is illustrated in fig. 2 on the page opposite.

### A TIMELINE FOR YOUR BIOSECURITY SYSTEM

A completely new biosecurity system takes time to establish. As shown in the timeline beginning on page 26, it can take roughly six months just to complete the initial gap analysis that will reveal the specific biosecurity needs of your country.

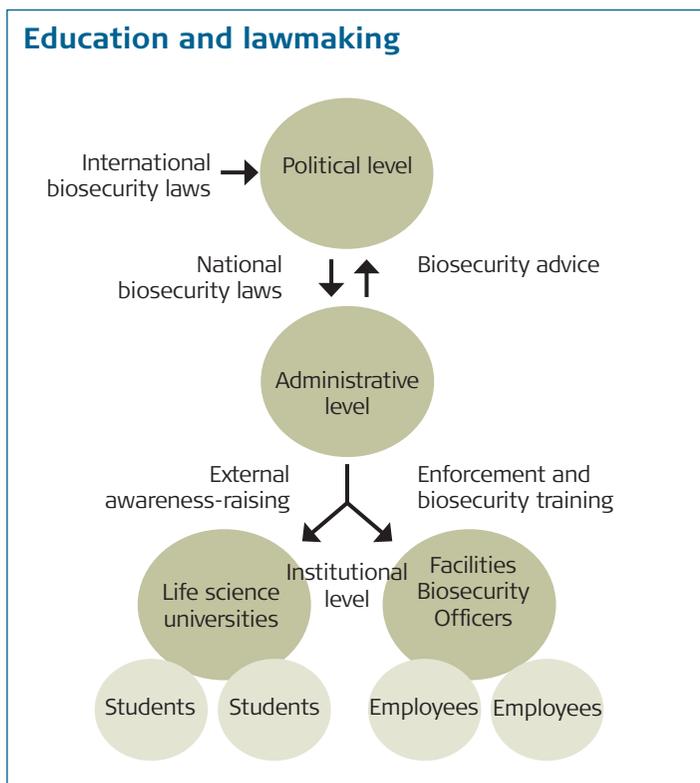
Enacting the necessary laws, establishing the National Biosecurity Agency and preparing the required working documents can also be a time-consuming process. Staff for the Agency must also be recruited and trained.

But the result of all this hard work should be well worth the effort. Once the system is up and run-



ning, it will serve your country well and make an important contribution to worldwide biosecurity.

The next few chapters will give you a more detailed overview of what needs to be done. The structure of these chapters will follow the structure of the timeline presented on page 26-27.



**Fig. 2:** To ensure effective laws that will be understood and respected, biosecurity education and awareness raising must go hand in hand with lawmaking.

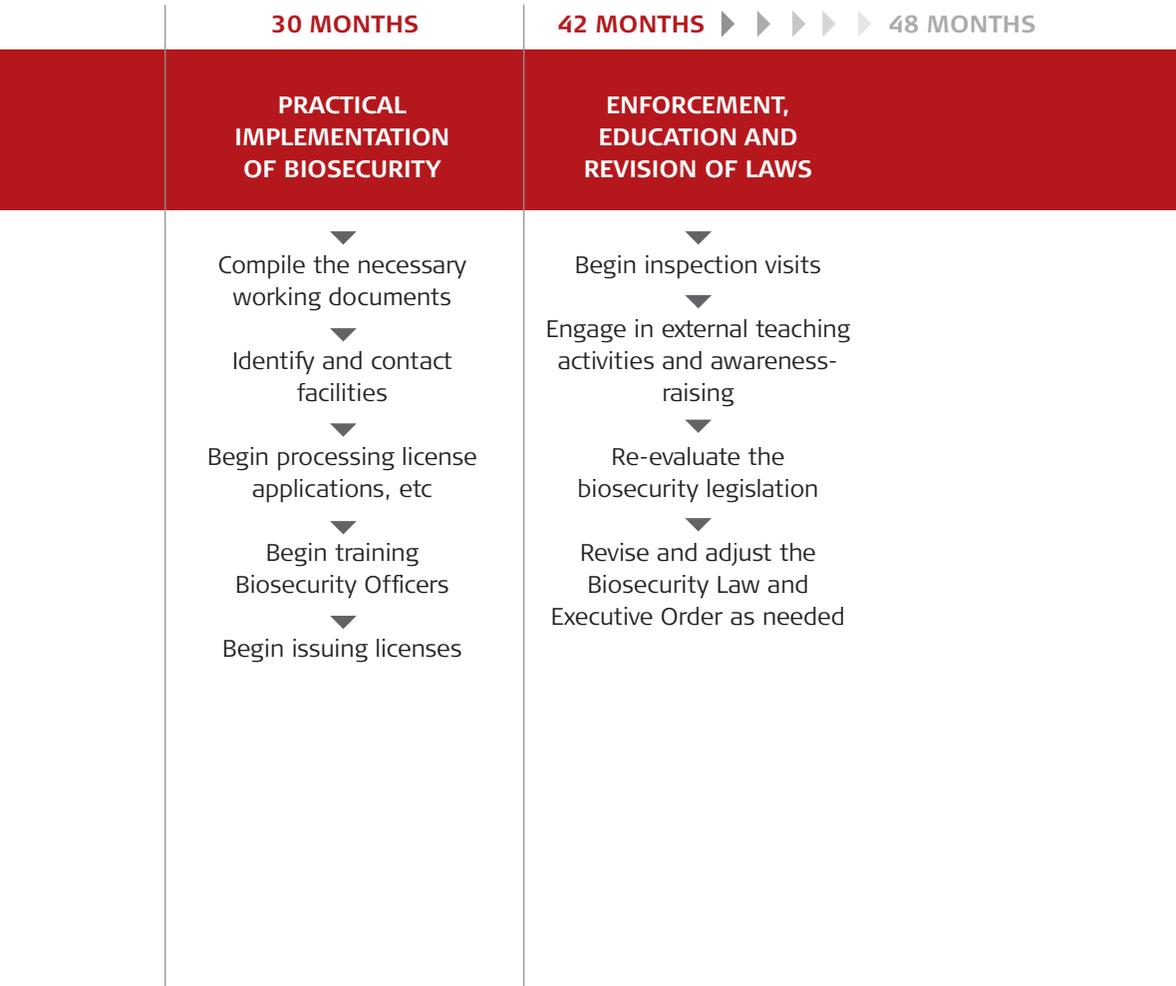


# TIMELINE FOR A NEW BIOSECURITY SYSTEM

<p><b>START</b></p> <p><b>INITIAL GAP ANALYSIS</b></p>	<p><b>6 MONTHS</b></p> <p><b>PREPARING A BIOSECURITY LAW</b></p>	<p><b>18 MONTHS</b></p> <p><b>ESTABLISHING A NATIONAL BIOSECURITY AGENCY</b></p>
<p>▼</p> <p>Assess the current state of biosecurity</p> <p>▼</p> <p>Secure input from relevant stakeholders</p> <p>▼</p> <p>Identify specific national biosecurity needs</p>	<p>▼</p> <p>Clarify which governmental body will be responsible for biosecurity</p> <p>▼</p> <p>Evaluate existing legislation that relates to biosecurity; resolve potential conflicts and overlaps</p> <p>▼</p> <p>Secure input from relevant stakeholders</p> <p>▼</p> <p>Compile a control list</p> <p>▼</p> <p>Enact the necessary Biosecurity Law</p>	<p>▼</p> <p>Establish the Agency</p> <p>▼</p> <p>Recruit staff</p> <p>▼</p> <p>Train staff</p> <p>▼</p> <p>Prepare a detailed Executive Order describing Agency responsibilities and tasks</p> <p>▼</p> <p>Establish a home page</p> <p>▼</p> <p>Inform stakeholders about the Agency</p>



**The timeline** shows a chronological list of the tasks which must be completed in order to achieve a fully functional biosecurity system. As shown in the time sequence, it will take about four years before the system is completely operational.





## CHAPTER 2:

# PREPARING A GAP ANALYSIS

*In order to create an effective Biosecurity Law, you must first assess the existing state of biosecurity in your country. This will pave the way for new legislation – and hopefully also for a positive relationship with the facilities.*



**B**ack in 2006, a Danish group of researchers made some disturbing discoveries about the state of biosecurity in Scandinavia.

In two separate studies – one of the Nordic countries in general and another of Denmark in particular – it was found that there was very little internal security at the laboratories where dual-use biological substances were present.

Moreover, backgrounds and identities of employees (potential ‘insiders’) were rarely checked. Gaining access to pathogen inventory lists would be relatively easy for any of them, and the same was true of the freezers in which the pathogens were stored. And if anything were ever stolen from those freezers, the theft might not even be discovered: fully 81% of the pathogen-containing facilities in Scandinavia had no routine inventory control<sup>1</sup>.

The surveys showed a number of other surprising results as well.

**See box** on the page opposite, ‘Private companies had the best biosecurity’.

### A GAP ANALYSIS IS A POWERFUL ARGUMENT

The above gap analysis marked the beginning of a lawmaking process that ended with a new Danish Biosecurity Law in 2008 and a Biosecurity Executive Order in 2009. The analysis identified a number of issues in Denmark that urgently needed to be addressed, and it served as a powerful argument in favor of the law.



## PRIVATE COMPANIES HAD THE BEST BIOSECURITY

Auditors working on the 2006 gap analysis of 22 Danish facilities discovered that private pharmaceutical companies were in better shape than public facilities when it came to biosecurity.

According to their analysis, private companies tended to have explicit policies on safety and security in order to comply with standards for good corporate governance. Meanwhile, the study noted, "some of the overall least secured facilities were public."

All the private pharmaceutical companies checked the background of their staff before employment, while none of the public facilities did so. On the other hand, there was not a single facility, public or private, that checked the background of the auditor who visited their facility and was granted access to sensitive areas.

And none of the facilities visited by the auditors came anywhere near to achieving a perfect biosecurity score.

Broadly speaking, a gap analysis should reveal biosecurity strengths and weaknesses and identify the specific biosecurity needs of your country. Among other things, your national gap analysis should uncover:

- the size of the community that works with biological substances and related materials
- the types of facilities that are involved



- the types of biological substances and related materials they work with
- the effectiveness of their biosecurity systems
- their most pressing biosecurity issues

When properly done, your gap analysis should be a convincing document – not only for lawmakers and the general public, but for the facilities that need to improve their biosecurity measures.

### MAKE A LIST OF RELEVANT FACILITIES

You should begin your gap analysis by identifying as many relevant research facilities, pharmaceutical and biotech companies, hospitals, diagnostic laboratories, universities, etc. as possible. By 'relevant', we mean public and private facilities that you believe may be working with biological substances and/or related materials.

Your list must also include relevant manufacturers, retailers, suppliers and distributors. Not to mention 'foreign' facilities that operate within your borders but whose official address and perhaps even their storage facilities are located in another country.

Facilities for the Danish gap analysis were identified partly through a web search and partly through personal communication with more than 50 researchers at key public and private research and production facilities.

### THE LIST OF FACILITIES WILL BE EXTREMELY USEFUL

Drawing up a list that includes practically every relevant facility in your country will take time. But the data in it will be extremely useful.



By giving you an idea of how many relevant facilities there are in your country, your list will help you to determine the size and cost of the Agency that will administer the law. Later, you will need this list again, when the time comes to seek stakeholder input for the proposed Biosecurity Law.

And the contact information in this list will of course be indispensable once the law is enacted; after that, your National Biosecurity Agency will need to communicate regularly with most of these facilities.

Your list should be updated whenever new, relevant facilities are established or brought to your attention. One way to identify 'new' facilities is through the transactions they have with other laboratories, retailers, etc.

### USE A QUESTIONNAIRE TO GATHER INFORMATION

To get an overview of existing biosecurity in your country, each facility on your list should be sent a biosecurity questionnaire. Not all will respond – and of those who do, some will probably fall outside the scope of biosecurity regulation. But there will no doubt be enough response to give you a general idea of the level of biosecurity.

Among many other things, it is important at this point to ask what sort of substances and materials these facilities work with. This will provide an idea of which biological substances and related materials are present in your country and help you to assess your country's biosecurity needs.

There are many other questions that should be asked – questions about physical security, employee screening and biosecurity culture, to name a few.



**You will find** a list of suggested questions on the CBB website.

### SOME OF THE FACILITIES SHOULD ALSO BE VISITED

In the study that provided Denmark with its gap analysis<sup>2</sup>, questionnaires were sent to facilities all over Scandinavia. This was followed up by the specific Danish survey, in which physical visits were made to 22 Danish facilities (representing 61% of those who were invited to participate) with a total of 94 laboratories.

These visits were an important supplement to the information received in writing through the questionnaires.

**See page 36**, 'Lessons learned: Questionnaires are not enough'.

During their visits to the facilities, the auditors from the Danish Centre for Biosecurity and Bio-preparedness had their own list of questions that were asked on-site. As with the suggested list of questions for the questionnaire.

**You will find** this list of on-site questions on the CBB website.

### MANY FACILITIES WELCOMED OUR VISIT

It may surprise some readers that our initial contacts with the various facilities in Denmark were often welcomed.

Rather than regarding the coming Biosecurity Law



as an annoyance or a hindrance to their work, many were actually glad that an organisation was finally being established that could help protect their research and biological material from unauthorised use. Some facilities had in fact already had some unpleasant experiences in this regard.

In our conversations with the facilities, we heard several accounts of suspicious phone calls from persons seeking access to sensitive knowledge or substances. These experiences underscored the need felt by the facilities for an expert partner that could help improve their biosecurity.

### GOOD COMMUNICATION IS KEY

---

Establishing a positive relationship with the facilities is vital to the success of a biosecurity system. This relationship begins with the initial gap analysis visits and should continue for as long as the facilities and the law continue to exist.

During the gap analysis phase, good communication with the facilities will not only facilitate getting the information you need. It will also provide the facilities with an 'early warning' that a new law is on the way, and will thus enable them prepare for it.

This, in turn, should enhance the credibility of the biosecurity authority and lay the groundwork for a fruitful, long-term collaboration. The facilities will only confide biosecurity-related problems to the Agency – and enable it to assist them – if they perceive it as being reasonable and co-operative.

Facilities must also be able to rely on the discretion of the Agency when it comes to trade secrets



and proprietary knowledge. Good communication cannot take place if the facility fears that its non-public business information could be compromised.

As you will see in the chapters to come, communication with stakeholders will be a major theme throughout this book. Its importance can never be underestimated.

### **Lessons learned:**

#### QUESTIONNAIRES ARE NOT ENOUGH

---

In our experience, the answers provided in a written questionnaire or printed form can differ greatly from the physical reality of on-site biosecurity. A facility may think it already has adequate biosecurity, but a trained inspector may have a different view of what needs to be done.

During CBB inspection visits, we have found that there is almost always some material present on-site for which a license should have been sought. This is especially true of related materials whose specifications can be difficult to understand.

It is therefore always best to supplement written responses with an on-site visit.

---

**1** Kristian H. Bork et.al., *Biosecurity in Scandinavia* (Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science, vol.5 nr.1, 2007) 62. Both studies were described in this article.

---

**2** Bork et.al., *Biosecurity in Scandinavia*, 62-71

---







## CHAPTER 3:

# CREATING A BIOSECURITY LAW

*The Biosecurity Law is the legal foundation upon which a comprehensive biosecurity system can be built.*



**P**aradoxically, one of the first things to think about when drafting biosecurity legislation is how to avoid over-regulation. Unnecessary and unreasonable rules will undermine credibility and respect for the law. Over-regulation can also overburden the Agency with a jungle of rules that defeat their own purpose because they are impossible to administer effectively.

On the other hand, laws that are not strict enough can of course create unacceptable biosecurity risks. A careless attitude towards risk can also affect public trust and even create a political backlash that could hinder the progress of legitimate scientific activity.

**See box** on page 47: 'A case of broken trust'.

## BIOSECURITY CAN PROTECT SCIENTIFIC DEVELOPMENT

---

Finding the right balance between biosecurity needs and legitimate scientific freedom is key to the success of your legislation.

The central goal of biosecurity legislation should be to protect potentially dangerous biological substances and related materials from theft and misuse. This in turn will prevent legitimate research materials from being used in a weapon of mass destruction.

At the same time, biosecurity legislation should create an atmosphere of public trust in which the scientific community can freely exploit needed resources and pursue legitimate technological development (see fig. 3 on next page).





**Fig. 3:** Protecting scientific materials and knowledge from abuse has a threefold benefit.

### FACILITIES MUST BE PREPARED FOR THE NEW LAW

To create 'reasonable' biosecurity legislation and administer it in a balanced manner, it is important to remember that the facilities will need to be prepared for the new law.

This means that they must be informed of the legislation in good time before it goes into effect. In addition, the Agency should do all it can to help them make any necessary changes that will enable them to comply with the law.

A good way to prepare the facilities for the new legislation is to include them in the legislative process (see the section 'relevant stakeholders').

### EXISTING LAWS CAN HARMONISE OR CLASH WITH BIOSECURITY

The next step in the legislation process should be to make a survey of existing laws and regulations that may touch on the area of biosecurity.



One reason to examine existing legislation is that some biosecurity needs may already be addressed by other laws. For example, there may be a law about the transportation of dangerous goods that adequately covers the need for security while transporting controlled biological substances and related materials.

Another reason for taking a close look at existing laws is the fact that some laws and regulations may actually conflict with the Biosecurity Law you wish to enact. Different administrative entities sometimes have conflicting agendas and interests, and these conflicts must be resolved before the final Biosecurity Law goes into force.

Health and safety regulations, for example, might require biohazard warning signs in areas where hazardous materials are stored. From a biosecurity standpoint, however, such a sign also tells a potential thief of the location of these materials. Fire safety regulations may also conflict with biosecurity needs.

**We will return** to this issue in Chapter 16, 'Preparing and conducting an inspection visit'.

### A DEDICATED BIOSECURITY LAW IS PREFERABLE TO 'ADD-ON' LEGISLATION

---

Next, you will need to decide whether to build your biosecurity legislation around existing laws or draft an entirely new and dedicated Biosecurity Law. Some countries have chosen to build on existing legislation.

Based on our own experience, however, we recom-



mend creating an entirely new and comprehensive law. We believe that specific biosecurity legislation creates a better focus on the issue of biosecurity and avoids conflicts between parties with differing interests.

Adding biosecurity regulations to a variety of other safety and security systems can, on the other hand, create a bureaucratic nightmare of add-on agencies and personnel groups that may find it difficult or impossible to work together towards a common goal.



### THE BIOSECURITY LAW CREATES A LEGAL FOUNDATION

---

The Biosecurity Law that we recommend will create a basic legal foundation upon which your biosecurity system can be built. It should accomplish the following:

- Clarify which governmental body is to be responsible for biosecurity. Depending on the needs of your country, this could, for example, be the Ministry of Defense, the Department of State, the Ministry of Health or some other relevant entity.

**See page 45, 'Lessons learned: Finding the right Ministry can take time'.**

- Provide for the establishment of a National Biosecurity Agency that reports to the chosen Ministry and is responsible for biosecurity.
- Authorise the Agency to administer the law, ensure compliance and issue further national rules and guidelines for biosecurity.
- Determine the penalties for breaking biosecurity laws.



- Establish an appeals process for decisions made by the Agency.

**You will find** an English-language version of the Danish Biosecurity Law on the CBB website.

## THE LAW SHOULD BE SUPPLEMENTED WITH AN EXECUTIVE ORDER

---

A Biosecurity Law such as the one described above will be a relatively short document that cannot stand alone. It must be supplemented with the specific national rules and guidelines that the Agency has been authorised to create. Once these guidelines have been drafted by the Agency, they should be issued as an Executive Order by the relevant Ministry.

This kind of two-tiered system has two major advantages. For one thing, it allows expert advisors from the National Biosecurity Agency to draft specific regulations that require specialised knowledge and experience.

It also allows greater flexibility: Executive Orders from a government Ministry can be implemented immediately, without a lengthy political process, and can thus also be quickly revised and updated in response to new developments and biosecurity challenges.

**We will expand** on the content of the Executive Order in Chapter 4, 'Creating a Biosecurity Agency and an Executive Order'.



**Lessons learned:****FINDING THE RIGHT MINISTRY CAN TAKE TIME**

---

Deciding which Ministry should bear the responsibility for biosecurity sounds deceptively simple. In our experience, however, it proved to be exceptionally time-consuming. Several government entities were interested in the task, and there were many discussions about which one to choose.

The lesson here is that such discussions are to be expected, and it is necessary to allow enough time for them. Remember too, that regardless of which Ministry or other entity assumes the official responsibility, the expertise and cooperation from other entities will be needed in order to adequately regulate the many issues that relate to biosecurity.

**ALL RELEVANT STAKEHOLDERS SHOULD BE INVOLVED IN THE LAWMAKING PROCESS**

---

As with all other biosecurity endeavors, good communication and stakeholder dialogue is essential during the lawmaking process. This means that all relevant stakeholders should be invited to provide input and suggestions regarding the new law.

Including your stakeholders in the legislation process will increase their respect for the law once it is enacted. And of course many of them will have specific and practical knowledge that will help ensure that all relevant issues are addressed.

Stakeholder participation could, for example, be accomplished by holding public hearings to which



relevant persons have been invited; one-on-one meetings could also be arranged. Another way to gain stakeholder participation is to send them a draft of the law before it is enacted and ask for written comments and feedback.

The list of relevant stakeholders could be quite long; in Denmark, a total of 48 entities were invited to provide input. Your list of stakeholders could, for example, include representatives from:

- facilities that will be subject to biosecurity regulation
- relevant industry and trade associations
- environmental groups
- the military or other institutions with bioweapons knowledge
- political parties
- educational institutions within the life sciences
- relevant Ministries  
(in practice, nearly all of them)
- agencies that administer related laws
- police and emergency services
- local and regional governments
- research funding foundations
- scientific academies
- publishers of scientific articles

### STAKEHOLDERS CAN BE CONSULTED MANY TIMES

Stakeholder participation is useful in many other biosecurity contexts. It will, for example, be extremely valuable when the time comes to draft the Executive Order. As you will see in the next chapters, the Executive Order is a longer and more detailed document than the Law and will therefore probably generate a greater amount of stakeholder input.



## A CASE OF BROKEN TRUST

---

A classic example of how public opinion can affect industrial and scientific endeavors is that of genetically modified organisms (GMOs). Especially in the 1980s and 90s, European wariness of gene technology resulted in public protests and political restrictions on the marketing of genetically modified foodstuffs.

This attitude also seems to have affected scientific progress. In 1997 – the year that a lamb with human genes was developed by a British genetic engineering company – only 5,000 licenses to conduct GMO experiments were issued within the European Union. In contrast, 20,000 licenses were issued that year in the US, where there was a much broader public acceptance of gene technology.

Much of the European GMO skepticism has been attributed to the failure of the British government and the European Commission to adequately restrict the sale of British beef during the 'mad cow disease' scandal of the 1990s. Quite simply, the public had lost confidence in government regulation; trust had been broken.

---

### **Sources:**

Gyldendal og Politikens Danmarkshistorie, *Begejstring og angst*, (2nd edition, 2002-2005)

Diahanna Lynch and David Vogel, *The Regulation of GMOs in Europe and the United States: A Case-Study of Contemporary European Regulatory Politics* (Council on Foreign Relations Press, 5 April 2001)

---





## CHAPTER 4:

# CREATING A BIOSECURITY AGENCY AND AN EXECUTIVE ORDER

*The next step towards a complete biosecurity system is to hire the right staff for your National Biosecurity Agency. At the same time, an Executive Order must be created that includes a control list and spells out how the Agency must perform its duties.*



**W**hen the Biosecurity Law is in place, it is time to begin establishing the National Biosecurity Agency that has been given the power to administer the Law, ensure enforcement and issue additional guidelines and regulations.

You will also need to create an Executive Order that supplements the Biosecurity Law with more specific requirements, regulations and descriptions of duties. It makes sense to involve the Agency in the drafting of this Order, so you will need to hire at least some Agency personnel before the Order can be written.

### THE AGENCY SHOULD NOT JUST BE A 'POLICEMAN'

As we have already indicated in previous chapters, the Agency must be more than a 'policeman'. Enforcement activities are of course important, but the Agency has many other crucial tasks.

Broadly speaking, the Agency should regard itself as a partner that can help and advise the facilities on how to live up to biosecurity standards. This requires specialised knowledge and a willingness to share this knowledge in an open and friendly manner.

In our experience, openness on the part of the Agency will be met with openness on the part of the facilities. They must feel that it is 'safe' to share any security problems – especially if they involve trade secrets – and seek help on how to address these issues.

Remember: at the end of the day, all Agency interaction with the facilities is based on a common interest in preventing security breaches, biologi-



cal warfare and bioterrorism – not to mention the continued and fruitful exploitation of legitimate science.

### AGENCY STAFF MUST HAVE A MIX OF SPECIALISED COMPETENCES

---

The first order of business when establishing the Agency will be to recruit the necessary staff. In this context, it is important to remember that, ideally, the Agency should be able to gather every aspect of biosecurity expertise in a single location.

This requires a staff with a broad range of competences in the areas of health, bioscience, microbiology, public administration, biopreparedness, related materials and process technology. It would also be an advantage to include persons with teaching experience.

We strongly believe that Agency competencies should also include the ability to ‘think like the enemy’.

**See page 52, ‘Lessons learned: Knowledge of biological weaponry is vital’.**

### STAFF NEEDS: ACADEMICS, CASEWORKERS AND RECEPTION/CLERICAL

---

The main tasks of the Agency will include case handling, inspection visits, biosecurity training, external outreach activities, personnel administration and other types of administrative support. The Agency will also spend much time drafting the Biosecurity Executive Order and other new biosecurity regulations and procedures.



**Lessons learned:****KNOWLEDGE OF BIOLOGICAL WEAPONRY IS VITAL**

---

We believe it is vital to have at least one biosecurity expert at the Agency who has specialised knowledge of biological weaponry. Otherwise, the Agency will not be fully able to anticipate how such weapons can be created and misused with the help of 'innocent' materials.

In other words, the Agency must be able to 'think like the enemy'.

There are not many people in the world who have this particular proficiency. The right person will most likely need special training and/or expert advice, possibly from sources in the military.

To perform these tasks, Agency staff should include:

- academics with the competences described above
- caseworkers with practical experience in the field of public administration
- reception and clerical staff

**NEARLY EVERYONE WILL WORK WITH PUBLIC ADMINISTRATION**

---

Many of the job functions mentioned above will be intertwined, so most Agency personnel should be able to perform more than one of these tasks.

Public administration is at the heart of the work done by any government agency, so practically everyone at the Agency will need this type of



knowledge – regardless of whether the task at hand involves issuing a license, performing an inspection visit, responding to a telephone query or conducting some other type of Agency business.

It is possible to teach the basics of biosecurity to a caseworker who does not have a background in the natural sciences. Depending on the situation you may, on the other hand, find it is a better solution to hire persons with a relevant biological background and then train them to be competent caseworkers.

### ACADEMIC EDUCATION IS IMPORTANT FOR CREDIBILITY

---

When interacting with personnel at the facilities, Agency staff will often be met with highly-educated experts in fields such as medicine and bio-science.

We have found that, to ensure credibility, it is important that at least some of the Agency personnel with whom the facilities meet have an equivalent education (preferably at PhD level) within the areas of health and bioscience. To understand the problems faced by the facilities, Agency staff must have a detailed understanding of laboratory work.

### AGENCY EXPERTISE MUST BE CONSTANTLY UPDATED

---

It is also extremely important that the relevant Agency employees are able to stay abreast of new biosecurity developments. As the national experts on biosecurity, they must be provided with the training and constantly-updated information that will keep them informed of all new technologies, trends, biosecurity threats and other challenges.



## THE ELEMENTS OF THE EXECUTIVE ORDER

---

The first big job for Agency staff, once it has been hired, is to create the Executive Order that will describe its work with the facilities in detail. The Order will be approved and issued by the relevant government Minister, but the Agency will in practice often do the actual drafting.

The Executive Order should contain:

- a control list of all biological substances (and related materials, if relevant in your country) that must be regulated by the Agency
- licensing requirements for the above materials, including vulnerability assessments and security plans
- requirements for inventory control, transport and disposal of the above materials
- requirements for reporting accidents, thefts, misuse and losses related to the above materials
- requirements for physical security and biosecurity procedures
- requirements for a Biosecurity Officer at each relevant facility
- requirements for informing the Agency about important staffing and security-related changes
- a provision that allows the Agency to create additional biosecurity regulations that are not part of the Executive Order

Since the Executive Order contains many more requirements and guidelines than the Biosecurity Law, you may also want to include more details about penalties and appeals process as they relate to the various elements listed above.



## REGULATIONS CAN ALWAYS BE ADDED OR UPDATED

---

We will expand on many of the elements in the Executive Order in this and later chapters. At this point, however, it's important to remember that your own experiences with biosecurity work will over time give rise to revisions and additions.

As previously mentioned, an Executive Order can be quickly updated to reflect new challenges, ideas, developments and feedback. Remember too that the Executive Order should empower the Agency to create new biosecurity-related requirements that are not part of the Order itself.

Once the Order is implemented, a great deal of Agency time will in fact be spent on creating very specific biosecurity regulations and procedures for the individual facilities.

**See page 63, 'Lessons learned:**  
The intent of the Order must be 'translated'.

## THE AUSTRALIA GROUP CAN PROVIDE A GOOD CONTROL LIST

---

An absolutely crucial part of the Executive Order is the control list, which forms the basis of nearly all other biosecurity regulations. It must name all the relevant biological substances that must be regulated and kept secure in order to prevent theft and malicious misuse. Related materials that are to be controlled should also be specifically named in the control list.



The so-called Australia Group has generated a good export control list that is used by many countries. It was designed to fight the cross-border spread of both chemical and biological weapons, but the biological portion of the list is equally well-suited for national biosecurity control.

The Australia Group list includes all relevant human, animal and plant pathogens and toxins. It also includes dual-use biological equipment, related technology and software. The list is regularly updated to reflect new technological developments.

**You will find** the Australia Group control list and more information about the Australia Group itself at [www.australiagroup.net](http://www.australiagroup.net).

### USING AN EXISTING EXPORT CONTROL LIST CAN BE AN ADVANTAGE

---

The EU Commission regulations for export control of dual-use items are based on the Australia Group list, and so is the biosecurity control list in the Danish Biosecurity Executive Order.

Using an existing export control list for biosecurity purposes can save a lot of time and trouble, provided it has been prepared by reliable experts and is regularly updated. But it has another advantage as well.

Facilities that have export activities will already be familiar with such control lists and understand why they are necessary. They will also find it easier to handle a single list that applies to both export control and biosecurity.



## THE AGENCY SHOULD BE ABLE TO MODIFY THE CONTROL LIST

---

If the Australia Group list (or another existing export control list) is used as a model for your biosecurity control list, the Executive Order should allow the Agency to modify it for national use.

To avoid over-regulation, for example, the Agency may want to make exceptions to the control list, based on its own expert risk assessments. Such assessments could be made proactively by the Agency or in response to a request made by a facility. Exceptions could, for example, include less virulent strains of certain bacteria.

The Agency may also want to add new elements to the control list. In Denmark, for example, the national Agency found that spray driers used by the pharmaceutical industry have dual-use potential and successfully argued for their inclusion in the Australia Group list.

## DRAWING UP YOUR OWN CONTROL LIST REQUIRES CAREFUL THOUGHT

---

The Australia Group does not allow member countries to make additions to its control list without an extensive approval process.

If your country chooses to make its own control list without being a member of the Group – or if it is a member of the Group and wishes to suggest an addition – there are a number of factors to be considered.

Among other things, the Agency should ask itself



whether the biological substance or related material in question:

- is well-suited for use as a weapon
- is suspected of having been previously used in a biological attack
- could cause serious damage to humans, animals, plants or the environment

The lack of a readily-available and effective treatment for a particular biological agent would be an additional argument in favour of inclusion in the control list. At the same time, however, the Agency should consider whether control of the material in question is practically feasible, and whether control measures could be expected to hinder its use as a weapon.

### MUCH OF THE EXECUTIVE ORDER WILL RELATE TO THE CONTROL LIST

---

With the control list as a foundation, some of the other elements of the Executive Order can now be addressed.

Licensing requirements must be created for working with the substances and materials on the control list. Requirements for physical security, inventory control, and the transport and disposal of controlled materials will apply to the control list items, as will the requirements for reporting accidents, theft, loss and misuse of these materials.

Creating these requirements will require a good deal of thought, because the facilities to which they will apply are so varied. Diagnostic facilities that are only in possession of controlled biological substances for a very short period of time will, for



example, have different requirements for inventory reporting than large research facilities with very large, permanent inventories of controlled substances and related materials.

Physical security requirements can also vary greatly, depending on such things as the facility's placement, floor plan and the types of materials with which it works.

### AVOID A 'ONE SIZE FITS ALL' APPROACH

The above instances are just a few examples of how requirements for licensing, control and reporting must allow for a variety of circumstances. In practice, this can be done by creating a set of application, control and reporting forms with blanks that can be filled out or left empty, depending on the type of facility. We will deal with license application forms and other types of working documents in Chapter 5.

Based on the answers provided in the application form, the Agency can then design a series of biosecurity requirements that are tailored to the exact needs of a given facility. This will be particularly relevant for physical security.

**You will find** much more on this subject in Chapters 11 and 12, both of which deal with various aspects of physical security.

Creating and administering such a licensing system can become very complex, and we will return to this subject several times, both in this section and Section 2. But it is precisely the complexity – or rather, the flexibility – of the system that makes it possible to avoid under- and over-regulation.



A 'one size fits all' approach will either create frustration among the facilities that are over-regulated, or it will create loopholes for the facilities that are under-regulated. Either way, respect for biosecurity regulations will be undermined.

### HOW TO FIND THE RIGHT LEGAL WORDINGS

---

To address the above-mentioned complexities in the Executive Order, you will need to create a legal wording that allows for a good deal of flexibility.

The Danish Executive Order can provide you with an example of how these and other general biosecurity requirements can be expressed.

**You will find** an English-language version of this Order on the CBB website, where you will also find a variety of sample forms and guidelines for how to fill them out.

### RULES FOR BIOSECURITY OFFICERS AND SECURITY CHANGES

---

As indicated earlier in this chapter, your Executive Order should also provide for the naming of at least one Biosecurity Officer at each facility. This is a very important function that will be dealt with in detail in Chapter 15, 'The work of Biosecurity Officers'.

The Order should also require that the Agency be informed of relevant changes in staffing (e.g. new Biosecurity Officers), security procedures, physical security, etc. These subjects will also be dealt with in more detail in subsequent chapters.

Again, you can refer to the Danish Executive Order



to see how these subjects were addressed in legal terms. But before you begin to copy this document word for word, there is one more thing to remember: your stakeholders. Their input will help you create an Executive Order that is truly attuned to the needs of your country.

### KEEP YOUR STAKEHOLDERS IN THE LOOP

---

As with the Biosecurity Law, stakeholder participation is an important part of drafting the Executive Order. Not least because the Order is a more detailed document than the Law and will no doubt have many more practical consequences for the facilities. Input can be secured in much the same way as described for the Biosecurity Law in Chapter 3.

Stakeholders who participate in the drafting of the Executive Order will of course be aware that new biosecurity requirements are being prepared. Once the Order is finished, however, an extra effort should be made to ensure that everyone knows about it.

### ORGANISE AN INFORMATION 'ROAD SHOW'

---

Informing your stakeholder could, for example, be accomplished by inviting relevant facilities and other stakeholders to a series of information 'road shows' at various locations in your country. Many of the facilities may be willing to offer their own premises as a venue for such a presentation.

An information tour of this kind gives the new Agency the opportunity to present itself 'in person'. At the same time, the Agency's future associates will have the opportunity to listen and



ask questions about the new Executive Order and discover how it applies to them.

### IT'S TIME TO PREPARE A WEBSITE

---

Stakeholders can also be kept in the loop with the help of a website – and now is also the time to create it.

Apart from contact information and an introduction to the Agency, the site should include information about the application process and the purpose and procedures of an inspection visit. Sections for biosecurity news, information for Biosecurity Officers and information about Agency training courses should also be created.

In addition, the site should provide a description of the content and purpose of your country's biosecurity legislation, along with a link to the full text of this legislation (including the control list). Necessary application forms should be downloadable from the website.

**For more inspiration**, you can take a look at the general contents and layout of the CBB website.

And now your National Biosecurity Agency is nearly ready to implement its regulation and training activities. But first there are some working documents to prepare.



**Lessons learned:****THE INTENT OF THE ORDER MUST BE  
'TRANSLATED'**

---

The Executive Order is meant to be a relatively detailed document – but it is still just a guideline. It's up to the Agency to create the facility-specific requirements that will ensure compliance with the general requirements of the Order.

In Denmark, we found that once our Executive Order was implemented, a very large part of the Agency's work – perhaps even the majority of its work – now consists of 'translating' the intent of the Order into specific regulations that ensure adequate and consistent biosecurity at each individual facility.

Especially in the beginning, this work can involve quite a bit of research. To determine appropriate levels of biosecurity, for example, the Danish Agency spent much time investigating the requirements used by other agencies in such areas as nuclear and chemical security.





## CHAPTER 5:

# PRACTICAL IMPLEMENTATION OF BIOSECURITY

*Having prepared the legal groundwork, the Agency can now create its working documents and begin such tasks as processing license applications and issuing licenses.*



Once the National Biosecurity Agency is up and running, it must ensure that every facility in the country lives up to the Biosecurity Law and Executive Order.

Among other things, this means that any facility that works with controlled materials must have an appropriate license. To receive this license, the facility must apply to the Agency and prove that it can live up to acceptable biosecurity standards.

### THE AGENCY WILL NEED MANY WORKING DOCUMENTS

---

In order to perform its licensing and other duties, however, the Agency must first create the necessary working documents. In keeping with the requirements of the Executive Order, these documents should include:

- license application forms
- Vulnerability Assessment and Security Plan forms
- forms for reporting the purchase, sale, transfer or destruction of controlled biological substances and related materials
- forms for reporting changes to the license
- year-end inventory reporting forms
- inventory forms for controlled biological substances
- inventory forms for related materials
- license templates

As noted in Chapter 4, the Executive Order should also require the naming of at least one Biosecurity Officer at each facility. The officer or officers will be named in the license application form and on the license itself, but they should also partici-



pate in a mandatory training course provided by the Agency. So a registration form for this course must also be included in the list of working documents.

### EXTRA REQUIREMENTS AND FORMS CAN BE ADDED

The Agency also has the prerogative to add other systems, procedures and requirements to the ones mandated in the Executive Order. The Danish Agency decided to add a system of personnel groups, each of which has different access privileges to controlled biological substances.

This system necessitated an extra reporting form – a personnel list – on which a facility must show all relevant persons and their access privileges. A separate personnel list is required for each substance that is present at the facility.

**We will describe** this system in more detail in Chapter 10, 'Employee security'.

### THEFT, ACCIDENTS AND LOSSES SHOULD BE REPORTED IMMEDIATELY

The documents mentioned above do not cover the reporting of losses (i.e. theft or misplacement) and accidents that relate to controlled materials. In the biosecurity model we recommend, the Agency should always be informed immediately of such events, and there are special procedures for this type of reporting.

**You will find** details in Chapter 14, 'Biopreparedness'.



**Lessons learned:****SHORT-TERM LICENSES MAY BE NECESSARY**

---

Ideally, a facility should not be allowed to work with controlled biological substances and related materials until it has a license from the Agency.

During the establishment phase of the biosecurity system, however, the Agency cannot expect every facility to live up to the standards of the new biosecurity legislation. Some of these facilities may have been in operation for decades without having to comply with such standards – and they should not have to cease work while implementing the measures required by the Agency.

In such cases, we recommend that the Agency issue a temporary license that is only valid for a year or so. This will allow enough time for the facilities to appoint a Biosecurity Officer and implement any new biosecurity measures, after which a longer-term license can be issued.

**WORKING DOCUMENTS CAN BE MODELED ON OUR EXAMPLES**

---

Creating these forms took a great deal of time, and much thought and discussion has gone into the process. If you choose to model your working documents on the examples we've shown, you can save much time and trouble.

**You will find** English-language examples of each of these forms on the CBB website. Examples of the application forms include a set of guidelines (also in English) designed to help the facility fill out the form in question.



## YOU MUST NOW IDENTIFY AND CONTACT RELEVANT FACILITIES

---

During the gap analysis phase described in Chapter 2, you will have identified and listed many of the facilities in your country that might need to be regulated in a comprehensive biosecurity system. You may also have contacted some or all of them in connection with a biosecurity questionnaire or through a visit to their premises.

It is now time to make a more formal identification and contact with these facilities and any others that may have come to your attention. All of them must be informed that a regulatory Agency for biosecurity has been established. All should be asked to formally state whether or not their activities should be regulated by the Agency according to the new Biosecurity Law and Executive Order.

Those who reply in the affirmative can then begin the licensing process (see below).

Some facilities may reply in the negative despite the fact that they are, in fact, working with controlled material. This will of course make them in violation of the law, a fact which will be discovered in due course – for example when the sale of a controlled substance to the facility is reported to the Agency by the retailer, as required by the law.

## LICENSE APPLICATIONS ARE PROCESSED BY A CASEWORKER

---

Processing license applications and the attached documents will be one of the main tasks of the Agency. The caseworkers mentioned in Chapter 4 should be the ones to review and assess the in-



formation in these forms and act as the primary contact persons from the Agency.

In reviewing the information provided on the forms, the caseworker must assess whether the facility in question has provided all the required information on the application form. The form should ask for some very specific data; details of the information that should be included in the license application may be found in Chapter 8, 'A general guide to licensing'.

The caseworker must also be sure that the facility lives up to relevant biosecurity standards as mandated in the Executive Order and spelled out by specific Agency requirements. If the information provided on the application form demonstrates that the facility does not live up to these standards and requirements, or if other circumstances make it necessary, new security measures should be required.

Details on how to evaluate the security needs of a facility may be found in Chapter 7, 'Vulnerability assessments and security plans'. Other chapters in Sections 2 and 3 will also deal with specific security issues that can be relevant for this evaluation.

### WHEN REQUIREMENTS ARE MET, A LICENSE CAN BE ISSUED

---

Once the Agency is satisfied that the facility has correctly filled out the application form and has achieved the required level of biosecurity – or will do so by a specified deadline – the license can be issued. In practice, no two licenses will be exactly alike, because the types of facilities and the scope of their work are so varied.



We will deal with a variety of specific licensing issues in several of the chapters in Section 2.

During the first year or so after the Agency begins operations, at least some of the licenses that are issued will have to be of a temporary nature.

**See page 68,** 'Lessons learned: Short-term licenses may be necessary'.

### CASEWORKERS SHOULD CONTINUE TO ACT AS CONTACT PERSONS

---

When a facility has received its license, the relevant caseworker should begin to function as permanent contact person for that facility. Communication between the Agency and the facility will continue over time in connection with such events as inspection visits, training of Biosecurity Officers and changes to the license.

Depending on the size and complexity of the facilities in question, one caseworker should be able to act as contact person for 10-20 facilities.

At this point in the implementation process, the caseworkers should also begin to establish and keep a complete file of all documents that relate to the facilities for which they are responsible.

**See box** on page 74, 'A file on each facility is indispensable'.

### FACILITIES SHOULD KEEP A BIOSECURITY DOSSIER

---

Facilities, meanwhile, should keep a confidential and securely-stored file that contains all of their



important security-related documents. For the purposes of this book, we will refer to this file as the Biosecurity Dossier.

We will mention the Biosecurity Dossier in several chapters of this book, but you will find the most detailed description in Chapter 15, 'The work of Biosecurity Officers'.

### BIOSECURITY OFFICERS MUST BE TRAINED BY THE AGENCY

---

Another Agency task that can begin at this point is the training of Biosecurity Officers. If the Officer has not already been trained in connection with a previous position, a registration form for the mandatory training course should be submitted as one of the attachments to the license application.

**For more details,** see Chapter 15.

### THE AGENCY SHOULD DEVELOP A DATABASE OF INFORMATION

---

Among the other activities that the Agency should begin to develop at this point is the establishment of a database of national biosecurity information. This database will consist of information that the facilities have provided in the various application and reporting forms. The database should be continually updated.

The primary purpose of such a database is to provide a complete overview of the location of all controlled materials in the country. This should make it possible to generate a variety of useful lists.



If, for example, a specific pathogen from your country is discovered in the biological arsenal of a foreign power, authorities will want to know exactly where the pathogen came from. A list of facilities that work with that pathogen could help identify or rule out a given facility.

It goes without saying that the database of controlled materials should be treated as classified information and protected with a high level of security.

### THE AGENCY CAN ALSO HAVE MANY OTHER DUTIES

As the Agency establishes itself and gains practical experience, it will also be able to provide assistance in other areas where biosecurity expertise is needed. Such tasks could include:

- answering queries from the public
- assisting the Foreign Office with biosecurity-related reports
- suggesting new substances or materials for inclusion in the control list

There are some other Agency activities that can only begin after the passage of additional time. We will discuss these activities in the next chapter.

### AGENCY EXPERTISE MUST BE CONTINUALLY UPDATED

The Agency staff must continually update its own knowledge, in order to keep pace with continually changing technology and biosecurity threats. Updating activities should in principle begin as soon as the Agency commences operations and continue for as long as the Agency exists.



In addition to participating in any relevant training courses, the Agency could have subscriptions to biosecurity-relevant publications, both national and international. Participation in international biosecurity conferences will also help keep the Agency abreast of new developments.

Such gatherings have the additional advantage of creating an international network of friendship and communication among the participants. This can over time become extremely useful.

#### A FILE ON EACH FACILITY IS INDISPENSABLE

For any activity that involves public administration – and this includes the biosecurity Agency – a system for cataloguing and filing case documents is extremely important.

Every facility under Agency jurisdiction should have its own file containing all relevant documents. This should include all application and license forms as well as any written correspondence, inspection reports, notes from meetings and telephone conversations, etc.

Such written documentation is indispensable in case of disagreements; it is also useful to review a facility's file when preparing for an inspection visit or an educational outreach. All documents should be dated and catalogued for easy retrieval.







## CHAPTER 6:

# ENFORCEMENT, EDUCATION AND REVISION OF LAWS

*Inspections and other enforcement activities will be among the last elements to be implemented in a new biosecurity system. The same is true of educational outreach programmes and the work of re-evaluating and revising biosecurity legislation.*



**R**outine inspection visits to the various facilities are an important part of the Agency's enforcement work. There will be nothing to inspect, however, until the facilities have had the time to apply for their licenses and implement the required security measures.

But once the required measures and procedures are in place at the facilities, a staff of inspectors from the Agency should be ready to pay them a visit and see the end result.

### YOU CANNOT INSPECT EVERYTHING AT ONCE

The first inspection visits will involve a learning curve, even for persons with great expertise in bioscience and/or public administration. Everyone will need to gain experience in what to look for, how to behave and how to manage the practical aspects of an inspection.

The first lesson to learn is that you cannot do everything at once.

Rather than trying to visit as many different types of facilities as possible in the first inspection year, we have found that it is best to gain inspection expertise in one area at a time. Once you feel confident working with one type of facility, you can move on to the next.

### FIRST VISITS SHOULD BE CAREFULLY PRIORITISED

In choosing the facilities on which to concentrate your first efforts, you should think carefully about which of them are most vulnerable and in need of the strongest security.



We believe the facilities that handle and store controlled biological substances should have the most stringent biosecurity requirements and should therefore also be given top inspection priority. So your first visits should be to facilities that fall within this category.

Clinical microbiological facilities that only work with controlled biological substances in a diagnostic capacity need a degree of biosecurity awareness, but these facilities can be visited at a later time. The same goes for facilities that handle or store related materials and do not work with biological substances.

In Section 2, you will learn more about the recommended biosecurity requirements for the various types of facilities.

### AN INSPECTION INVOLVES MANY QUESTIONS

The main purpose of an inspection visit is of course to ensure compliance with the biosecurity requirements of the Executive Order and compliance with any additional requirements made by the National Biosecurity Agency. Inspectors should ask to see laboratories, storage facilities and physical security installations.

They should also ask to see written documentation such as

- up-to-date inventory lists
- training certificates
- written security procedures



In later chapters, we will discuss a number of other important documents which the facility should also make available for inspection.

To ascertain the legitimacy of the work that is being done at the facility, inspectors should ask questions about its current projects. They should also be able to speak with employees.

### IDEALLY, PUNITIVE SANCTIONS SHOULD BE RARE

This may all sound a bit like the Spanish Inquisition. And of course it's true that the Agency must be an authority to whom the facilities must answer. Ideally, however, an inspection visit should not just be a round of questioning but a dialogue between equals with a common goal.

Punitive sanctions for non-compliance – withdrawal of licenses, fines and even prison sentences – are of course possible; they have been described and authorised in the Executive Order. Hopefully, though, such sanctions will rarely be necessary.

### INSPECTORS CAN ALSO PROVIDE ADVICE AND SUPPORT

Inspection visits also have an educational aspect, insofar as the Agency can provide on-the-spot advice and support while its inspectors are visiting the various facilities. An inspection visit can in fact be the perfect time for a facility to express specific biosecurity concerns; Agency inspectors can then draw on their expertise to help work out a good solution.

In some cases, an inspection will reveal potentially dangerous situations that are easily remedied,



once the facility has been made aware of the problem.

**See box** on page 82, 'Remember to hide the key'.

You will find many more details and step-by-step recommendations about inspection visits in Chapter 16, 'Preparing and conducting an inspection visit.'

### THE AGENCY ALSO HAS A BROADER EDUCATIONAL OBLIGATION

---

Because the Agency has gathered all relevant biosecurity expertise under its 'roof', it should also have a broader obligation to educate. Once the basic systems of licensing and inspection have been established, the Agency should begin to reach beyond the facilities and share its knowledge with a wide variety of other stakeholders.

First and foremost, this stakeholder community must include students at relevant universities and other educational institutions. The purpose of this outreach should be to instill a bioethical mindset and a good biosecurity attitude in the young people who will be the scientists and opinion leaders of tomorrow.

The Agency should also share biosecurity and bio-preparedness knowledge with

- scientific organisations
- pharmaceutical and other industry organisations
- safety and emergency service personnel
- relevant government and trans-national agencies
- any other group that the Agency finds relevant



## REMEMBER TO HIDE THE KEY

---



This photo recreates a situation encountered during a real-life inspection at a Danish facility where a regard for convenience created a biosecurity risk. As you can see, the key to a freezer containing controlled substances is

readily accessible to legitimate staff as well as ill-intentioned thieves.

## THERE ARE MANY WAYS TO SHARE KNOWLEDGE

---

Knowledge-sharing should be tailored to the needs of each target group. Presentations could, for example, consist of short talks, longer course programmes, informational brochures or annual activity reports.

A practical solution for verbal presentations is to prepare a few 'standard' lectures that are designed for specific target groups (facility staff, university students, scientific gatherings, etc). With a few minor adjustments, such talks can be re-used many times. Powerpoint slides can support the effectiveness of these lectures.

The Agency should also participate actively in national and international biosecurity conferences at which it can communicate its experiences and share its expertise. External communication can also take place through newsletters, website updates and articles in scientific journals and other publications.



Among the subjects that will be discussed in Section 3 of this book is the role of Agency outreach programmes as they apply to biosecurity culture, bioethics and emerging biosecurity challenges.

### LEGISLATION SHOULD BE REVISED AT REGULAR INTERVALS

---

With the passage of time, both the Agency and the facilities will gain much experience with the practical realities of the biosecurity legislation that has been implemented. Both parties will no doubt find that there are problems and issues that were not anticipated in the original legislation.

In other words, revisions will be necessary. This will primarily relate to the Executive Order, which is the easiest to revise, but there may be more fundamental issues that are best addressed with a revision to the Biosecurity Law.

In any case, the relevant legislation should be reviewed for possible revision a few years after implementation. And because biosecurity involves challenges that are continuously changing and evolving, such reviews should continue to take place at regular intervals for as long as the legislation exists.

### ONCE AGAIN: STAKEHOLDER PARTICIPATION IS ESSENTIAL

---

In the revision process, stakeholder participation will be an absolute necessity. It is the facilities that must live with requirements they may feel are unreasonable. In the time since the original legislation was implemented, they may also have discovered some previously unnoticed loopholes – or even



feel the need to express particular satisfaction with some aspect of the legislation.

Their voices must be heard.

### A SATISFACTION SURVEY CAN SUPPORT THE REVISION PROCESS

---

During the revision process, the Agency should be interested in finding out such things as whether the facilities feel that the biosecurity regulations have placed them at a disadvantage compared to other countries, and whether the required physical security is a hindrance to their daily work routines. It is also important to know, for example, whether the training provided to Biosecurity Officers enables them to perform their jobs effectively.

A practical way to secure stakeholder feedback about the effect of biosecurity legislation is to conduct a satisfaction survey. The survey should ask for feedback from the facilities about such subjects as:

- whether they understand the purpose of biosecurity regulations
- the amount of daily biosecurity work they must perform
- their satisfaction with the training course for Biosecurity Officers
- their experiences with inspection visits
- whether the forms they must fill out are user-friendly
- suggested improvements to the legislation

The Agency's own experiences with the facilities will no doubt enable it to develop many other questions for this survey. And of course the Agency will



probably have issues of its own which can also be addressed in the process of revision.

### APPROPRIATE REVISIONS WILL INCREASE RESPECT FOR THE LAW

---

The process of revising biosecurity legislation exemplifies the spirit of communication and cooperation in which all biosecurity work should take place.

It will not necessarily be possible to accommodate all the needs and suggestions described in the satisfaction survey. But it is important that the needs of the various facilities are taken into account and accommodated whenever this is compatible with good biosecurity practices.

As we have pointed out several times, appropriate flexibility can only increase respect for the law.

#### **Lessons learned:**

##### BIOSECURITY EXPRESSES SOCIAL RESPONSIBILITY

---

More and more private companies have begun to work with 'corporate social responsibility', or CSR, as it also called. The concept refers the idea that a company has obligations to society that extend beyond selling a product and making a profit.

In our contact with the various facilities, we have found that some of the private corporations that work with controlled materials now mention their biosecurity licenses as part of their external communication about CSR. And it is certainly true that compliance with biosecurity regulations fulfills an





obligation to society – in this case, an obligation to help protect it from biological weapons of mass destruction.

Non-corporate facilities such as universities and hospitals can express a scientific social responsibility in the same way as the corporations. The scientific social responsibility extends beyond the immediate goal of increasing scientific knowledge and has the same ultimate goal as corporate social responsibility.

In Section 3 of this book, we will discuss the issues raised by scientific social responsibility in much greater detail.



# SECTION 2:

## BIOSECURITY IN PRACTICE

---

This section will provide a deeper look at some of the most important biosecurity tasks.

We will begin with a detailed look at the vulnerability assessments and security plans that are the starting point for improving biosecurity at the facilities. Next, we will discuss recommended licensing practices and learn how the information from the vulnerability assessments and security plans can be used to establish specific licensing requirements for the individual facility.

Recommended requirements for physical and employee-related security for the various types of facilities will also be found in this section, as well as a thorough description of the work of the Biosecurity Officer and a step-by-step guide to conducting an inspection visit.

Finally, we will discuss the concept of biopreparedness and how it relates to biosecurity.





## CHAPTER 7:

# VULNERABILITY ASSESSMENTS AND SECURITY PLANS

*Biosecurity weaknesses must be addressed and improved before a facility can receive a license to operate. It is up to the Agency to review existing security and decide whether new measures are needed.*



**A**s described in Chapter 4, the Executive Order should require facilities to provide the Agency with a Vulnerability Assessment and Security Plan before they can receive a license to work with controlled materials.

In the biosecurity system we recommend, the Vulnerability Assessment and Security Plan is a separate form that must be filled out and attached as an appendix to the main license application.

**The Vulnerability Assessment** identifies any threats and security vulnerabilities associated with the possession, manufacture, use, storage, sale, purchase, transport, transfer and disposal of the controlled materials.

**The Security Plan** indicates the security measures that will be taken to address any vulnerabilities. Its purpose is to prevent, detect and respond to theft or misuse of the above materials.

Security measures in this context should address:

- physical security
- employee-related security
- procedures for inventory control and handling of controlled materials
- biopreparedness procedures

We will discuss each of the above subject areas in greater detail in later chapters of this book.

#### IT IS IMPORTANT TO ASK ABOUT BIOSECURITY PROCEDURES

---

It's a good idea to design the Vulnerability Assessment and Security Plan as a series of questions that



can reveal any biosecurity weaknesses that need to be remedied. Some of these questions should ask for descriptions of biosecurity procedures; other questions should simply ask for a yes-no response.

Yes-no questions, when properly worded, can immediately reveal a security gap. But it's also important to ask the descriptive type of question about biosecurity procedures. These procedures are hugely important, regardless of whether they relate to physical security, the hiring of new employees, the screening of foreign partners, the handling of dual-use biological substances or any other biosecurity issue.

Standardised biosecurity procedures place biosecurity right where it belongs: at the center of the facility's daily tasks. This in turn increases biosecurity awareness and strengthens biosecurity culture.

### QUESTIONS SHOULD BE ASKED ABOUT EXTERNAL CONTACTS

---

The facility should also be asked to describe activities that might involve the risk of controlled substances and related materials falling into the 'wrong' hands. Does the facility have international activities, foreign guests, external partners and/or student employees?

Does it screen its foreign clients and external partners before selling or transferring controlled materials to them?

This type of screening is extremely important; there are painful examples of facilities that have



unwittingly helped build up the biological arsenals of other countries because no questions were asked of their 'customers'. **See box** below.

### IRAQI BIOWEAPONS WERE BUILT WITH WESTERN MATERIALS

---

In the aftermath of the Gulf War between Iran and Iraq in 1990-91, UN investigators discovered that Iraq had developed an alarmingly large arsenal of biological warheads in the 1980s. Perhaps equally dismaying was the fact that a great deal of the pathogens and equipment used to create this arsenal were purchased from reputable companies in Europe and the US.

Most of these companies had no idea of what their 'customer' was planning. The fact that certain orders were unusually large aroused no suspicion, and very little screening took place to investigate how bacteria (including deadly strains of anthrax and *clostridium perfringens*) were to be used.

The case is a clear illustration of the need to ask some very pointed questions before making transactions that involve dual-use materials.

---

**Source:**

R. Jeffrey Smith, Iraq's Drive for a Biological Arsenal  
(The Washington Post, 21 Nov. 1997)

---



## ALL CONTROLLED MATERIALS MUST BE ACCOUNTED FOR

---

The Vulnerability Assessment and Security Plan should also ask the facility to describe its procedures for handling and accounting for controlled material. Depending on the facility and its activity profile, this could include descriptions of how materials are transported, how stored inventory is registered, and how excess materials are disposed of.

Clinical microbiology departments and other diagnostic facilities should describe procedures for how they propose to transport, dispose of or seek a license for continued storage of controlled biological substances that were isolated as a result of their activities.

Facilities should also be asked descriptive questions about biopreparedness procedures in case of theft, accidental release and other irregularities that relate to controlled materials.

## SECURITY GAPS MUST BE ADDRESSED

---

If a facility responds with a 'no' to any of your yes-no questions, it should be asked to describe the steps it will take to remedy the situation. This description is the Security Plan, and the facility should include a deadline for its implementation.

It will then be up to the Agency to assess whether these measures are sufficient, or whether additional action is required.



**We will discuss** security issues in greater detail in Chapters 10, 11 and 12.

### QUESTIONS MUST BE CAREFULLY WORDED

---

The questions that are asked by the Agency in relation to the Vulnerability Assessment and Security Plan should be carefully chosen and worded to ensure that the answers contain relevant and useable information. Descriptive questions are important – but there is a limit to their usefulness.

Experience has taught us that we must also ask very specific questions about security. Facilities that are asked open questions about the quality of their security measures will almost invariably respond that no additional security is necessary – and this creates frustration if the Agency later finds that their security is, in fact, inadequate.

**You can find** inspiration about creating effective questions on the CBB website, where we have placed an English-language version of the Danish Vulnerability Assessment and Security Plan form.

It should be noted, however, that some of the questions in the Danish form contain country-specific terminology and concepts. This is also true of the written guidelines that are attached to the form. You must of course tailor your documents to suit the needs of your own country.

### FACILITIES WILL NEED GUIDANCE FOR FILLING OUT THE FORM

---

Not all the questions in this form will be relevant for every facility. Foreign-based retailers without



local storage facilities will not need to answer inventory questions, nor will diagnostic facilities that destroy their isolates shortly after determining what they are. And facilities that only work with related materials will not need to answer questions about biological substances.

Written guidance should be provided to indicate which questions must be answered and which questions may be left blank by the various facilities. Guidance could, for example, take the form of a matrix such as the one shown in fig. 4.

**See page 96-97, 'Lessons learned: A little help goes a long way'.**

### LOCAL RISK ASSESSMENTS CAN BE USEFUL

---

In many countries, facilities use a tool known as a risk assessment to help evaluate local, facility-specific risks. The key question that a facility must ask in this type of risk assessment is: What are the situations at your workplace in which your controlled materials are most vulnerable to theft or misuse?

Vulnerable workplace situations could, for example, include a short span of time during which a supervising scientist must leave a room in which controlled biological substances are being handled. Or a situation in which a cleaning assistant needs to access a restricted storage area where no authorised supervisor is available to accompany that person.

Such assessments require careful thought in order to cover as many eventualities as possible. And for



every situation that is identified, a solution must be devised to address the problem.

The vulnerabilities identified during this process can become part of the facility's Vulnerability Assessment. And the solutions can be incorporated into the Security Plan.

### THE AGENCY MUST DECIDE HOW MUCH SECURITY IS NEEDED

---

It is now up to the Agency to review the completed form and find the level of security that should be

#### **Lessons learned:**

##### A LITTLE HELP GOES A LONG WAY

---

**Fig. 4:** The matrix shown on the page opposite is used in the Danish biosecurity system to indicate which questions on the Vulnerability Assessment and Security Plan form must be answered and which may be left blank, depending on the type of facility and the purpose of the desired license. It is designed to suit the needs of the most common types of facilities in Denmark (see Chapter 9 for special cases).

The matrix is part of a two-page written guideline that accompanies the form itself. It is a good idea to provide this type of guidance for all of the forms that are used in a biosecurity system.

The Agency should of course be able to answer any question a facility might have about how to fill out the biosecurity forms described in this book. But carefully-constructed guidelines can anticipate many such questions and thereby save time and trouble.



required of the facility. In its review, the Agency must consider several questions:

- Does the facility have any security gaps?
- Can the Security Plan sufficiently close these gaps?
- If not, what extra requirements should the Agency impose?
- Does the facility need a higher level of security than others of its type?

In answering the above questions, the Agency will need to take an extra look at the facility's activity profile.

In addition to the Vulnerability Assessment and Security Plan form and its accompanying guidelines, you will find many other sample forms from the Danish biosecurity system on the CBB website. Each form includes a set of suggested guidelines, in some cases supplemented with matrices such as the one shown here.

As with all our examples from the Danish biosecurity system, these matrices can only be regarded as an inspiration. Your matrix documents – if you decide to use them – should of course reflect the types of facilities that are present in your country.

	<b>Licence to possess biological substances</b>	<b>Licence to possess related material</b>	<b>Licence for diagnostics</b>	<b>Retailers of related material with stock in Denmark</b>	<b>Retailers without stock in Denmark</b>
Section 1	1a, 1b, 1d	Not to be completed	1c	Not to be completed	Not to be completed
Section 2	2a	Not to be completed	2a	Not to be completed	Not to be completed
Section 3	3a – 3d	3a – 3d	Not to be completed	3a – 3d	3a – 3d
Section 4	Procedures: 1-3	Procedures: 1-2	Procedures: 3-5	Procedures: 1-2	None



## SOME FACILITIES ARE MORE VULNERABLE THAN OTHERS

---

The nature of the work being done at the facility could be a factor that increases or decreases the needed security. Facilities that only work with controlled substances in a diagnostic capacity, for example, are generally less threatened than those with a large and varied inventory of biological agents and related materials.

Whether or not the facility sells its products to foreign governments can also make a difference in terms of required security. Another factor that can make a facility more or less vulnerable is the visibility of the work it is doing. Highly visible projects are of course also more likely to be noticed by a potential thief.

In the next few chapters of this section, we will take an in-depth look at the licensing requirements and levels of security the Agency may call for, based on the type of facility and its individual needs and vulnerabilities.







## CHAPTER 8:

# A GENERAL GUIDE TO LICENSING

*Before granting a license to a facility, the Agency must be sure that all controlled material is accounted for, and that all biosecurity responsibilities are clearly defined. It should also make sure that the purpose of working with controlled materials is 'legitimate'.*



**T**o perform its licensing duties effectively, the Agency must have much more information than what is provided in the Vulnerability Assessment and Security Plan.

Apart from the security plans and procedures described in the above document, the Agency must know exactly what sort of controlled materials are present at a given facility. It must also know exactly who is responsible for ensuring that acceptable biosecurity standards are observed. And it must be convinced that the facility's work has a legitimate and lawful purpose.

In practice – and as mentioned in Chapter 5 – this means that the main application form for a license to work with controlled materials must provide some extremely specific information.

This application form should be filled out by every facility, regardless of whether it is a diagnostic laboratory, a retailer of controlled material, a department in a university hospital or some other entity.

A few exceptions can be made to certain licensing requirements; these will be described in Chapter 9, 'Exceptions and special licensing cases'.

**See also** box on page 107, 'Diagnostic facilities should not be omitted'.

### NAMES AND ADDRESSES SHOULD BE AS SPECIFIC AS POSSIBLE

---

First of all, the license application should state the address of the facility in question as well as the name of the responsible manager and the name or names of the Biosecurity Officer(s).



In this context, 'address' refers not to the address of an entire hospital or of a corporate headquarters, but to the specific laboratory, clinic, department or project site at which the controlled materials are present. Each entity within a larger organisation that wishes to work with controlled materials should submit its own license application, as well as its own Vulnerability Assessment and Security Plan.

The name of the responsible manager should be the facility's overall director or CEO. In practice, the CEO of a larger organisation will often delegate his or her biosecurity responsibilities to a relevant manager. The name on the license application will, however, ensure maximum accountability from top leadership as well as from the Biosecurity Officers who work directly with controlled materials.

### A LICENSE SHOULD ONLY BE VALID FOR SPECIFIC MATERIALS

---

As for the controlled materials themselves, the license application should provide the Agency with a list of all the materials that it wishes to work with.

The final license, if and when it is issued, should only be valid for the items stated on the application form. If the facility later needs to work with other types of controlled materials, it should apply for a change to the license.

This will ensure that a license is only issued when the Agency is completely aware of how it will be used. It also ensures that the Agency's database of controlled materials is always up to date.

**See also** the section on page 109 about change reporting.





A license application should inform the Agency of the exact location and quantity of all controlled items.

### THE QUANTITY AND LOCATION OF STORED MATERIALS MUST BE SHOWN

---

The list of materials on the application form should include the exact quantities of these items as well as the identity of the building and room in which they are stored.

Such requirements may sound unnecessarily fussy – but the whole purpose of a biosecurity system is to ensure that no controlled material is forgotten or ‘goes missing’ from any site or storage room. A strict accounting system must begin with the knowledge of where everything is to begin with.

This knowledge is the necessary starting point for the inventory control procedures that the facility must describe in the Vulnerability Assessment and Security Plan. You will find additional details on this and related subjects in Chapter 13, ‘Inventory control’.



## BIOSECURITY-RELEVANT PROJECTS SHOULD BE DESCRIBED IN DETAIL

---

The Agency must also be convinced that the purpose of working with controlled materials is a legitimate one that does not involve a hidden bioweapons agenda. For this reason, the license application should also include a detailed description of the project or activity in which the controlled materials will be used.

This description should include the aim and nature of the project or activity as well as its duration (if it is time-limited, e.g. a PhD project). It should also include the name, education and job description of the main responsible for the project or activity and the identity of any collaborating facilities, including the names of relevant contact persons.

It should also clarify how the project or activity is being funded and include an estimate of the total resource consumption. The estimate should be broken down to show how much is being provided by the facility itself and how much is being provided by external contributors, if any. Such contributors should also be identified.

## INSPIRATION CAN BE FOUND ON THE CBB WEBSITE

---

As with the other working documents described in this book, the CBB website contains an English-language version of the Danish license application form. It also contains the guidelines used by facilities when filling out the form.

To help the facilities determine which parts of the application form are relevant to them and which



are not, the guideline document includes a matrix similar to the one supplied with the Vulnerability Assessment and Security Plan.

The above documents can provide inspiration for creating your own application form and guidelines. As with all of our sample forms and documents, however, you must of course adjust and design your application form and guidance material to suit the conditions that apply to your own country.

### **MOST LICENSES SHOULD ONLY BE VALID FOR A SPECIFIED TIME**

---

As a general rule, facilities should be issued a license that is valid for no more than about five years, after which a new application process should take place in order to renew the licenses.

**See page 110, 'Lessons learned: Time-limited licenses ensure up-to-date information'.**

To avoid over-regulation, however, special rules should apply for clinical microbiology departments and other diagnostic laboratories that do not work with related materials and do not store controlled biological substances for more than a very short time.

Such facilities can be issued a permanent license that only allows them to work with controlled substances in a diagnostic capacity.

It should be noted that if the diagnostic facility wishes to store the controlled substances for more than a couple of weeks after its diagnosis has been made, it should be subject to the same period of license validity as other facilities.



## DIAGNOSTIC FACILITIES SHOULD NOT BE OMITTED

---

Some may find it odd that we recommend the licensing of diagnostic facilities. After all, such units do not keep dangerous biological substances in long-term storage; pathogens that are isolated in connection with a diagnosis are usually destroyed almost immediately after the diagnosis has been made.

However, these laboratories have a high throughput of samples containing dangerous pathogens, and skilled microbiologists are handling these samples on a daily basis. Diagnostic facilities are therefore a potential source of material for a biological weapon, and they could also be a source of experienced microbiologists who could isolate this material with a view to illegitimate use.

We therefore feel it is wise to bring diagnostic laboratories into a national licensing system, although exceptions can be made to some of the rules that apply to other types of facilities.

## THE AGENCY CAN MAKE ONE OF FOUR LICENSING DECISIONS

---

Together with the information provided by the Vulnerability Assessment and Security Plan and any other attachments the Agency may decide to require, the information on the license application form will provide a good basis for making a licensing decision.

Once the Agency has received all the necessary and correctly-completed forms, it should be able to process them within a relatively short period



of time (about two weeks would be appropriate). In its response to the facility, the Agency can decide to:

- grant a license with no attached conditions
- grant a license on condition that the facility lives up to specified requirements (eg. extra physical security, improved inventory control, etc.)
- deny the license
- notify the facility that a license is not necessary

### DECISIONS MUST INCLUDE DEADLINES AND ADVICE ABOUT APPEALS

---

In our experience, some facilities actually do apply for licenses that are not necessary. This is often because they are unsure of whether a given biological substance or related material is on the control list.

On the other hand, there will also be facilities that must fulfill additional biosecurity requirements in order to obtain a license. The Agency response in such cases should include a deadline for when these requirements must be met.

If the license is denied, the response from the Agency should include guidance on how to appeal this decision (as per the appeals process developed during the establishment of the Agency).

### REQUIREMENTS AND CONDITIONS SHOULD BE STATED ON THE LICENSE

---

For facilities seeking a license to work with controlled materials, the license document itself should specifically state:

- the period of license validity



- the specific controlled materials with which the facility is allowed to work
- the sort of activities that are permitted
- the names of the responsible manager and Biosecurity Officer(s)
- any extra requirements named by the Agency
- the deadline for complying with these requirements
- a requirement stating that the facility must notify the Agency of any change in the above data

For extra security, a system of codes can be used to describe the controlled materials mentioned in the license. We will return to this and other inventory-related subjects in Chapter 13.

If a facility loses its license or decides to terminate its operations, it should be required to provide the Agency with a description of how it will dispose of its controlled materials. This will ensure that nothing is 'lost' in the process of liquidation.

### THE AGENCY SHOULD BE NOTIFIED OF ANY CHANGES

---

As noted above, the Agency should require facilities to report any changes to the information that is stated on the license – be it names, addresses, materials, storage facilities or any other facts. Reporting should take place in good time before the change is implemented. Failure to do so should involve a risk of suspension or loss of the license.

This type of change reporting is crucial, because it ensures that the Agency is constantly updated on the state of biosecurity within its jurisdiction.



It also allows the Agency to react to the change notification and, if necessary, issue new requirements based on the new information.

Among the sample forms on the CBB website, **you will find** an English translation of the change reporting form used in Denmark.

### THE AGENCY SHOULD BE PREPARED FOR 'SPECIAL CASES'

---

Some facilities may have activity profiles that require a somewhat different approach than what is described above.

In the next chapter, we will take a look at some of these 'special cases'.

#### **Lessons learned:**

##### TIME-LIMITED LICENSES ENSURE UP-TO-DATE INFORMATION

---

Over time, many changes can take place at facilities that store and work with controlled materials. Five years after a license is issued, the facility in question may have moved to new premises and may not even be working with the substances that are named on its license.

Ideally, these and other changes should always be reported to the Agency on the appropriate form. But in Denmark, we believe that a time-limited license can ensure that any 'forgotten' changes are caught and noted during the license renewal process. This provides the Agency with an extra assurance that its information is up-to-date.







## CHAPTER 9:

# EXCEPTIONS AND SPECIAL LICENSING

*In a flexible system such as the one we propose, it should be possible to make exceptions to biosecurity rules. This chapter will deal with some of the most important 'special cases'.*



**N**ot all of the many facilities that work with controlled materials will need to meet the same licensing requirements.

We have already described (in Chapter 8) one important example of this: the many clinical microbiology departments and other diagnostic laboratories that only handle controlled biological substances for a very short period of time. As previously mentioned, we believe these facilities should not have to renew their license at regular intervals; they can be issued a permanent license that only allows diagnostic activities.

### **SOME FACILITIES NEED FEWER SECURITY MEASURES**

---

In the biosecurity system we recommend, other types of licensing exceptions can also be made. For example, facilities that work solely with related materials may not need to fill out the rather extensive portions of the Vulnerability Assessment and Security Plan that deal with physical and employee security.

The Danish biosecurity system makes this exception, based on the view that such facilities have fewer security risks than facilities working with controlled biological substances. Most controlled related materials are rather large pieces of equipment that are often bolted to the ground and are not easy to steal.

But there are other facilities with an activity profile that may require no license at all from your Agency. They should still have biosecurity obligations, however.



## 'FOREIGN' RETAILERS SHOULD REPORT THEIR TRANSACTIONS

---

Foreign-based retailers that have offices but no storage facilities in your country are subject to the licensing rules, if any, in the country where the materials are manufactured and stored. But if such a retailer wishes to operate within your borders, the Agency should be convinced that the purpose of this activity is legitimate. The Agency should also know all relevant details about the controlled materials that this retailer brings into your country.

In other words, your biosecurity system must include some provision for keeping the Agency informed about exactly which controlled materials are sold or transferred within your borders by these retailers. This information should include exact descriptions and quantities and identify the facilities involved in the transactions.

Without this information, the Agency database will be incomplete, and your biosecurity system will contain an unfortunate loophole. Apart from the security risk, such a loophole could distort competition between the retailers inside your country who adhere to reporting rules and the retailers outside your country who do not.

## IN SOME CASES, KNOWLEDGE AND INFORMATION SHOULD BE REGULATED

---

Another special licensing issue that should be carefully considered relates to facilities that work with *dual-use technology* – sometimes also referred to as 'dual-use research of concern' (DURC). As mentioned in the introduction to this book,



dual-use technology is a type of related material that is not a piece of equipment but a quantity of *information and knowledge*. It is an expertise which can be used for legitimate, scientific purposes but which also can be used to create a biological weapon.

Such information could, for example, include instructions for how to genetically alter bacteria strains to make them more contagious or more deadly.

Even if your biosecurity system does not yet include related materials, you should consider making an exception in favour of regulating dual-use technology.

Some types of dual-use technology have immediate potential for weaponisation, and we believe the facilities that develop and work with such technology should therefore be licensed. Licensing may not be necessary if the potential for weaponisation is not as immediate, but other forms of regulation and guidance should be considered.

### THE AGENCY MUST WORK OUT INDIVIDUAL LICENSING RULES

---

It is the job of the Agency to assess the work of the facilities that develop this type of technology and decide if and how they should be licensed or otherwise regulated.

Assessing the weaponising potential of a scientific project can be extremely difficult, and we will discuss this and related questions in greater detail in Chapter 18, 'Dual-use technology'.



At this point, however, it should be noted that the question of whether and how to license a facility that develops and works with dual-use technology should be based on an individual evaluation rather than a standard set of rules. Requirements should be made suit the specific situation.

### THE NEED FOR PHYSICAL SECURITY CAN ALSO VARY GREATLY

---

As we have already indicated, the need for physical security can vary greatly, depending on the type of facility and other factors. In the next chapter, we will examine some specific solutions and levels of physical security and see how they may be applied to the various facilities.

#### **Lessons learned:**

##### FLEXIBLE RULES PREVENT OVER-REGULATION

---

To avoid over-regulation, certain items on your control list can sometimes be excepted from control rules. In the Danish biosecurity system, we have chosen to create an exception for diagnostic activities that involve a live, unidentified culture that may turn out to be a controlled biological substance.

As long as the culture remains unidentified, it is excepted from normal reporting requirements – even if there is a strong suspicion that it is a controlled pathogen.

If the culture turns out to be a substance that is on the control list, any licensed diagnostic facility that is working with it can, in this system, be excused from having to file reports to the Agency ▶ ▶ ▶





about the discovery, transport, transfer or destruction of the pathogen – as long as the entire activity (including destruction) is completed within 14 days.

If the facility wants to keep the identified substance for a longer period of time, it must seek a license that permits storage, possession and handling of controlled biological substances.

The exceptions described above can be enormously helpful. Without such an exception, hospitals that regularly transfer 'suspicious' cultures to a diagnostic facility for analysis could be overwhelmed with transportation paperwork. A diagnostic facility could also drown in paperwork if it were required to file a report with the Agency every time it established the identity of a controlled pathogen.







## CHAPTER 10:

# EMPLOYEE SECURITY

*To reduce the risk of harmful activity by so-called 'insiders', good employee security procedures are crucial. But facility staff must also have a strong biosecurity culture.*



**M**onitoring the behaviour, access privileges and background of facility staff is an aspect of biosecurity that was brought into sharp focus after the anthrax attacks of 2001. The person presumed to have committed these crimes was a so-called 'insider': a facility employee with access to dangerous biological substances. Unfortunately, he did not live up to the trust that had been placed in him.

The employee security procedures we recommend in this chapter are designed to help ensure that employees who work with controlled materials do not abuse their trusted status.

### NOT EVERY EMPLOYEES NEEDS THE SAME ACCESS PRIVILEGES

---

A very simple way to reduce the risk of an insider abusing his or her status is to reduce the number of employees who have access to controlled materials. Persons who do not have an absolute need to work with or even know about these materials should not have the same access privileges and knowledge as those who do.

Facilities should also develop procedures to check the background of potential employees before they are hired. In addition, they should have procedures and equipment that can record employee activities in relation to controlled materials and ensure that unauthorised persons do not enter sensitive areas.

A useful first step for instituting these employee security systems is to divide facility personnel into different groups, each of which is assigned specific access privileges and requirements for training and background checks. We recommend the four-group system mentioned in Chapter 5.



## GROUP 1 SHOULD CONSIST ONLY OF BIOSECURITY OFFICERS

---

Group 1 – the first and most highly-trusted employee group – should consist only of the Biosecurity Officer(s). Background checks for this position should be the most extensive of all; in addition to references and documentation of identity, education and previous positions, the facility should check whether this person has a criminal record. The National Biosecurity Agency should also make an independent assessment of this person's suitability for the job.

Biosecurity Officers should have independent access to controlled biological substances and all confidential information about the facility's biosecurity. Officers must receive biosecurity training from the Agency and must keep themselves informed of new biosecurity trends and threats.

**See also** Chapter 15, 'The work of Biosecurity Officers'.

Among his or her many other duties, it should be the Biosecurity Officer who decides how to categorise the other employees at the facility.

## GROUP 2: SCIENTIFIC STAFF WITH INDEPENDENT ACCESS

---

The second personnel group should consist of principal scientists, technicians and other senior staff members who need independent access to specific controlled substances as part of their work. Background checks for this group should include references from previous workplaces and documentation of identity and education.



Group 2 personnel should receive biosecurity training from the Biosecurity Officer; these employees will share much of the responsibility for living up to biosecurity requirements at the facility, so their training should provide knowledge of the purpose and intent of biosecurity legislation.

Employees in this group should also have detailed knowledge and understanding of all facility procedures that relate to controlled materials. This includes procedures for inventory control and substance disposal as well as for accidents, theft and other irregularities.

### GROUP 3: STAFFS THAT DO NOT REQUIRE INDEPENDENT ACCESS

---

Group 3 staff can include a broad range of employees, from cleaning staff to university students who are attached to the facility while working on a dissertation. It could also include senior staff who do not need independent access to controlled substances.

At least some of the employees in Group 3 will need access to areas where controlled substances are stored or handled, but Group 1 or 2 personnel should be present if they work with the materials themselves. Only Group 1 or 2 personnel should have access to the keys that can unlock the containers (freezers, incubators, etc.) in which the controlled materials are stored.

Background checks for this group should be the same as for Group 2. Some persons in this group will be expected to contribute to the facility's biosecurity culture, and should therefore be trained



by the Biosecurity Officer so that they have an understanding of the basic principles of biosecurity. They should also be familiar with relevant rules and emergency procedures.

The Biosecurity Officer should decide, on an individual basis, the level of knowledge that is required for employees in this group.

#### GROUP 4: PERSONS WHO DO NOT 'NEED TO KNOW'

---

Persons in Group 4 may or may not actually be employees, but they are in contact with the facility in connection with their work. This group could include guests, technicians or craftsmen from the 'outside' as well as persons who are employed at the facility but who have no legitimate need to know about its controlled materials.

These persons should have no access to controlled substances and should only have access to areas or rooms in which these materials are stored or handled if accompanied by someone from Group 1 or 2.

No background check is required for persons who have no knowledge of the controlled biological substances at the facility. Knowledge of biosecurity rules and procedures is not relevant for this group.

It should be noted that neither Group 3 nor Group 4 employees should ever be left alone in a room where controlled substances have been removed from storage. If no one from Group 1 or 2 can be in the room while this material is being handled, the work should be stopped and the material locked away.



## ACCESS TO KEYS AND ALARMS SHOULD BE RESTRICTED

---

Within this system of recommended access privileges, there is now one remaining question: who should have access to the relevant keys and alarms? We suggest the following:

Group 4 personnel should have no access to container keys, room keys or the keys to a shutter system that might be installed around a locked container as extra protection. They should likewise have no access to or knowledge of any protective alarm systems.

Relevant employees in Group 3 may be permitted access to room keys, shutter keys and alarm systems – but only if their work requires it. Possession and use of container keys – that is, the keys that open the freezers, incubators, etc. in which controlled biological substances are stored – should only be allowed for Groups 1 and 2.

Because of its sensitive nature, the Biosecurity Dossier should also be kept locked away, and the Biosecurity Officer should be the only one with independent access to the relevant key.

If necessary, the Officer can allow access to relevant documents in the Dossier for Group 2 or 3 employees, but only if their work requires it.

**We will discuss** this system again – including the use of alarms and security shutters – in Chapter 12, 'Lock and key: choosing the right security system'.



## PERSONNEL LISTS CAN HELP ENSURE PERSONAL ACCOUNTABILITY

---

The purpose of the above system is to ensure accountability from all persons who have access to controlled materials. To support this accountability, we recommend that a personnel list be drawn up that shows exactly which persons from Groups 2 and 3 are authorised to work with each of the controlled substances that are present at a facility.

In addition to the name of the substance and the names, personnel group numbers and job titles of the employees that are working with it, the personnel list should include a space where each employee can sign off after receiving appropriate biosecurity training.

This personnel list should be drawn up by the Biosecurity Officer and kept in the Biosecurity Dossier (see Chapter 15). The lists should be regularly updated to reflect changes in names or access privileges, and they should be shown to Agency representatives on demand.

On the CBB website, you will find an example of the personnel list form that is used in Denmark.

## STAFF MOVEMENTS IN SENSITIVE AREAS SHOULD BE REGISTERED

---

As mentioned at the beginning of this chapter, facilities should also have systems and procedures to identify and register the movements of persons who have accessed sensitive areas or handled controlled substances. Logbooks, duty





Personalised electronic card readers can automatically register the date and time at which a particular employee has accessed a sensitive area.

rosters and the like can, for example, be used to record names, dates and times at which specific areas or substances have been accessed.

Electronic card readers that serve as a 'key' to specific areas or rooms can automatically record names, access times, etc. At the same time, they can also serve as a physical barrier against unauthorised intruders. Such readers can be included in a comprehensive physical security system. We will deal with this subject in more detail in Chapter 12.

As an additional employee security precaution, facilities may consider using a system of employee identification badges that are worn at all times while at the workplace. Such systems are already used by many businesses around the world, whether or not they have biosecurity issues, to help ensure that unauthorised persons are not given access to sensitive areas or information.

As we have mentioned several times, however, all security systems and procedures depend on good biosecurity culture to make them work. Employee security begins and ends with employees that are dedicated to this culture.



## EMPLOYEES SHOULD NOTICE AND REPORT SUSPICIOUS CIRCUMSTANCES

---

One way in which employees at a facility can demonstrate their commitment to biosecurity culture is by simply being aware of what is going on around them. Odd behaviour, strangers in the 'wrong' place, irregularities in inventory lists, and other unusual circumstances could represent a threat that needs to be noticed and reported to a Biosecurity Officer or to the Agency.

Some of these signs and circumstances may be so subtle that one might tend to brush them off, thinking "it's probably nothing" or "it's none of my business". A classic situation involves the employee who is greeted in a friendly manner by someone who then asks for a favour:

"I know you're not supposed to do this, but could you just open this door for me, just this once?"

In this regard, it's important to recognise that even minor incidents could be a sign of a larger threat involving facility staff (insiders), non-employees (outsiders) or both.

## PROBLEMATIC BEHAVIOUR CAN SIGNAL AN INSIDER THREAT

---

Insider threats are perhaps the most difficult to deal with, because nobody wants to suspect or falsely accuse a colleague of misconduct. An insider threat could come from an employee who attempts to:

- remove inventory without authorisation



- gain access to areas or computer terminals for which they are not authorised
- cover up and not report inventory discrepancies
- generate additional inventory that is not authorised or required

A staff member who behaves aggressively or demonstrates other behavioural problems can pose a special type of insider threat that also requires awareness. In the US anthrax letter case in 2001, the suspicious and problematic behaviour of a mentally unstable employee was ignored by colleagues and management alike until it was too late, with catastrophic results.

Problematic or suspicious behaviour could include:

- the expression of extreme political viewpoints
- pronounced changes in personality, e.g. from extrovert to introvert
- personal threats
- harassment of other employees
- giving wrong or misleading information to superiors
- continuous late working hours (weekends and nights)

#### FACILITY STAFF SHOULD ALSO BE ALERT TO OUTSIDER THREATS

---

A biosecurity threat from non-employees – the so-called ‘outsider’ threat – is a biosecurity problem that requires good physical security systems. As mentioned above, we will provide detailed recommendations for this in Chapter 12.

However, employees at facilities with a good biosecurity culture can also help minimise outsider



threats through watchful awareness. In view of the fact that outsiders with malicious intent might try to enlist the help of an insider, such awareness is very important.

Signs of an outsider threat could include:

- suspicious attempts to buy or transfer controlled substances
- suspicious requests for laboratory access (no legitimate purpose)
- theft of ID cards, key cards, etc.
- attempts to access information systems, especially access control systems
- visits from 'government officials' who cannot produce adequate identification
- the use of false IDs or other documents to gain access to a facility

### EMPLOYEES SHOULD BE ENCOURAGED TO STEP FORWARD

---

Employees may be reluctant to step forward and mention a particular problem, especially if an incident seems to be minor. They may feel they are being overly zealous, or that they might cause unnecessary trouble or bother for a colleague.

It is in situations like this that an open and trusting relationship with the Agency can help: facility employees who feel uncomfortable about mentioning something their manager may find it easier to take their concern directly to the Agency.

In any case, facilities need to develop a biosecurity culture in which there is no stigma or reprisal attached to reporting an unusual circumstance.



Even if an irregularity does not involve an immediate biosecurity threat, it should be noticed, reported and remedied if possible. An inventory discrepancy, for example, may be the result of a simple clerical error. But if the problem is not reported and resolved, it will contribute to a culture in which theft becomes easier and less noticeable.







## CHAPTER 11:

# THE BASICS OF PHYSICAL SECURITY

*This chapter will present some basic tools, terms and quality standards that are used in relation to physical security systems. This knowledge will help the Agency set national standards for the physical protection of controlled materials.*



**T**he purpose of physical security is to provide tangible and effective protection against theft, sabotage and other malicious acts that involve controlled materials. The topics described in this chapter will primarily deal with the protection of sensitive knowledge and controlled biological substances that are stored for more than a few weeks, rather than with controlled equipment.

### PHYSICAL SECURITY IS BOTH MECHANICAL AND ELECTRONIC

---

Physical security can include both mechanical devices (e.g. barriers, locks, reinforced construction, security doors) and electronic equipment (e.g. sensors, alarms, card readers, and other types of surveillance equipment). Taken together, such devices and equipment should be able to detect, delay and create a response to any type of unauthorised intrusion:

- Electronic devices can *detect* unauthorised movement.
- Mechanical devices can *delay* a break-in.
- Alarm transmissions to a monitoring centre can trigger an appropriate *response* from police or security guards.

### SYSTEMS MUST GUARD AGAINST BOTH OUTSIDERS AND INSIDERS

---

The most obvious goal of physical security is to prevent an outsider with malicious intent from gaining access to sensitive areas and storage containers. But physical security should also hinder facility staff (insiders) who try to abuse their status by removing controlled materials from the premises, either alone or together with outsiders.



Physical security should also help prevent the abuse of controlled materials *inside* the facility. Such cases could, for example, involve insiders who are secretly using the facility's controlled biological substances for unauthorised purposes.

### SPECIAL RULES ARE NEEDED FOR CLINICAL DIAGNOSTIC FACILITIES

---

Clinical diagnostic facilities that do not store controlled biological substances for long periods of time after a diagnosis has been made will not need physical security systems that are designed to protect storage areas.

Controlled substances that are isolated in connection with the diagnosis of a disease should instead be protected by labeling them 'anonymously' – that is, with the use of codes instead of the actual substance names. The key that links these codes to actual names should of course be securely protected (either physically or digitally), and access to it should only be granted on a 'need to know' basis.

If codes are not used, the sample or samples in question will of course need to be kept under lock and key until they can be destroyed.

The above system for handling controlled isolates should be supplemented with obligatory procedures to ensure that these substances are destroyed or handed over to physically secured facilities within a couple of weeks after the diagnostic process is completed. These procedures should be a part of the licensing requirements for clinical diagnostic facilities.



## RAPID CULTURE DIAGNOSTICS CAN LOWER RISKS

---

Diagnostic facilities can also choose to lower their risk profile by using rapid culture diagnostics – a technique also referred to as culture-independent diagnostics. The use of this technique would be an advantage from a biosecurity point of view, because it completely eliminates the isolation phase.

**We will return** to this subject in Chapter 19, 'Future challenges'.

## SUBSTANCES SHOULD BE CATEGORISED ACCORDING TO RISK

---

Not all controlled biological substances pose the same type of security threat. For example, some substances are less virulent than others. Other substances have a history of being successfully used as a biological weapon and may therefore be a more likely target for theft and misuse.

Because of such differences, we strongly recommend designing a system in which the substances at greatest risk are protected with the highest level of security.

As a first step, the Agency or a consulting expert should assess the level of risk that is presented by each of the controlled biological substances within the Agency's jurisdiction. We recommend using this assessment to place the substances in one of three categories, with Category 3 containing the substances that present the greatest risk.



## TWO MAIN PARAMETERS ARE AT PLAY: LIKELIHOOD AND CONSEQUENCE

---

To decide whether a substance belongs in Category 1, 2 or 3, it can be analysed in relation to two parameters:

- the *likelihood* of that substance being used offensively
- the potential *consequences* of its usage as a weapon

To determine likelihood, the following may be examined:

- the historic use of the material
- the ease with which it could be transformed into a weapon (technique)
- the ease with which it may be obtained (availability)

In terms of consequences, one could consider the following:

- the mortality/morbidity of the substance
- the existence of possible countermeasures (treatments)
- the level of contagion (transmission) exhibited by the substance.

The interplay between these factors is illustrated in fig. 5, 'Threat characterisation', on page 141.

## OTHER FACTORS: BUILDING DESIGN AND STATISTICS

---

In designing an effective physical security system, particular attention must be paid to the above risk categories. But there are other factors that should also be considered.



The most important of these has to do with the number of employees who work with the facility's controlled substances. From a purely statistical standpoint, the more people who have independent access to a given substance, the higher the risk of abuse.

The physical layout of a facility can also affect the design of a physical security system. Ground floor laboratories with windows, for example, will require more physical security than top-floor workplaces with no outdoor stairs, galleries or fire escapes.

### FINDING THE RIGHT SECURITY LEVEL CAN BE SIMPLE – OR COMPLEX

---

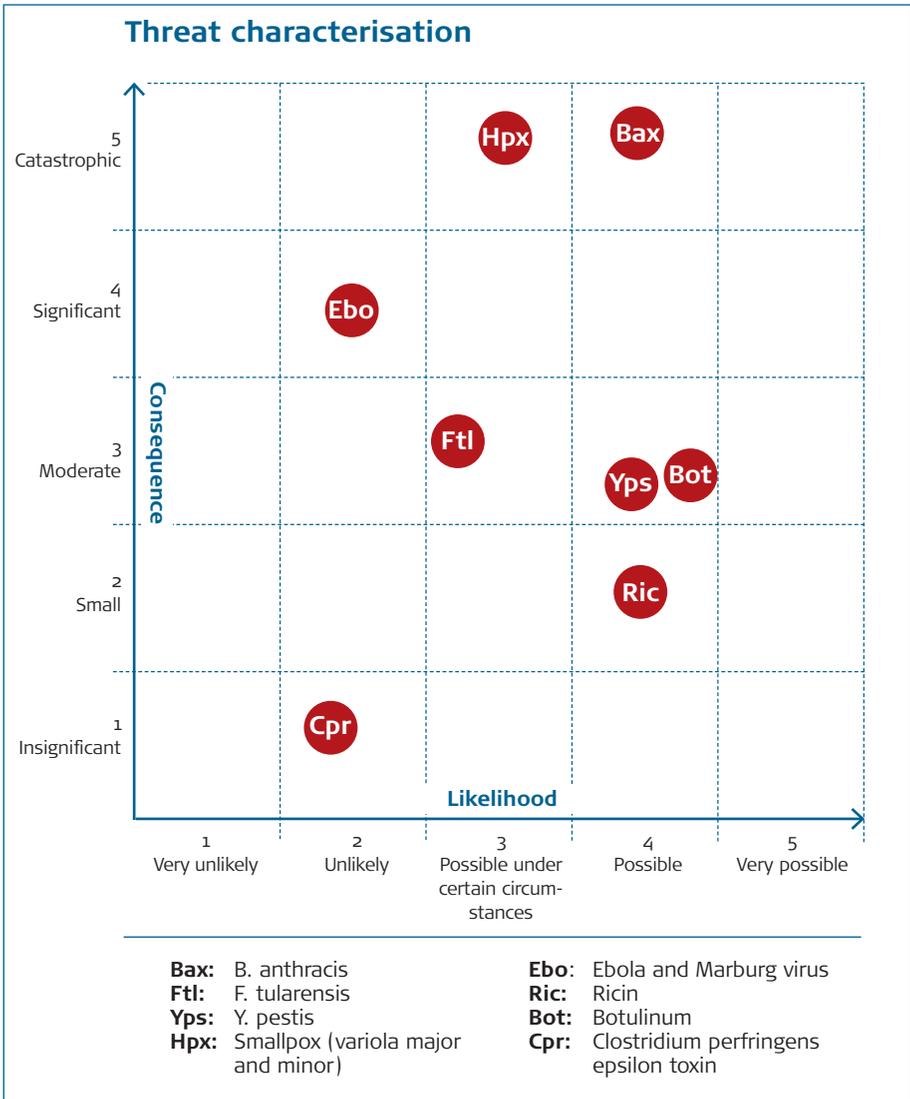
Once the three levels of risk have been established for the controlled substances in your jurisdiction, it can be a fairly simple process to assign each substance to a corresponding level of physical security.

As previously mentioned, however, there is an important factor that can complicate this equation: the number of persons who have independent access to a given substance. In Denmark, we believe that this factor alone can heighten the risk of even a relatively 'safe' pathogen.

For this reason, we recommend that the Agency assign a basic level of security (Level 1) to a substance in Category 1 unless five or more persons are allowed independent access to it. In this case, the substance should be assigned to Level 2.

Substances in Categories 2 and 3 should always be assigned to Security Levels 2 and 3, respectively.





**Fig. 5:** The chart shown here is an example of how to assess the threat posed by a variety of controlled biological substances. It shows, for example, that in Denmark we believe there is a high likelihood that B. anthracis (Bax) might be used as a biological weapon, and that the consequences of such use could be catastrophic. This makes B. anthracis, in our view, one of the most dangerous biological substances in the world.

Your own risk assessments may differ from the ones shown here, depending, for example, on the type and availability of the biological substances that are found in your country.



## WHAT DOES A FACILITY REALLY NEED?

---

The purpose of the above system is not only to ensure adequate levels of protection – it is also designed to encourage facilities think twice about the type of substances they possess and the number of employees who have independent access to them.

Among other things, the system can prevent facilities from ‘automatically’ granting independent substance access to a large number of employees who don’t really need it. By the same token, facilities that merely store Category 2 or 3 substances without really working with them may find, on reflection, that it could be a good idea to simply destroy this material or transfer it to another facility.

Either one of the above actions can minimise risks and result in less demanding security precautions. Moreover, minimising employee access to controlled substances can have an added benefit in the area of inventory control.

**See page 146,** ‘Lessons learned: Too many cooks spoil the paperwork’.

In the next few sections of this chapter, we will give you a basic overview of the content of each recommended Security Level. We will provide additional and more specific information in Chapter 12, ‘Lock and key: choosing the right security system’

## LEVEL 1: WHAT EVERY FACILITY SHOULD HAVE

---

Every facility with long-term storage of controlled biological substances, regardless of the category,



should be fitted with a basic level of physical protection consisting of barriers, alarms and locks. We will describe the choice, placement and use of these items in more detail in Chapter 12.

This protection must work hand in hand with the system of access privileges described in Chapter 10 as well as a system of inventory management which we will describe in Chapter 13, 'Inventory control'.

### LEVEL 2: EXTRA INSPECTIONS, TRAINING AND REPORTING

---

In addition to the basic requirements described above, facilities that have been assigned Security Level 2 should also submit to more frequent Agency inspections as well as heightened inventory control and extra staff training. We will describe these requirements in more detail in Chapter 12.

These extra obligations relate to the fact that the facility staff will be working with more dangerous pathogens that require extra attention and/or the facility has a greater number of employees who have independent access to controlled substances.

The latter is in itself is a complicating factor and an added risk.

### LEVEL 3: HEIGHTENED PHYSICAL SECURITY

---

Facilities that require this level of physical security will be working with the most threatening biological substances of all – pathogens for which the likelihood of abuse is particularly high and which could have catastrophic results if they were used as weapons of mass destruction.



Therefore: in addition to all of the Level 2 requirements, these facilities should have an added amount of physical protection. We will describe some of the possibilities more specifically in Chapter 12.

### SECURITY PRODUCTS SHOULD BE CERTIFIED BY A RELIABLE AUTHORITY

---

Regardless of the Security Level, it is extremely important that the physical barriers that protect a facility's controlled materials can provide a high level of resistance to intruders. In other words, the relevant doors, windows, security shutters, etc. should be as impenetrable as necessary.

For a non-specialist, however, it is almost impossible to evaluate the ability of a window or door to withstand a determined break-in effort. Therefore, the Agency should require facilities to produce written certification that the above fixtures comply with security standards that have been set by a reliable authority.

Compliance with such standards guarantees that all facilities within Agency jurisdiction have the same level of protection against intruders. It also saves time and trouble for the Agency: instead of inspecting every door, lock and window of every facility, the Agency can simply ask to see the relevant certification (see the section on page 145 about certificates of compliance).

### IF POSSIBLE, FACILITIES SHOULD COMPLY WITH CEN STANDARDS

---

In a great many countries, the authority that sets the standards for physical security products is



the European Standardization Committee (CEN). Among other things, these standards apply to doors, locks, windows, security shutters, window grilles and alarm systems.

If at all possible, we highly recommend that your Agency chooses security equipment that lives up to these standards. Compliance with CEN standards is your guarantee that the above-mentioned fixtures have a certain level of resistance to typical burglary tools (crowbars, screwdrivers, lock picks, etc.).

In your country, you may not be able to find suppliers of fixtures that comply with CEN standards. If this is the case, you should try to find products that are certified to comply with comparable standards from another relevant and trustworthy organisation. This could, for example, be an association of insurance companies, an association of companies that manufacture security products, or a neutral organisation such as the American National Standards Institute.

### FACILITIES WILL NEED CERTIFICATES OF COMPLIANCE

---

Regardless of whether the fixtures in question comply with the standards of CEN or those of another reliable organisation, the suppliers of these products should be able to provide facilities with written certificates of compliance.

These certificates are a facility's proof that necessary security standards have been met. The certificates should be kept in the facility's Biosecurity Dossier and shown to Agency inspectors on demand.



The next chapter will deal with specific types of physical protection and some specific CEN standards.

**Lessons learned:****TOO MANY 'COOKS' SPOIL THE PAPERWORK**

---

We have found that restricting the number of persons with access to controlled pathogens not only minimizes the risk of theft and misuse. It can also improve the way facilities keep track of these substances, because fewer people are involved in the necessary system of inventory control.

We will describe this system in more detail in Chapter 13. At this point, however, we may point out that in our experience, when a large number of persons share the responsibility for stocktaking and registration of inventory, it tends to increase the likelihood of confusion, inconsistencies and mistakes.







## CHAPTER 12:

# LOCK AND KEY: CHOOSING THE RIGHT SECURITY SYSTEM

*Once a nationwide set of rules and norms for physical security is in place, facilities can select specific products and systems that live up to these requirements. A variety of options are available, depending on the needs of the facility.*



In this chapter, we will discuss a variety of physical security solutions that are appropriate for Security Level 1 and 2 facilities, respectively. We will also discuss the interplay between physical security and the employee groups described in Chapter 10, and touch upon a few IT security issues.

It should be noted that security needs and issues will vary from one facility to another; each facility should therefore work out the specifics of physical protection in close cooperation with the Agency.

**See also** the box on page 161: 'Expensive mistakes can be avoided'.

### A SIMPLE SYSTEM – WITH MANY SPECIFICS

At its heart, the system of physical security we recommend is built up around three simple elements:

- a locked container
- an extra barrier
- a good biosecurity culture

But there is of course a great number of security products of varying quality that might be used in this system.

We will begin with a review of specific security solutions that apply to any facility that stores controlled biological substances, regardless of its Security Level. These are minimum requirements – the foundation upon which extra requirements can be added for Security Levels 2 and 3.



## CONTROLLED SUBSTANCES SHOULD HAVE TWO LAYERS OF PROTECTION

---

Physical security systems begin with the containers in which controlled biological substances are stored: the cabinets, freezers, fermenters, incubators, etc. As described in Chapter 10, these containers should be locked at all times unless someone from Employee Group 1 or 2 is present, and staff from these two groups should be the only ones who possess the relevant keys.

The above-mentioned containers should be surrounded by an extra 'layer' of physical security, so that there are at least two barriers against an intruder. We suggest choosing one of two solutions for this extra barrier: a securely constructed room or a secure shutter system.

## SECURE CONSTRUCTION METHODS CAN PROTECT AN ENTIRE ROOM

---

This extra layer could, for example, be provided by securing the entire room in which the pathogens are kept (see fig. 6). Many facilities may already have a room that is well-suited for this purpose.

This option is well suited for facilities that are working on a number of different projects at the same time. Such facilities may keep controlled substances in a variety of different freezers, incubators, fermenters etc., which makes it practical to secure the entire room in which these containers are placed.

If this option is chosen, the walls, ceiling and floor of the room should be constructed in a 'secure'



manner. In practice, this means the construction materials should include a layer of brick, concrete, steel or the like.

The room should also be fitted with high-quality security doors and locks. We recommend a level of security that corresponds to the following CEN standards:

- Doors: EN 1627, resistance class 5
- Locks: EN 12209, grade 5
- Cylinders for locks: EN 1303, grade 6
- Lever handles and knob furniture: EN 1906, grade 1

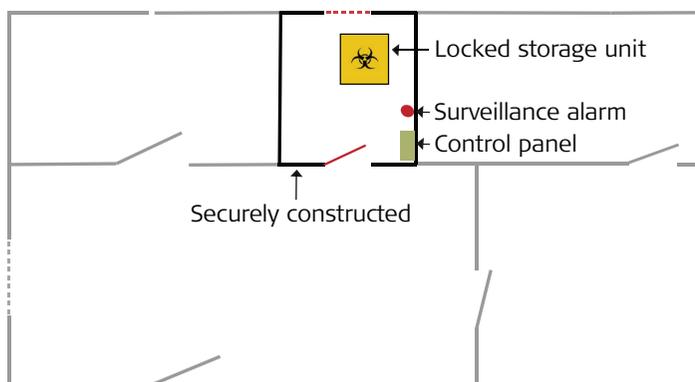
Ground-floor windows and upper-floor windows with outside access (fire escapes, galleries, etc.) should, in addition, be fitted with secure window frames and security glazing or grilles. Again using the CEN system as a guide, we recommend the following:

- Window frames: EN 1627, resistance class 5
- Security glazing: EN 356 P8B, resistance: burglary
- Window grilles: EN 1627, resistance class 5

Rooms that are protected in the above manner should be cleared and locked when no one from Employee Group 1 or 2 – or relevant persons from Group 3 – can be present.

In the context of this chapter, a 'relevant' person may be defined as someone who is specifically authorised to work with a particular controlled substance – in the above case, the material that is stored in the secure room. Such authorisation should be documented in the system of personnel lists described in Chapter 10.





**Fig. 6:** A ground floor, securely-constructed room containing biological substances in a locked container. Walls, ceilings, floors and doors are reinforced. Windows are protected with security glazing or grilles. The entire room is protected with electronic surveillance; both the alarm itself and the transmission equipment are in the room that is being monitored.

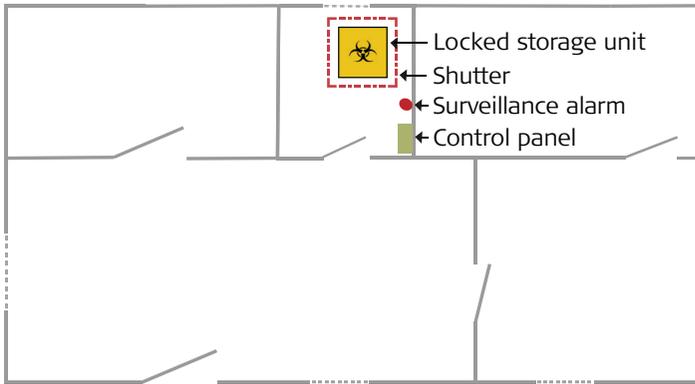
## SECURITY SHUTTERS CAN PROTECT A SPECIFIC STORAGE CONTAINER

Instead of protecting an entire room, the extra layer of protection could be provided by installing security shutters that can be drawn across part of a room or rolled down around the container itself (see fig. 7). This option is useful in cases where it would be impractical or extremely expensive to secure the entire room.

Security shutters must be anchored to a securely-constructed foundation – one or more brick walls, for example, or a concrete floor. We recommend that the shutters provide a level of security that corresponds to the CEN standard EN 1627, resistance class 5.

The shutters should always be locked when no one from Employee Group 1 or 2 – or a relevant person





**Fig. 7:** A ground-floor room in which biological substances in a locked container are protected by security shutters. No extra security is needed for walls, doors or windows. Electronic surveillance is the same as in fig. 6.

from Group 3 – can be present in the room in which the shutters are installed.

### ELECTRONIC CARD READERS CAN LIMIT ACCESS TO PROTECTED ROOMS

---

Only persons in Employee Group 1, 2 or relevant employees in Group 3 should be able to open the locks that are used for security shutters and securely-constructed rooms, and the keys should be traceable to specifically authorised persons.

To this end, it can be useful to install a system of personalised electronic card readers (also mentioned in Chapter 10) that will open these locks.

This will restrict the number of people with access to storage areas for controlled substances. At the same time, it can monitor and log the movements of employees who do have this access. Logged information can be saved for a specified period of time before being deleted.



## STORAGE AREAS SHOULD BE MONITORED BY AN ALARM SYSTEM

---

In addition to the security options described above, the room or shuttered area in which controlled biological substances are stored should always be equipped with a security-certified, automatic burglar alarm system.

This system should be installed by a licensed company, and surveillance should cover the entire room or shuttered area. We recommend an alarm system that lives up to the CEN standard EN 50131, grade 2.

The alarm system should have sensors that can detect unauthorised movement anywhere in the monitored area. It should also be able to transmit this information to an approved monitoring centre where police or security guards can be alerted.

The part of the alarm system that receives and re-transmits information and alarms to the monitoring centre should be placed in the area that is under sensor surveillance (see fig. 6 and 7). This placement will make it impossible to tamper with the transmitting system without setting off the alarm.

The alarm should be switched on after normal working hours if no one from Employee Group 1 or 2 – or relevant persons from Group 3 – can be present in the room where controlled materials are stored.

The code that is needed to switch off the alarm system should only be given to relevant employees whose names are registered in the facility's personnel list.



## AUDIBLE ALARMS ARE MORE EFFICIENT THAN VIDEO TRANSMISSIONS

---

The alarm system we recommend is designed to transmit an audible alarm rather than live video images from the monitored area. This is because we believe that 'soundless' video images are not a particularly good first-line defense against burglary.

Such images make it necessary for someone at the monitoring centre to be attentively watching the video monitoring screen at all times. In practice, this is actually rather difficult – and a moment's distraction could be enough to compromise security.

An audible alarm, on the other hand, will instantly make a security guard aware that something is wrong.

## DIFFICULT DECISIONS MAY BE NECESSARY

---

If a facility cannot live up to the minimum physical security requirements described above, it should strongly consider whether or not it should be working with dangerous pathogens at all. This is a question that should be resolved through strategic discussions with the facility's top level of leadership.

Before a decision is made, it may be useful to contact the Agency and discuss the possibility of alternative solutions. The facility may be able to suggest and provide good reasons for using a different method of achieving the needed level of physical security, and the Agency should be prepared to consider whether it could accept such a solution.



## EXTRA SECURITY FOR LEVEL 2 SHOULD BOOST BIOSECURITY CULTURE

---

As mentioned in Chapter 11, Security Level 2 facilities should be required to submit to more frequent Agency inspections, heightened inventory control and extra staff training. These requirements should give an extra boost to the facility's biosecurity culture and thus provide extra assurance that no biosecurity procedure is 'forgotten', insufficiently explained or inadequately executed.

Bearing this in mind, inspections at these facilities could, for example, be conducted annually as opposed to every 3-5 years for Security Level 1. These visits (which may be unannounced) should include emergency drills to test the facility's alarm systems and procedures in cases of theft, loss or accidental release of controlled biological substances.

Biosecurity Officers and employees in Group 2 should, in addition, receive detailed biosecurity training from the Agency, with obligatory updating/refresher courses every three years.

We also recommend that updated inventory lists of controlled substances be sent to the Agency four times a year as opposed to once a year for Security Level 1.

**You will find** more details about inventory procedures in Chapter 13, 'Inventory control'.

## LEVEL 3 FACILITIES NEED INDIVIDUALISED SOLUTIONS

---

Facilities at Security Level 3 must, in the system we



recommend, also live up to these 'cultural' security requirements. In addition, however, they should be required to install extra physical security. Such requirements should be prepared by the Agency, based on an individual assessment of the facility's needs.

A facility could, for example, increase the area that is securely constructed. This could involve securing all the corridors and rooms (including any outer windows) that surround the room in which controlled substances are stored. The Agency could also require secure construction for an entire floor – or an entire building.

If this type of construction project is not feasible, extra protection could be provided with a combination of a securely-constructed room and a shutter system.

Other security 'extras' could include such features as:

- perimeter protection (fences and gates) around part or all of the facility
- on-site security guards after normal working hours
- a receptionist who can register all 'outsider' visits
- video cameras to supplement an audible alarm system
- extra employee security clearance procedures

### INFORMATION CAN BE PROTECTED BOTH PHYSICALLY AND DIGITALLY

---

There is one more type of 'barrier' that we will deal with in this chapter: the barrier that protects sensitive information from unauthorised use.



Examples of sensitive information include a facility's inventory list of controlled biological substances – or almost any other type of information that is kept in the Biosecurity Dossier which, for practical reasons, may be in the form of a physical binder.

**See Chapter 15, 'The work of Biosecurity Officers'.**

As noted in Chapter 10 and again in Chapter 15, this binder must be securely locked away when not in use, and the Biosecurity Officer should be the only one who is allowed independent access to the key.

The Agency, meanwhile, will have security issues of its own in this regard. An Agency document describing the location of all controlled biological substances in the country is of course an extremely sensitive piece of information. Sensitive Agency papers could also include such things as correspondence from named institutions requesting permission to work with specifically-named biological agents.

### COMPUTER DRIVES MUST BE EFFECTIVELY PROTECTED

---

In practice, both the Agency and the facilities will also store much sensitive information on computer drives. The Agency database described in Chapter 5, for example, contains biosecurity information about every facility in the country.

Protecting this type information will require a top-notch system designed by a known and reliable company that specialises in IT security.

Websites, emails and other IT-based media can



also contain sensitive information. The Agency should carefully consider which parts of its website should be available to the general public. It should also consider which of its application forms should be available for downloading to 'outside' computers.

### **EVEN 'BLANK' FORMS CAN POSE A CHALLENGE TO IT SECURITY**

---

The form that contains a Vulnerability Assessment and Security Plan represents a special IT security challenge. Even when it has not been filled out, this form contains information about possible security solutions which could, in some situations, be useful to someone with malicious intent.

Once the form has been filled out, the security issue becomes even more sensitive. The Vulnerability Assessment and Security Plan will then contain very specific and confidential information about security at the facility in question.

To deal with this issue, the Agency might consider excluding this form from the download area of its website. Instead of downloading it, facilities could ask the Agency to send the 'blank' form to their email address.

The completed Vulnerability Assessment and Security Plan form should not be sent electronically at all. It should always be sent to the Agency via registered mail.



**Lessons learned:****EXPENSIVE MISTAKES CAN BE AVOIDED**

---

Installing a physical security system can be both complicated and expensive – especially if it is later found that the security installations chosen by the facility do not live up to the letter of the law and the requirements of the Agency.

To avoid expensive mistakes, the Agency should encourage facilities to consult with an Agency representative before investing in any type of physical security. Such consultations should also take place before beginning construction projects involving secure rooms.





## CHAPTER 13:

# INVENTORY CONTROL

*To make sure that controlled materials never 'go missing' without being noticed, every facility needs a meticulous accounting system that keeps track of its inventory.*



In Chapters 10, 11 and 12, we described two related systems that protect controlled materials from misuse: employee security and physical security. Employee security is designed to regulate who has access to controlled materials, while physical security should ensure that unauthorised persons do not have such access.

But no system is perfect, which is why a third form of protection – inventory control – is indispensable. Inventory control is meant to ensure that if anything ‘goes missing’ in spite of the above-mentioned precautions, the loss will be noticed and investigated.

### INVENTORY CONTROL IS SOMETIMES UNDER-APPRECIATED

---

The basic principle of inventory control is to know where everything is, all of the time. It involves counting vials, drawing up lists, recording how substances are used and reporting every movement of controlled materials in and out of every facility within an Agency’s jurisdiction.

Historically, some facilities have found it difficult to take this type of work seriously. This was certainly the case in the anthrax incident to which we have referred several times in this book. After the anthrax powder attacks, investigators found serious flaws in the inventory control system at the laboratory from which it is presumed that the powder was taken.

Apart from the risk of unnoticed theft and misuse, slipshod inventory procedures can also pose other types of dangers.



**See box** on page 173-174, 'Vials of smallpox found in a cardboard box'.

### A CONTROL SYSTEM SHOULD BEGIN AT 'GROUND ZERO'

---

The starting point for a system of inventory control should be the inventory list on a facility's license application (see Chapter 8). This is the 'ground zero' from which all subsequent changes should be registered and reported to the Agency.

As described in Chapter 8, this initial inventory list should include the exact quantities of each controlled substance that is present at the facility, as well as the identity of the building and room in which they are stored. If you choose to include related materials in your control system, these items should be specified in the same way.

In the system we recommend, most clinical diagnostic facilities are not licensed to store controlled biological substances or related materials. For this reason, they are not required to fill out the inventory portion of the license application form, nor will they need most of the inventory control system that we now will describe.

They should, however, be subject to other types of control. We will return to this subject later in this chapter.

### INVENTORY LISTS SHOULD RECORD ALL CHANGES IN STOCK

---

Once the existing supply of controlled materials at a facility has been thoroughly documented, the



facility should begin to keep updated inventory lists that chronologically record every change in that supply. This includes:

- the sale, purchase or transfer of controlled materials
- consumption of controlled biological substances in legitimate projects
- destruction of controlled biological substances
- new production of controlled biological substances

In addition to changes that relate to daily work routines, the facility should also record changes due to:

- the theft, misuse or loss of controlled materials
- the accidental release of controlled biological substances

We recommend that a separate inventory list be kept for each controlled substance or item of related material that is present at the facility. On each list, a dated entry should be made every time there is a change in the quantity of the material in question.

#### INFORMATION SHOULD INCLUDE LOCATIONS, QUANTITIES, ETC.

---

Entries on an inventory list should include the exact location of the material, the nature of inventory update (e.g. purchase, disappearance, legitimate consumption) and updated information about the quantity of that material. The inventory list for a controlled substance should specify the name or code name for that substance; for related materials, the inventory list should specify



the type and model number of the equipment in question.

All entries should be initialed by the person making the entry and then countersigned by the Biosecurity Officer, who thus guarantees that the information is complete and correct. Updated inventory lists should always be available for inspection by an Agency representative.

### ALL CONTROLLED STOCK SHOULD BE COUNTED EVERY QUARTER

---

Four times a year, the Biosecurity Officer should conduct a formal stocktaking of their entire inventory of controlled material and record the result on the appropriate inventory lists. This quarterly stocktaking should be done for all biological substances and related materials – even those that have not been touched during the preceding quarter.

This will ensure that any ‘unnoticed’ losses or other discrepancies are discovered and recorded. It should go without saying that every irregularity should be immediately reported to the Agency and investigated – with the help of the police, if necessary. Discrepancies should of course also be noted on the relevant inventory list.

**See also page 170** ‘Lessons learned: Stocktaking can be simplified’.

### INVENTORY LISTS SHOULD BE SENT TO THE AGENCY EACH YEAR

---

Once a year, completely updated copies of all inventory lists should be sent to the Agency. As



mentioned in Chapter 12, Security Level 2 and 3 facilities should be required to send these lists to the Agency on a quarterly basis.

Inventory lists contain sensitive information, but if codes are used to denote the various biological substances, the lists can be sent by ordinary mail or e-mail. If codes are not used, the lists should be sent by registered mail; at the facility itself, the lists should be stored under lock and key in the Biosecurity Dossier.

### TRANSPORTATION OF INVENTORY MUST BE SAFE AND SECURE

---

Facilities should also have procedures to ensure the safe transportation of controlled inventory from one place to another. Many countries already have legislation that governs the transportation of dangerous goods. Your country may be one of them, in which case much extra regulation can be avoided.

If not, your Agency should develop requirements to ensure that the facilities always use shipping agencies or carriers that

- are capable of safely packaging and transporting dangerous goods
- can ensure that the controlled items are delivered to the right recipient
- have adequate security against theft and loss

### SHIPMENTS OF CONTROLLED MATERIALS SHOULD BE REPORTED TO THE AGENCY

---

As an extra safeguard against theft, losses and incorrect deliveries, we recommend a reporting



system in which the Agency is immediately informed of any purchase, sale or inventory transfer that involves the shipment of controlled materials from one facility to another.

These reports should be made by the facility that is sending the shipment as well as the facility that is receiving the shipment. Their reports should be sent to the Agency no later than about 14 days after the shipment has taken place.

This procedure creates a kind of double-entry bookkeeping system in which a shipment of controlled material is recorded twice: once when the material is 'subtracted' from a facility, and again when it is 'added' to another facility.

### SHIPMENT REPORTS SHOULD PROVIDE EXACT INFORMATION

---

Information in these shipment reports should include descriptions and exact quantities of the controlled materials in question. Reports should also note the place of origin and the final destination of these materials.

If a facility is shipping out its last quantity of a particular controlled substance, the report should also state that the facility no longer has that substance in storage.

Clinical diagnostic facilities – due to the nature of their work – would be overwhelmed by the above reporting system. For this reason, they should generally not be required to file shipment reports unless they know for certain that their samples contain an isolated, controlled substance.



## Lessons learned: STOCKTAKING CAN BE SIMPLIFIED

---



There is one way to simplify the stock-taking process a bit. Instead of counting up large quantities of substance-filled tubes every quarter, the tubes can be counted *once* and then pack-

aged, sealed and labeled. This method is particularly useful for substances that are rarely used.

In the photograph shown here, the sealed material has been encased in plastic wrapping.

The next quarter at stocktaking time, it will then only be necessary to make sure that the seal on the packaging has not been broken. The entire contents of the sealed package can then be included in the inventory list.

## EXPORT CONTROLS SHOULD REGULATE CROSS-BORDER SHIPMENTS

---

Facilities outside the borders of your country are of course also outside the Agency's jurisdiction. However, sales or transfers to and from such entities should still be recorded by facilities under Agency administration.

As mentioned in Chapter 9, the Agency should also develop a system to stay informed of the controlled materials that a foreign retailer brings



into your country. Activities involving foreign clients should also be governed by a system of *export control*.

The primary purpose of export control regulation is to ensure that potentially dangerous goods and technologies do not end up in the arsenal of a foreign government or terrorist group. Many countries have systems in which exporters of such materials must apply for export licenses.

### INVENTORY CONTROL FOR CLINICAL DIAGNOSTIC FACILITIES

---

We have previously described a number of special requirements for clinical diagnostic facilities. While such facilities are exempted from most inventory control regulation, they should still comply with requirements for safe transportation, coded labeling of controlled substances and speedy destruction of isolates (see Chapter 11).

We have also noted that diagnostic facilities should not be expected to report the shipment of biological samples in and out of the facility as long as the exact contents of these samples are unknown. Bearing this in mind, shipment reports *should* sometimes be made in the case of so-called ring tests. This activity is a type of quality assurance trial that involves sending a biological substance to several different facilities, all of which are asked to analyse the substance for specific parameters.

Clinical diagnostic facilities that participate in a ring test should be required to inform the Agency of the receipt of test material within two weeks of



making their analyses, in cases where the samples are shown to contain a controlled pathogen. The facility that sends these ring tests out for analysis should likewise be required to report such shipments to the Agency.

### FACILITIES CAN USE AGENCY FORMS – OR THEIR OWN

---

On the CBB website, you will find examples of the inventory-related forms used by the Danish Agency. These examples include:

- forms for creating inventory lists
- a form for reporting shipments (purchase, sale or transfer) of controlled materials.

As always, our examples can only serve as inspiration for the creation of forms that are tailored to the needs of your own country.

Instead of using the Agency forms, facilities may feel more comfortable using their own inventory registration systems. This should be permissible, as long as these documents contain the same information and are given the same level of security as the Agency documents.

### THERE WILL STILL BE DIFFICULTIES AND UNCERTAINTIES

---

A final note on inventory control: we are well aware of the difficulties involved in trying to keep track of substances that can be cultured and propagated and thus transformed from a minute amount into a much larger quantity.

While taking stock of a facility's inventory – while



counting vials and boxes and making note of substance transfers in and out of a facility - one might be tempted to ask: Is this vial really full? Has this substance been cultured to replace some stolen quantity? How can we know for sure?

The answer is, we can't. Even so, we believe that a conscientious effort to account for every usage of a controlled substance contributes to a culture in which theft and misuse is less likely. Like any other prevention effort, inventory control is a fine supplement to a responsible biosecurity culture. But it can never be a replacement.

#### VIALS OF SMALLPOX FOUND IN A CARDBOARD BOX

In July 2014, six glass vials containing smallpox virus were discovered in a cardboard box at a US laboratory in Maryland. Tests performed by the US Centers for Disease Control (CDC) later revealed that the virus in at least two of these vials was alive and infectious.

The vials containing the deadly virus were found during a storage room cleanup; it was later determined that they had been lying in their forgotten repository since 1954.

Smallpox was declared eradicated in the 1980s. Today, only two high-security laboratories in the world – one in the US and one in Russia – are officially in possession of the smallpox virus.

According to the CDC, the disturbing discovery in Maryland points to “a problem in inventory control.”





In the wake of the smallpox case and two other US laboratory incidents, the CDC initiated a process to improve inventory accounting and safety procedures at federally-funded laboratories across the country.

---

**Sources:**

Mike Stobbe, *Forgotten Vials of Smallpox Found in Storage Room* (Associated Press, 8 July 2014)

Jen Christensen, *CDC: Smallpox found in NIH storage room is alive* (CNN, 11 July, 2014)

Jocelyn Kaiser, *Lab incidents lead to safety crackdown at CDC* (Science Insider, 11 July, 2014)

---







## CHAPTER 14:

# BIOPREPAREDNESS

*Even with the best biosecurity system, terrorist attacks, accidents and security breaches of a more or less serious nature can occur. Biopreparedness involves knowing what to do if this happens.*



**A**s mentioned in Chapter 1, biopreparedness is an essential element of any biosecurity system. A biopreparedness plan is also a required element in the Vulnerability Assessment and Security Plan described in Chapter 7.

But what does all this mean in practical terms?

### BIOSECURITY AND BIOPREPAREDNESS STAFF MUST WORK TOGETHER

---

First of all, it means that in addition to being the centre for all biosecurity expertise, it would be an advantage if the Agency also could be your national centre for biopreparedness. The two areas are closely related; an organisation that encompasses both would enable knowledge-sharing and other synergies that can save precious time in emergencies and promote efficiency in daily operations.

The Danish biosecurity Agency is organised in this way, as mandated by the Danish Biosecurity Law. But it is of course also possible for the Agency to work with together with a separate biopreparedness authority.

If your country chooses to use two separate authorities – one for biosecurity and another for biopreparedness – the two organisations should cooperate on a regular basis and keep each other closely informed of relevant developments.

### BIOPREPAREDNESS CAN MINIMISE THE EFFECT OF AN INCIDENT

---

Broadly speaking, biopreparedness is the ability to quickly minimise or eliminate the effect of an



undesired, illegal or dangerous incident that involves controlled biological substances and related materials.

Such incidents may not always be the result of malicious intent, nor will they always involve an immediate danger. Indeed, when such incidents occur, the level of danger is often unknown to begin with and must be ascertained by a biopreparedness response team. We will discuss the specific responsibilities and functions of such a team later in this chapter.

But every incident, large or small, will require some kind of prompt action by the Agency or biopreparedness authority as well as by the facility at which the incident took place. Sometimes the incident should also involve police action.

The type of action that is required will of course depend on the nature of the incident.

### MANY SITUATIONS REQUIRE BIOPREPAREDNESS EXPERTISE

---

Within the scope of the system that we recommend, there are three basic situations that require biopreparedness action:

- the suspected or confirmed *presence* of unlicensed, controlled materials
- the unauthorised *absence* of controlled materials
- the accidental or intentional *release* of controlled biological pathogens

We will deal with each of these situations in turn and describe the measures that should be im-



plemented. But first we'll look at some general issues.

### IT IS EVERYONE'S DUTY TO REPORT AN INCIDENT

Anyone who witnesses or discovers an incident related to one of the above situations should immediately report it to the Agency or biopreparedness authority. This applies to everything from misplaced inventory to the intentional release of a dangerous biological pathogen.

The person who makes such a report will often be a Biosecurity Officer. But it could also, for example, be an Agency representative who finds a piece of unlicensed, controlled equipment during a routine inspection. It might also be a laboratory employee who notices that a freezer full of controlled biological substances has been broken into.

The reporting obligation of facility employees should be stated in a specific clause of the Executive Order.

**On the CBB website**, you will find an example of such a clause in §20 of the Danish Executive Order.

### BIOPREPAREDNESS MAY ALSO INVOLVE ORDINARY CITIZENS

If your biosecurity Agency also functions as a national centre for biopreparedness, it may sometimes receive reports and requests for assistance from non-facility sources such as the police, other government agencies, emergency personnel and



even ordinary citizens. In particular, such requests may arise in connection with a possible biological emergency.

This type of request cannot be mandated by law in the same way as the reporting obligation for facilities. But the relevant authority should be prepared to receive and take action on such calls. The response should be tailored to suit the situation.

### **FACILITIES SHOULD HAVE WRITTEN BIOPREPAREDNESS PROCEDURES**

---

At the institutional level, the legally required, written biopreparedness plan for a facility should include emergency procedures in case of accidental or malicious release of biological pathogens. These procedures should be known to all facility employees, and regular drills should be conducted to make sure that everyone knows what to do.

In practice, the Biosecurity Officer will be responsible for ensuring that all biopreparedness procedures are followed and that the proper biopreparedness training has taken place. But the ultimate responsibility for this lies with the manager that is named on the facility's license.

Since it is part of the Vulnerability Assessment and Security Plan, the facility's biopreparedness plan will be approved and (if necessary) adjusted by the Agency.

### **A BIOPREPAREDNESS HOTLINE SHOULD BE ESTABLISHED**

---

To receive incident reports, a 24/7 telephone hotline



manned by an on-duty senior biopreparedness expert should be established. The duty expert will thus be able to receive reports at any hour and make an assessment of a situation involving dangerous biological materials.

Depending on the seriousness of the incident, the duty expert should also be able provide instructions for immediate, on-site countermeasures. If necessary, he or she should then activate a response team and initiate further action.

### RESPONSE TEAMS NEED SPECIALISED COMPETENCES

---

In a biological emergency, the role of a response team is to quickly identify the biological pathogen that has been released into the environment, and to define and demarcate the affected area. The team must also quickly identify those persons who may have been exposed to the pathogen so that they can receive medical treatment within a relatively short window of time.

The Agency or biopreparedness authority should ideally have several response teams at its disposal to deal with incidents that involve controlled materials. In Denmark, we use two-person teams consisting of a senior medical or veterinary doctor and a biopreparedness specialist. Between them, they have the following competences:

- field investigation experience
- specialised knowledge of bioweapons
- expertise within dispersal analysis
- expert knowledge of microbiology



The response team should have round-the-clock access to a laboratory where samples from the site of an incident can be tested for the presence of controlled biological substances. Coordinating staff should also be available to help organize the efforts of the team and any other agencies or emergency services that might be involved in a particular incident.

### SPECIALISTS SHOULD BE AVAILABLE ON SHORT NOTICE

---

It will most likely not be possible to employ all the above-mentioned specialists as full-time response team members. In their daily work, they may be employed in many other capacities, either at the Agency/biopreparedness authority or at an 'outside' facility. But the duty expert who answers the telephone hotline should know exactly how to locate the necessary personnel on very short notice.

In this context – as in many others – it is an advantage if the biosecurity Agency is also the national centre for biopreparedness. This will make it easier to build up the necessary network of response team members.

In the next few sections of this chapter, we will discuss the actions that are necessary for each of the previously-mentioned types of biopreparedness incidents. For the purposes of this book, our discussion will relate to incidents at facilities under Agency jurisdiction – but many of the responses we describe can be used in other contexts as well.



## THE UNAUTHORISED *PRESENCE* OF CONTROLLED MATERIALS

The suspected or confirmed presence of unlicensed, controlled materials at a facility could turn out to be a relatively harmless situation. But if it involves a dangerous biological pathogen, it could also be the sign of an incident that endangers human life, and could even involve bioterrorism. In any case, it should always be reported to the biopreparedness hotline.

### SOME CASES CAN BE EASILY RESOLVED

Once a call has been received, the duty expert must decide whether or not there is a need for response team action.

If the facility has already identified the nature of the unlicensed material, a response team may not be necessary. The material in question could, for example, be an unlicensed fermentor or an identified and safely-stored biological substance for which the facility has 'forgotten' to seek a license.

In such cases, the duty expert can simply inform the facility's responsible manager that the material in question must either be properly licensed or disposed of in a safe manner. The Agency should of course follow up to make sure that the required action is taken.

### IS THE SUBSTANCE SAFELY CONTAINED?

If the incident involves a controlled biological substance about which there is some uncertainty, a response team may be needed. This will depend on



whether or not the substance is contained – that is, safely stored in a way that poses no danger to the surrounding environment.

If it can be immediately determined that the substance is safely contained, it can be identified at a convenient time by laboratory analysis. Once the substance has been identified, the facility can be instructed to either get it licensed or to safely dispose of it. Again, the Agency should follow up on the matter.

But if there is even a remote chance that the material in question is not contained – that it has been released into the environment and may pose an immediate danger – the duty expert, the facility and the response team should all follow the procedures described below in the section ‘Release of controlled pathogens’.

### POLICE ACTION MAY NOT BE NECESSARY

In the system we recommend, the presence at a facility of unlicensed, controlled materials – regardless of whether or not such materials are actually being used – is a formal breach of the Biosecurity Law. However, the Agency or biopreparedness authority should exercise common sense when deciding whether or not to report this situation to the police.

For example, if an otherwise responsible and respected facility simply forgets to apply for a particular license, the mistake should not necessarily involve police action – especially if there have been no serious consequences.



## THE UNAUTHORISED *ABSENCE* OF CONTROLLED MATERIALS

The unauthorised absence of controlled materials refers to missing inventory that is not the result of normal use. The absence could be due to theft, but it could also be the result of an error in inventory control – or a case of simple misplacement.

### THE SITUATION COULD BE DANGEROUS

---

The duty expert who receives a report about missing materials should if necessary provide instructions for any immediate action. Based on his or her assessment of the situation, this could, for example, include making sure that a destroyed lock is immediately replaced.

If there is any suspicion or indication that a missing biological substance may have been released into the surrounding area, the duty expert and the facility should follow the procedures described below in the section 'Release of controlled pathogens'.

The Agency should at some point also speak to the Biosecurity Officer and the responsible manager of the facility about new security measures that could prevent such disappearances. Depending on the situation, such measures could include improved biosecurity culture, better physical security, better inventory control, intensified training of laboratory staff, etc.

### THEFT OF MATERIALS MUST INVOLVE A POLICE INVESTIGATION

---

The theft of controlled materials is by definition a



criminal act that could involve hostile governments or bioterrorist activity.

Missing inventory with visible signs of a break-in to a room, a freezer or other storage unit are indications of theft. But it is also possible that the thief has left no visible trace of his or her activity. Therefore: if there is even a slight chance that missing material has been stolen, a police investigation will be necessary.

Once the police have been informed of the matter, the Agency and/or biopreparedness authority should make their experts available to provide assistance to the investigation.

### THE *RELEASE* OF CONTROLLED BIOLOGICAL PATHOGENS

The release of controlled biological substances – whether accidental or intentional – is a serious matter that can endanger human, animal and plant life. It involves the risk of the pathogen spreading beyond the immediate area of release, thus placing a larger and larger region in the danger zone.

An accidental release could, for example, be caused by a defective fermentor; intentional releases include attacks such as the anthrax letters mentioned in the introduction to this book.

### AN EMERGENCY RESPONSE CAN INVOLVE MANY ACTIONS AND PLAYERS

---

Based on an immediate assessment of risks and possible threats, the duty expert who receives



such a report should provide the caller with any necessary instructions for self-protection and tell that person what, if anything, can safely be done to contain or minimise the immediate danger. Such actions should include keeping others away from the area where the substance release occurred.

If the incident involves a facility that is regulated by the Biosecurity Law, the facility should of course also follow the procedures in its own bio-preparedness plan.

If there is any risk that the incident involves bio-terrorism, or that medical and rescue assistance is needed, the duty expert should immediately inform local police and emergency services. He or she should also organise an appropriate response team.

As indicated above, a biological emergency of this kind can involve many different persons, agencies and services. The biopreparedness response team should therefore have a coordinating staff as well as laboratory technicians at its disposal.

### RESPONSE TEAMS WILL HAVE MANY RESPONSIBILITIES

---

A full-scale field investigation by a response team can involve many tasks. Among other things, the team should be able to:

- perform a dispersal analysis to determine the extent of possible contamination
- take on-site samples from areas that may be contaminated



- secure evidence and documentation needed for police investigations
- identify and disable any delivery systems
- halt and contain the contamination
- provide status reports to the coordinating staff
- initiate decontamination activities

The samples taken from the site should be immediately sent to the response team's laboratory, where the experts on duty can determine the nature of the substance that has been released. The response team should also work with and provide advice to police and emergency services.

### A RESPONSE TEAM CAN ALSO PREVENT PANIC

Hopefully, an actual bioterrorism attack or biological disaster will rarely if ever occur. But the efforts of the response team may also be needed for situations that turn out to be less serious. In such cases, a rapid and effective response can quickly rule out any worst-case scenarios and prevent unnecessary panic.

**See also** 'Lessons learned: The Agency should work discreetly whenever possible'.

Whatever the situation, everyone – the response team, the laboratory experts and the coordinating staff – should always be well-trained, well-drilled and able to employ their expertise at any time and on short notice.



**Lessons learned:****THE AGENCY SHOULD WORK DISCREETLY  
WHENEVER POSSIBLE**

---

Over the years, the Danish Agency has been called upon a number of times to investigate the possible presence of a dangerous biological pathogen. In such cases, our policy is to work as discreetly as possible without compromising safety and security.

In some cases, we found it necessary to send a response team that could take samples from the site in question and bring them back to our laboratory for analysis. In the majority of cases, however, we were able to make an expert threat assessment and rule out the presence of a pathogen without any extensive field work that could have attracted attention and created public unease.

It is important to note, however, that it is not always possible – or even desirable – to work discreetly. In situations of imminent danger, the public must be warned, and media coverage is to be expected.







## CHAPTER 15:

# THE WORK OF BIOSECURITY OFFICERS

*The Biosecurity Officer is key to implementing a good biosecurity culture at the facility. So it is extremely important that this person has the right qualifications, the right training – and the right mindset.*



**F**rom a practical standpoint, the Biosecurity Officer is one of the most important elements of a good biosecurity system. His or her efforts will set the biosecurity tone for the entire facility and are therefore key to creating the biosecurity culture that is necessary for the system to work.

For this reason, it is extremely important that the facilities choose the right person for the job, and that the Agency makes sure this person is adequately trained.

It is also important that a Biosecurity Officer is always present at the workplace. We highly recommend that the facility appoints more than one person to this position, in order to allow for vacations, illness and other types of absence. Another good reason to appoint at least two Officers is that the responsibilities of the Biosecurity Officer can be quite extensive.

#### **DUTIES: TRAINING, REPORTING, UPDATING AND MORE**

---

The duties of the Biosecurity Officer include (but are not necessarily limited to):

- ensuring a strong biosecurity culture at the facility
- training personnel at the facility in relevant aspects of biosecurity
- ensuring that all biosecurity procedures are correctly followed
- being aware of irregularities and suspicious behaviour
- maintaining an up-to-date list of controlled inventory
- reporting the purchase, sale or handover of controlled materials



- reporting changes that can affect the facility's license
- reporting any biosecurity problems or incidents
- maintaining a biosecurity dossier (see the relevant section below)
- participating in department meetings at which biosecurity issues can be discussed
- participating in inspection visits by the Agency
- staying informed of new biosecurity trends, threats, etc.

It should be apparent from this list that the Biosecurity Officer is the primary liaison between the facility and the Agency. In this capacity, the Officer or Officers bear a great deal of practical responsibility for implementing Agency policies and directives.

The responsibility and access to sensitive information that are associated with this position makes it advisable to check whether the prospective Biosecurity Officer has any kind of criminal record.

#### QUALIFICATIONS: KNOWLEDGE, CREDIBILITY AND CONFIDENCE

---

A Biosecurity Officer should have a thorough knowledge of the controlled materials that are used by the facility. This includes *which* materials are being used, *where* they are stored, how they being used, *who* is using them and the *hazards* that are involved with this use.

The Officer should be employed in the area where the controlled materials are handled and stored and should have a good knowledge of the work processes at the facility. He or she should be so well-acquainted with the workplace that they can



develop an individualised approach to teaching, inventory accounting, etc.

In principle, a Biosecurity Officer could be a laboratory technician, a senior medical doctor or anyone else who works at the facility on a daily basis. However, the facility should carefully consider whether a candidate for this position has enough workplace knowledge and professional credibility. Good communication skills are also necessary.

The work of a Biosecurity Officer can require both firmness and 'friendly persuasion'. The Officer should have a natural sense of confidence and authority, and he or she should be able to lead – both in words and by example.

### BIOSECURITY OFFICERS SHOULD BE TRAINED BY THE AGENCY

---

It is up to the Agency to provide the Biosecurity Officer with the necessary training for the job. Once completed, the training should be documented with a certificate of completion that allows the person to work as Biosecurity Officer for a specified period of time – three years, for example.

After that, the certification can be renewed after a refresher course that includes new, biosecurity-relevant knowledge and developments.

In Denmark, Biosecurity Officers are trained by the Agency at a mandatory, one-day course that is free of charge.

**See also** 'Lessons learned: Find the right level of training'.



**Lessons learned:****FIND THE RIGHT LEVEL OF TRAINING**

---

When the Danish biosecurity Agency first began to train Biosecurity Officers, we based our instruction on the assumption that most of the new Officers would be working at the level of laboratory technician. This turned out to be far from true.

Some trainees were certainly lab technicians, but the group also included senior medical doctors and others with a very high level of education. The lesson to be learned here is that training of Biosecurity Officers should be planned so that no one feels that the level is too high or too low.

This can of course be a challenge – but much can be accomplished by keeping a very sharp focus on biosecurity issues. These issues are by definition new to everyone at the training course, regardless of their previous education.

**TRAINING SHOULD COVER A BROAD RANGE OF SUBJECTS**

---

Training of the Biosecurity Officer should of course include instruction in the elements and principles of biosecurity, a review of relevant legislation and forms (such as the Vulnerability Assessment and Security Plan) and a thorough description of the duties and tasks of a Biosecurity Officer.

Training should also encompass a look at the *reasons* for biosecurity: internal and external security threats. It should also explain why it is necessary to screen employees as well as clients, as well



as the need for preparedness in case of biological emergencies. Bioethics is also relevant in this context.

**See more** on this subject in Chapter 17, 'Biosecurity culture and bioethics'.

The Officer should also be given a basic knowledge and understanding of biological weapons, the persons and groups who use them and how dual-use materials from 'innocent' facilities can become 'weaponised'. There should also be a review of new and emerging technologies that pose new types of biosecurity threats.

We will deal with this subject in several chapters of Section 3.

### BIOSECURITY OFFICERS MUST TRAIN THEIR COLLEAGUES

---

Once a Biosecurity Officer is trained, it is his or her duty to train others at the facility. This training will provide the basis and motivation for a good biosecurity culture in which everyone understands the need for licensing, security procedures and appropriate physical security.

Not everyone at the facility should receive the same type of training from the Biosecurity Officer. Instruction should be tailored to each of the employee categories described in Chapter 10. Sensitive information must of course not be given to those who do not need it for their work.

Every relevant employee at the facility should learn the basics of a good biosecurity culture and



responsible behaviour. This includes such things as noticing and reporting irregularities, preventing outsiders from entering restricted areas and not disclosing information that could be misused.

It should be up to the Biosecurity Officer to decide how best to accomplish this training. Depending on individual preferences and needs, instruction could take place in groups or in a one-on-one setting. Some instruction may be followed up with tests or practice drills – for example, a drill on how to react in case of a suspected release of a biological pathogen.

### THE AGENCY CAN HELP WITH THE TASK OF TRAINING

---

The responsibility for training colleagues and creating a good biosecurity culture at the workplace can sometimes feel overwhelming for a Biosecurity Officer, especially if he or she is the only Officer at the facility.

The Agency should therefore be willing to lend a hand with this educational task. One way to do this is to create a checklist of subjects that could be covered, and allow the Biosecurity Officer to pick and choose from this list according to the specific needs of the facility.

Another way to help is to offer Agency representatives as guest instructors or sparring partners for drawing up a lesson plan.

**See page 203,** 'Lessons learned: Biosecurity Officers may need teaching support'.



## BIOSECURITY OFFICERS MUST KEEP A BIOSECURITY DOSSIER

---

As previously mentioned, the Biosecurity Officer is also responsible for maintaining a Biosecurity Dossier, which is a collection of important – and sensitive – documents about biosecurity at the facility. Documents in this dossier should include:

- the facility's license
- documentation for the training of the Biosecurity Officer(s)
- copies of relevant legislation, including the latest control list
- all application and reporting forms that have been filled out by the facility
- up-to-date inventory lists of all controlled materials at the facility
- any codes that are used to identify controlled substances
- the facility's Vulnerability Assessment and Security Plan
- all materials used for employee training
- all biosecurity-related correspondence to and from the facility
- names of employees who have access to specific keys, card readers and alarm codes
- the list of Employee Groups described in Chapter 10
- descriptions of biosecurity procedures that are used at the facility
- any other biosecurity-related information about the facility

The Biosecurity Officer should be responsible for keeping all information in this dossier up to date. The dossier should be made accessible to the



Agency on request, and should always be shown to Agency inspectors during an inspection visit.

### THE DOSSIER MUST BE KEPT IN A LOCKED COMPARTMENT

---

During inspection visits, the Biosecurity Dossier will be an important tool that can ensure agreement between the written documentation and the actual on-site conditions. For this reason, it is practical not to store these documents electronically; instead, all the papers should be kept in a physical binder that can be carried around during a tour of inspection.

The information in the Biosecurity Dossier is of course confidential and extremely sensitive. When not in use, the Biosecurity Officer should be responsible for keeping the dossier in a locked and secure compartment or safe. The Officer should be the only person to have unrestricted access to this container; he or she may, however, grant access to other persons on a need-to-use basis.

Facilities that work solely with controlled equipment should not necessarily be required to lock up the dossier.

### A BIOSECURITY NEWSLETTER CAN BE AN IMPORTANT TOOL

---

In order to discharge his or her duties successfully, the Biosecurity Officer must keep abreast of all new developments, technologies, threats and trends that relate to biosecurity. The Agency refresher course mentioned above is one way to do this, but the Agency can also help by creating a newsletter for Biosecurity Officers.



This newsletter could contain such items as:

- updates on new national and international biosecurity regulations
- information about new Agency publications
- summaries of important biosecurity-related articles, with links leading to the full text
- news about Agency activities
- any other news that the Agency deems relevant

Apart from this, the Biosecurity Officer is of course also personally responsible for seeking out other sources of information that can keep him or her updated.

### THE RIGHT MINDSET IS ALSO NECESSARY

Many of the Biosecurity Officer's duties are not so much a matter of training and knowledge as they are of mindset. Noticing the fact that a procedure has been neglected, or being aware that 'something odd' is going on requires a certain willingness to open one's eyes and ears and report any problems or suspicions – even at the risk of being mistaken or making oneself 'unpopular'.

Mindset is an aspect of biosecurity culture that will be discussed further in Chapter 17.



**Lessons learned:****BIOSECURITY OFFICERS MAY NEED TEACHING SUPPORT**

---

In a 2013 user survey among Danish Biosecurity Officers, many of them showed an interest in supplementing their training work at the facility with a guest instructor from the Danish biosecurity Agency. As a result, we now actively encourage Biosecurity Officers to give the Agency a call if they would like to have on-site teaching support from an Agency expert.

We recommend that your own Agency provides similar encouragement to the Biosecurity Officers in your country. New Officers may find it especially helpful to draw upon the knowledge and experience that the Agency can provide.





## CHAPTER 16:

# PREPARING AND CONDUCTING AN INSPECTION VISIT

*This chapter will provide you with a step-by-step guide to the three phases of an inspection visit: preparation, inspection and follow-up.*



In Chapter 6, we noted that the primary purpose of an inspection visit is to ensure that the facility lives up to the requirements of its license. We also reviewed the basics of these visits: who to inspect, what to look for and what to ask. And we touched on some of the educational aspects of an inspection visit.

This chapter will provide a more detailed how-to for each of the three phases of an inspection visit: the preparation, the visit itself and the follow-up work that takes place after the visit. We will also take a closer look at some of the problems that can arise during an inspection.

The step-by-step procedures described below are a general framework based on the way inspection visits are conducted in Denmark. They can of course be expanded and adjusted to accommodate other needs and systems.

### THERE CAN BE SEVERAL REASONS TO VISIT THE FACILITY

---

If possible, a licensed facility should be inspected at least once every 3-4 years to ensure continued compliance with licensing requirements. In the meantime, however, there can be other reasons for the Agency to visit a facility.

The Danish Agency, for example, is empowered via the Executive Order to pay an informal visit to an unlicensed facility to find out whether it has any materials that should be licensed. An Agency representative may also visit a licensed facility by invitation, for example to help the Biosecurity Officer with a training task or to give a presentation on biosecurity culture.



On a very few occasions, the Agency may decide to visit a facility because of a suspicion that something is amiss. This type of inspection visit, although rare, should be given top priority. It should be noted, however, that if a suspicion is particularly strong, the matter should be turned over to the police.

### INSPECTIONS SHOULD BE CAREFULLY PLANNED

A 'normal' inspection visit can last anywhere from 1-4 hours, depending on the type of facility, but the preparations and follow-up work take the equivalent of an entire week or more.

To ensure a smooth flow of inspections, it's a good idea for Agency staff to sit down about twice a year and draw up a list of the facilities they would like to visit in the months to come. Each facility on the list can then be assigned a date and an inspection team.

It's also a good idea to have someone who is responsible for arranging all the practical details of an inspection visit – assigning teams, scheduling visits, arranging transportation, etc.

It is practical for an inspection team to consist of:

**a primary inspector** who leads the team and conducts the interviews. This person should be an experienced inspector with a relevant scientific degree and a good knowledge of controlled materials and laboratory work.

**an assisting inspector** who takes notes, makes observations, takes photos and can ask supplementary questions. This person could be 'in training' to become primary inspector.



In some cases, you may want to add an observer to the team.

The facility's responsible manager and Biosecurity Officer should be informed of the inspection visit in good time before it takes place. This will allow them time to prepare – or to ask for a rescheduling, if the timing is inconvenient.

### THE CASEWORKER SHOULD BE PART OF THE PLANNING PROCESS

---

At the Agency, preparations for an inspection should also involve the facility's caseworker, who (as described in Chapter 5) is the permanent contact person for the facility and will therefore be familiar with any special problems or circumstances that should be noted.

Ideally, the caseworker should act as one of the team's inspectors, but he or she may not have the necessary education and/or experience for this task. In any case, the inspection team and the caseworker should together review the facility's file (licensing paperwork, inventory forms, correspondence, etc.) and discuss the issues that should be covered during the visit.

### CREATE A LIST OF FOCUS POINTS FOR THE INSPECTION

---

Points to discuss with the caseworker should include such things as:

- Licensing status: is the facility still properly licensed for all of its current activities?



- The Vulnerability Assessment and Security Plan: does it need to be updated?
- Inventory reporting: does the facility properly report all changes in controlled inventory (purchases, sales, handovers and disposals)?
- Inventory updating: does the facility correctly update its lists of controlled inventory?
- Reporting practices in general: does the facility properly report all relevant changes (staffing, building use, etc.) before they take place?
- Procedures: has the facility prepared written descriptions of all biosecurity-related procedures? Are the procedures adequate?
- Training: is all staff training properly documented?
- Physical security: are all physical security installations properly documented to reflect the required level of security?
- Changes at the facility: are there any new buildings, new controlled equipment, new projects, etc. that the inspector should see or ask about?
- Are there any other issues that the inspector or the caseworker feels are important?

Any uncertainties about the issues mentioned above should become part of a list of focus points that should be addressed during the inspection visit.

### BEGIN THE VISIT BY SPEAKING WITH THE RESPONSIBLE MANAGER

---

A typical agenda for an inspection visit could look something like this:

- Opening meeting
- Review of the facility's biosecurity



- Tour of the facility
- Internal meeting of the inspection team
- Closing meeting

Both the responsible manager and the Biosecurity Officer should be present at the beginning of the visit. In most cases, the manager won't need to attend the entire opening meeting, but the inspectors should at least have a talk with him or her about biosecurity.

For this interview, it will sometimes be relevant to bring up some of the previously mentioned focus points. But it is also important to try to get an idea of the manager's attitude towards biosecurity in general. Does he or she understand the importance of licensing, physical security, biosecurity procedures and inspections?

### REVIEW THE BIOSECURITY DOSSIER WITH THE BIOSECURITY OFFICER

---

After speaking with the manager, it's time for an in-depth talk with the Biosecurity Officer.

At this point, the Biosecurity Dossier should be made available to the inspectors, who need to make sure that the information in it (license information, inventory accounting, physical security certificates, personnel lists, written biosecurity procedures, etc.) is complete, up to date and adequate.

Inspectors should talk to the Biosecurity Officer about the focus points and about biosecurity practices and attitudes in general at the facility.



## A CONFLICT OF INTERESTS

---



Inspection visits can sometimes reveal situations that need to be remedied. This photo shows a

real-life example of how fire safety regulations can cause a difficult conflict with biosecurity needs. As you can see, the door is equipped with a code lock for extra security. But immediately next to this system is a manual override to allow escape in case of fire, which of course makes the code lock useless.

## ALLOW ENOUGH TIME FOR QUESTIONS AND LEARNING

---

Inspectors can also take this opportunity to review the duties of a Biosecurity Officer and give him or her a chance to ask questions.

In our experience, Biosecurity Officers often have many questions, so it's important to allow enough time for this. They may, for example, need advice about teaching, or advice on how to get support from management or colleagues for the implementation of new biosecurity procedures. Or they may need to update their knowledge of new biosecurity requirements.

Over the years, we have found that this type of communication is just as important as checking the facility's biosecurity procedures and physical security, because it involves learnings that will strengthen the biosecurity culture.



## PAY ATTENTION TO PROJECTS INVOLVING DUAL-USE TECHNOLOGY

---

While interviewing the Biosecurity Officer, it's always a good idea to talk about the activities and projects that are taking place at the facility. New projects, for example, may involve new types of controlled biological substances, and the Agency needs to be sure that the facility has remembered to get these substances licensed.

Another reason to discuss new or ongoing projects at the facility is that some of them could involve dual-use technology. We will discuss this type of technology in greater detail in Chapter 18, but at this point we may note that dual-use technology is not a substance or piece of equipment. It is *knowledge and information* (for example, new gene-modifying techniques that can make a bacterial infection less treatable) that can be used for legitimate purposes but can also be used to create a biological weapon.

At the very least, the Agency should be aware of these projects and consider whether they should be licensed or monitored. As previously mentioned, you can read more about the technical and ethical aspects of dual-use technology in Chapter 18.

## COMPARE WRITTEN INFORMATION WITH ACTUAL CONDITIONS

---

After meeting with the responsible manager and the Biosecurity Officer, it's time for a guided tour of the facility. Inspectors should be well-prepared and know what they want to see and ask about.

Your guide on this tour should be the Biosecurity



Officer, who should also bring along the biosecurity dossier. With the dossier in hand, inspectors can compare the written information in it with the actual conditions at the facility.

During the tour, the primary inspector will be in constant dialogue with the Biosecurity Officer, so it will be up to the assistant inspector to take notes and act as an extra pair of eyes and ears. This includes asking supplementary questions and, if necessary, taking photographs.

**See box** on page 215, 'Photos from an inspection must be protected'.

### ASK ABOUT ANYTHING THAT SEEMS RELEVANT

During the tour of the facility, particular attention should be paid to laboratories, production areas and storage areas, especially with regard to the presence and/or use of controlled materials. If the inspector is in doubt about whether a particular substance or piece of equipment is licensed, he or she should ask about it.

Other points to remember during the tour include:

- physical security: ask to see alarms, card readers, security fencing, cameras, etc. and ask how they work.
- speak to an 'ordinary' employee (Employee Group 2 or 3): ask whether that person has been trained in biosecurity and has participated in biopreparedness exercises. Make a note of the person's name.

A final word on inspections: checklists and focus



points are fine as reminders, but it's also important to react to observations that may not be on the to-do list. This requires nothing more than an alert mind and a dose of common sense. An inspector should be able to ask about anything that seems relevant.

### DISCUSS BOTH POSITIVE AND NEGATIVE IMPRESSIONS

---

Once the inspection is finished, the inspectors should take a few minutes in private to discuss their impressions from the interviews and the guided tour. After that, a final meeting can be held at which the inspectors review their impressions together with the Biosecurity Officer (and, if needed, the responsible manager) and tell them what they can expect to see in the final inspection report.

At this meeting, it will be important to highlight the positive aspects of the visit as well as any biosecurity flaws that may have been observed.

### FOLLOW UP WITH A LIST OF NECESSARY ACTIONS

---

Back at the Agency, the inspection team may want to have a follow-up meeting with the relevant caseworker before preparing the previously mentioned follow-up report. It should be sent to the facility within a reasonably short period of time after the visit (2-3 weeks or so). The report should include:

- general impressions – positive as well as negative – from the visit
- a list of any deviations from biosecurity regulations



- a list of any corrective actions that the Agency may require, along with deadlines for implementation
- requests for any missing documentation – e.g. written biosecurity procedures, technical specifications for security equipment, proof of training, etc.

The Agency may also want to include non-mandatory recommendations, such as an offer to provide biosecurity instruction to the facility's employees.

#### PHOTOS FROM AN INSPECTION MUST BE PROTECTED

---

Taking photos during an inspection visit will not always be necessary, but the facility should be informed ahead of time that the Agency may want some pictures to document problems or resolve issues that are in doubt. This could, for example, involve taking a photo of a piece of equipment that may or may not be licensed.

It goes without saying that taking a picture in a laboratory full of controlled materials – and perhaps also some trade secrets – is a highly sensitive matter. The facility must be able to rely on the Agency's absolute discretion, and the primary inspector should clearly inform the facility of how any photographs will be treated.

Photographs from an inspection visit should be stored electronically and protected with an access code. The photographs on the camera itself should then be permanently deleted.



## MAKE SURE THAT ACTIONS ARE IMPLEMENTED ON TIME

---

Once the report has been sent, it will be up to the caseworker to make sure that the facility takes the required follow-up action. This includes reminding the facility of any deadlines – and reacting if deadlines are not met. When the corrective action has been taken, the caseworker should make a note of this for the case file.

Follow-up work can sometimes take a long time to complete, especially if it involves deadlines that need to be extended. The case should be kept open until every loose end has been ‘tied’.

## PROBLEMS DURING THE INSPECTION REQUIRE DIPLOMACY AND TACT

---

As indicated above, an inspection team can occasionally run into problems during an inspection. For example, a responsible manager may refuse to participate in a meeting, or will not grant access to the areas, documents or persons that the team needs to see. Inspectors may also be refused permission to take necessary photographs.

There may also be other kinds of difficulties. The facility may repeatedly ask to reschedule a planned inspection, or ‘forget’ to book a meeting room on the day the inspection is set to take place. In other cases, the tone of a meeting can actually become too ‘cozy’, with lots of irrelevant chatter that prevents the inspectors from getting down to business.

Dealing with these issues requires both firmness and tact, and inspectors should always try to re-



solve any issues in a diplomatic manner. In cases where the conversation seems to be getting off-track, it might just be a question of respectfully re-taking control of the agenda.

### **IF NECESSARY, AN INSPECTION CAN BE HALTED**

---

Proper training will help prepare inspectors for such difficulties.

**See page 219, 'Lessons learned: Inspectors need specialised training'.**

But sometimes, despite the inspectors' best efforts, it will not be possible to resolve the problem on-site. In such cases, the team should be prepared to stop the inspection altogether and return to the Agency.

The most powerful persuader in these cases is your country's Biosecurity Law, which legitimises the inspection process and places the facility at risk of losing its license if it refuses to cooperate. A registered letter, addressed to the responsible manager and referring to the legal consequences of non-cooperation, will almost certainly open the necessary doors and enable a new inspection to take place.

### **A FINAL NOTE ABOUT ON-SITE BEHAVIOUR**

---

Apart from any specialised training, inspectors should also observe some common-sense rules about how to behave during an inspection. They should be neatly dressed, and their tone of address should be professional, respectful – and firm when necessary. If at all possible, the inspection



should be conducted as a friendly dialogue rather than a confrontation.

The primary inspector should be allowed to take the lead during the inspection, and any disagreements between the two inspectors should only be discussed in private. Supplementary questions from the assisting inspector should never appear to contradict the primary inspector.

It is in the nature of their job that Agency inspectors will become privy to highly sensitive information, and this is a privilege that must not be taken lightly. Information from the facilities must always be securely stored and protected, and inspectors must never give an impression of treating this information carelessly.



**Lessons learned:****INSPECTORS NEED SPECIALISED TRAINING**

---

To perform their job effectively, Agency inspectors will need special training in such areas as questioning techniques and the handling of potential conflicts. They should also learn how to plan their visits, write follow-up reports and handle deviations and/or non-compliance with biosecurity regulations.

In Denmark, we have found it practical to share this training task with a specialised, external consulting firm. Together with the consultant, we have designed a two-day training programme that is customised to our needs and to the requirements of our Executive Order.

The course is run by the consulting firm and includes both theoretical instruction and practical role-playing.

In addition to the above, Danish inspectors must also receive practical, peer-to-peer training as assistant inspectors before they are allowed to take on the primary responsibility for an inspection.





# SECTION 3:

## IMPORTANT BIOSECURITY ISSUES

---

In this section, you will encounter a number of scientific and ethical issues that require extra reflection. Among other things, we will present an ethical code that asks for a level of personal commitment from everyone who works in the life sciences.

We will also examine the thorny question of how to promote free scientific inquiry while protecting society from scientific knowledge that serves perverted ends. We will discuss the choices made by 'the bad scientist' and the need for responsible scientific practices and bioethical education. And we'll take a look into the future, at the emerging technologies that pose even greater challenges to biosecurity than the ones we face today.

We will conclude this section – and this book – with some open-ended dilemmas that invite further discussion and thought.





## CHAPTER 17:

# BIOSECURITY CULTURE AND BIOETHICS

*Biosecurity culture has an ethical dimension that requires personal engagement as well as a commitment from the entire scientific community.*



**W**e have already touched upon biosecurity culture in several chapters of this book. Among many other things, it is the force and spirit that ensures the success of procedures for physical security, employee security and inventory control.

But every task and issue described in this book has in fact a 'cultural' aspect that is more about mindset and ethics than about rules and regulations. At its heart, Biosecurity culture is a workplace ethic that combines an understanding of why a biosecurity system is necessary with a willingness to make that system work.

### SCIENTISTS MUST BE COMMITTED TO BOTH SECURITY AND SCIENCE

---

This willingness and understanding was markedly absent at the military research laboratory which, by all accounts, was the source of the anthrax attacks of 2001.

One person sent the letters filled with deadly spores. But the entire disaster might have been prevented if anyone from the laboratory staff or management had stepped in to stop the spiral of events. No one did.

As pointed out in the introduction to this book, the lack of awareness, procedures and respect for biosecurity made it easy to steal dangerous materials from the facility and cause great harm with them.

In 2002, one year after attack, an independent security review performed by Sandia National Laboratories pointed out that there were still a great



many critical weaknesses at the facility. Among other things, the report mentioned:

- the lack of an overall security plan
- an inadequate alarm system
- a vulnerable IT system
- inadequate background checks of employees with access to controlled substances
- inadequate inventory control

But at the heart of it all was a lack of biosecurity culture:

“Perhaps the most important observation in this report is that the culture... (at the facility, ed.) does not reflect the same indisputable commitment to security as it does to research,” the report stated.

### A BIOETHICAL CODE – AND A COMMITMENT TO DO NO HARM

---

Biosecurity has been vastly improved in the US since the Sandia report was written. But the report’s key observation is still relevant for facilities and scientists around the world.

Quite simply, it is not enough to be committed to the principles scientific inquiry. A responsible scientist should be equally committed to ensuring that his or her discoveries and knowledge cause no harm. This is the essence and the ethic of biosecurity culture.

It is of course also the essence of the Hippocratic Oath, to which any scientist with a medical degree is already bound.



On 25 March 2005, the scientific journal *Science* published a 'Code of ethics for the life sciences' that spells out this bioethical commitment in greater detail. It represents an attempt by the authors to create an international consensus in the scientific community about its ethical obligations to society.

**You will find** a summary of this code on page 231-232.

### BIOSECURITY CULTURE GOES HAND IN HAND WITH BIOETHICS

---

In reading through this ethical code, you will hopefully recall a number of biosecurity issues that have already been raised in this book. Among other things, the code expresses the scientific social responsibility mentioned in Chapter 6, and it underscores the principles of restricted access described in Chapters 10, 11 and 12. It should also call to mind the whole purpose of biosecurity legislation and control.

Perhaps most importantly, the code highlights the need for a sense of personal responsibility that is the focus of Section 3 in this book. All the biosecurity issues we raise in this section call for personal reflection – and a willingness to act.

This goes beyond the responsibility to notice and report odd or suspicious circumstances. We have already discussed the importance of such action, but there is another aspect of biosecurity culture that involves issues of conscience.



## THE THREE BIOETHICAL COMPETENCES

---

To deal with the difficult ethical issues that are inherent in the life sciences, three basic, bioethical competences are needed.

- Awareness – recognising that risks and dilemmas exist, and being able to spot them.
- Reflection – weighing the benefits of a scientific project against the possible harm it could cause.
- Action – taking steps to achieve an acceptable balance between science and biosecurity.

These bioethical competences should be part of the training for anyone pursuing an education within the life sciences. But it is equally important to impart this knowledge to those who are already employed in this field: the scientists, the laboratory assistants, the technicians and especially the leaders.

## THE 'BAD SCIENTIST' MAKES UNETHICAL CHOICES

---

No effective biological weapon of mass destruction can be developed without the help of someone with the necessary scientific know-how. This may sometimes involve the classic 'mad scientist' – but it is more likely that the helper is a 'bad' scientist: a person of sound mind who has made a conscious choice to use his or her expertise to serve a harmful, destructive purpose.

Naïve scientists who simply assume that any science is responsible science can make equally bad choices without necessarily meaning to.



Point 8 of the ethical code challenges everyone who works in the life sciences to make different kind of choice – a choice to say “no” to any type of research they consider unethical.

In the same manner, Point 3 of the code challenges the members of the scientific community to alert the public or the appropriate authorities to any activity that is likely to contribute to bioterrorism or biowarfare.

### THE SCIENTIFIC COMMUNITY MUST INVOLVE ITSELF IN BIOETHICS

---

Most of the points in the ethical code require a collective as well as an individual commitment. Difficult, individual choices need to be supported by a responsible scientific community that has agreed to abide by a set of rules and procedures and is willing to discuss its work from a bioethical point of view.

Such discussions should have their natural place in scientific publications, at meetings of scientific societies and at congresses, workplaces and educational institutions. Relevant political discussions and public hearings also need thoughtful input from the scientific community.

Critical reviews of research proposals and peer reviews of scientific articles should also include a discussion of ethical issues – particularly if the project or article in question involves technologies with a potential to cause harm. We will discuss this issue in greater detail in Chapter 18, ‘Dual-use technology’.



## STUDENTS SHOULD LEARN TO DEAL WITH ETHICAL DILEMMAS

---

We have discussed the importance of biosecurity education several times in this book. An understanding of biosecurity procedures and the reasoning behind them is a prerequisite for good biosecurity culture, and this applies not only to Agency employees, Biosecurity Officers and facility staff but to politicians, students and any other relevant group.

In 2012, the Danish Agency developed and launched an educational programme aimed at giving university students within the natural sciences a set of ethical competences that can prepare them to deal with the scientific and ethical dilemmas they may encounter during their careers.

**See box** on page 227, 'The three bioethical competences'.

This instruction is based on the bioethical code described in this chapter. Theoretical aspects of bioethics and biosecurity culture are supported by real-life scenarios in which students discuss how they might react if they were in the same situations.

## SCIENCE DOES NOT EXIST IN A SOCIAL AND POLITICAL VACUUM

---

It could be argued that pure science has no ethical aspect – that the 'evil' resides only in the applications that are attached to scientific discoveries, and that no biosecurity or other regulatory require-



ment should hinder the pursuit of pure knowledge. This argument more or less presupposes the existence of a 'golden age' of unfettered scientific freedom.

But the world has changed – if indeed a 'golden age' ever really existed. Today, at any rate, the scientific community does not exist in a social and political vacuum. It must relate and respond to threats from terrorist groups and hostile governments – and live with political pressure and public opinion.

If it does not – if the community chooses to isolate itself from the needs and requirements of society – it may find itself confronted with other types of obstacles. As mentioned in Chapter 3, for example, negative public opinion and political backlash can slow or even stop scientific development in certain areas.

Moreover, it is not impossible to imagine a scenario in which a research facility is forced to shut down altogether if a biological attack or disastrous accident is traced back to the facility's own lack of biosecurity culture. When public trust is broken, a facility's prestige may be lost – not to mention its funding, its license, or both.

### SCIENTIFIC OPENNESS CAN PROMOTE PUBLIC TRUST

---

Maintaining public trust – and thereby ensuring the freedom to pursue responsible scientific goals – is a balancing act in which the scientific community must learn to use openness as well as caution.

For example: if a particular project has attracted



negative public attention, the questions that are raised should be addressed openly from a scientific community that has already weighed the ethical and security-related pros and cons of the issue.

A well-prepared explanation of costs and benefits, and a de-mystification of risks is a more trustworthy approach than a tight-lipped “no comment”. Security and confidentiality do not need to be compromised if the arguments are sufficiently well considered.

### SCIENTIFIC KNOWLEDGE CAN ALSO RAISE BIOETHICAL ISSUES

---

Point 5 of the ethical code deals with an area of biosecurity that is of increasing concern and which raises some very difficult questions. It is not about the spread of biological pathogens; it is about the dissemination of information and knowledge.

We will deal with these issues in the next chapter.

### CODE OF ETHICS FOR THE LIFE SCIENCES

---

All persons and institutions engaged in any aspect of the life sciences must

1. Work to ensure that their discoveries and knowledge do no harm.
2. Work for ethical and beneficent advancement, development, and use of scientific knowledge.
3. Call to the attention of the public, or appropriate authorities, activities (including unethical research) that there are reasonable grounds to believe are likely to contribute to bioterrorism or biowarfare.





4. Seek to ensure that only persons with a strong sense of bioethics are allowed access to biological agents that could be used as biological weapons.
5. Seek to restrict dissemination of information and knowledge that could be used for bioterrorism or biowarfare to those who need to use this knowledge for beneficial and legitimate purposes.
6. Review and monitor research activities to ensure that the benefits of this work outweigh the risks.
7. Abide by laws and regulations that apply to the conduct of science unless to do so would be unethical, and recognise a responsibility to try to change laws and regulations that conflict with ethics.
8. Recognise, without penalty, all persons' rights of conscientious objection to participation in research that they consider ethically or morally objectionable.
9. Faithfully transmit this code and the ethical principles upon which it is based to all who are or may become engaged in the conduct of science.

---

**Source:**

Margaret A. Somerville and Ronald M. Atlas, *Ethics: A Weapon to Counter Bioterrorism* (Science, vol. 307, 1881-1882, 25 March 2005)

---







## CHAPTER 18:

# DUAL-USE TECHNOLOGY

*Legitimate scientific knowledge that can be used to create a biological weapon raises special concerns for the scientific community. Can such knowledge be openly shared at conferences, in scientific publications and elsewhere?*



In February 2001, a group of Australian scientists published an unexpected and disturbing discovery. In their efforts to make a mouse contraceptive vaccine for pest control, they had come to develop a gene-modified version of the mousepox virus that killed all of its victims by inhibiting a part of their immune system.

The virus turned out to be so 'effective' that it even killed half of the mice that had been immunised against it.

When the discovery was published in the *Journal of Virology* along with a description of materials and methods, it raised highly-publicised fears that the technology developed in the mousepox experiments could be used to create a similarly modified smallpox virus. In a world where smallpox has been eradicated, and where immunisation against the disease no longer takes place, this would be a catastrophe.

Even if immunisation were re-introduced, such a virus would have huge potential as a biological weapon.

### SENSITIVE TECHNOLOGY CAN BE AS DEADLY AS A PATHOGEN

---

The operative word in this scenario is *technology*. A laboratory can be secured against theft or accidental release of a virulent pathogen. But what about the *technological know-how* that is published in scientific journals around the world?

Such knowledge could enable others to produce the same or perhaps a similar and even more



deadly pathogen without ever coming near the laboratory where it was first created and stored.

This is the dilemma of *dual-use technology* (also referred to as *dual-use research of concern*, or DURC). How can society be protected against a legitimate (or accidentally discovered) and publicised technology that could also be used as a blueprint for a weapon of mass destruction?

### 'HARMLESS' SUBSTANCES CAN CREATE YET ANOTHER DILEMMA

---

Another dilemma is the fact that dual-use technology can involve harmless and therefore unregulated substances such as the mousepox virus. Persons or facilities who work solely with such materials are not necessarily subject to the laws that regulate the use of more dangerous pathogens.

As we have demonstrated, however, an individual or a facility can use harmless materials to create substances that are every bit as dangerous as smallpox, anthrax or other types of regulated biological agents. The Agency should therefore know about such work and regulate it if necessary.

But how can the Agency find out about potentially dangerous experiments when the facilities performing them are not licensed? How can it deal with a problem about which it does not even know?

### DUAL-USE TECHNOLOGY IS KNOWLEDGE THAT CAN BE MISUSED

---

In the context of this book, dual-use technology involves any kind of legitimate biological know-how with the potential for misuse. Such knowledge



may be found in scientific publications, but it can also reside in educational materials, a conference presentation, unpublished manuscripts, data sets, laboratory procedures – or simply within the mind of the scientist.

A document known as the Fink Committee Report lists several classes of experiments that should be of particular concern to this discussion. Inspired by this report, we may note that dual-use technology could, for example, include experimentally-generated knowledge of how to:

- change a pathogen to make it undetectable or resistant to vaccines or treatment
- change a pathogen's host spectrum
- augment the pathogenic potential of a microorganism
- augment the infectiousness of a pathogen
- create new biological substances that could cause serious harm
- create new delivery systems for biological substances via aerosols, drinking water, foodstuffs, etc.

The Fink Committee Report was published in the US in 2004 by the National Academies Press. It was the first National Academies report to examine national security and the life sciences.

### DUAL-USE TECHNOLOGY RAISES ETHICAL AND SCIENTIFIC ISSUES

---

Dealing with dual-use technology can require careful thought and reflection. The issues raised in this area have implications for everything from research and security to scientific publishing, public communications and a variety of ethical issues.



Public opinion can also be a concern. As we have also discussed in Chapters 3 and 17, negative publicity can create a public and political reaction that can bring legitimate scientific efforts to a standstill.

In one well-known case involving dual-use technology, it was the scientific community itself that imposed a moratorium on research.

**See box** on page 245-246, 'Dual-use controversy halted scientific development'.

### SCIENTISTS MUST BE AWARE OF DUAL-USE TECHNOLOGY RISKS

---

Determining the dual-use potential of a given technology is not a simple question. Scientists working on a particular project are of course interested in generating new knowledge, and it is part of the scientific process that such knowledge must be shared.

The danger of sharing this knowledge with the 'wrong' people does not necessarily enter into the discussion. It is important, however, for the scientific community to be aware of the dual-use problem, and to seek help to assess and reduce any risks.

It is also important for the Agency to be able provide this kind of help. As indicated in Chapter 4, the Agency should be able to 'think like the enemy' and thus spot any potential for misuse.

### DUAL-USE TECHNOLOGIES CAN BE LICENSED

---

The Agency should also consider issuing licensing requirements for dual-use technologies. The



Danish Executive Order, for example, empowers the Agency to regulate existing dual-use technologies as well as potential dual-use technologies that are still only in an experimental stage.

In other words, the Agency can review the design and purpose of an experiment before it begins and issue specific licensing requirements for how it may be conducted. Or it can review the results of a completed experiment and issue licensing requirements for how these results may be published.

In the sections below, you will find descriptions of how such reviews can be conducted and the type of licensing requirements that could be issued.

Regardless of whether a technology is licensed or not, however, the Agency should be prepared to give advice on how risks can be reduced. In the sections below you will also find specific suggestions on how to reduce risks.

### THE RESPONSIBILITY FOR PREVENTING MISUSE SHOULD BE SHARED

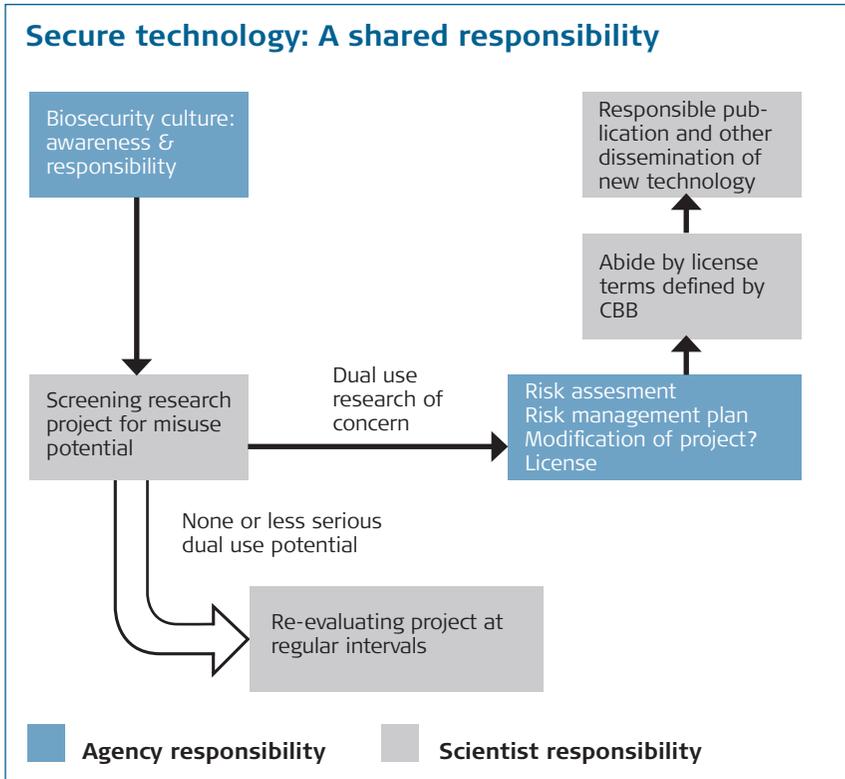
---

The Agency should not be alone in dealing with the risks of dual-use technology. At the institutional level, the facilities – and, more specifically, the scientists who work there – should also bear some of the responsibility for ensuring that dual-use technologies are not misused.

The flow chart pictured in fig. 8 on page 241 describes how these responsibilities could be shared.

As an additional aid, you will find a questionnaire





**Fig. 8:** The responsibility for preventing the misuse of dual-use technology should be shared between the Agency and the facilities that work with such technology.

on the CBB website that is designed to help determine whether or not a given project may involve dual-use research of concern.

### THE AGENCY SHOULD CONDUCT DUAL-USE EDUCATION

As indicated in the flow chart, the Agency should educate the scientific community about dual-use technology.

Scientists at the facilities should learn how to spot projects that involve dual-use research of concern



and assess whether such projects involve serious risks. They should also learn to regard this type of assessment and reflection as a natural part of the scientific process.

The dual-use issues described here relate directly to point 5 of the 'Code of ethics for the life sciences' discussed in Chapter 17. They also relate to the three ethical competences which are also discussed in that chapter. So in addition to talking about risks and mitigation, the Agency's instruction about dual-use technology should also cover both the code and competences.

### SCIENTISTS SHOULD SCREEN THEIR OWN PROJECT PROPOSALS

---

Armed with the knowledge and competences needed to deal with dual-use technology issues, it should be the scientists' responsibility to screen their own research proposals and look for dual-use technology risks.

Projects with little or no potential for misuse can be set in motion after the initial screening. They should, however, be regularly reviewed to ensure that new developments or discoveries have not changed the initial risk assessment.

If the initial screening reveals a more serious risk of misuse, the Agency should be consulted for a closer look at the risks. The Agency can then help create a plan for how these risks may be addressed.

### THE AGENCY SHOULD PROVIDE RISK-REDUCING ADVICE AND REGULATION

---

A risk-reducing plan from the Agency could, for ex-



ample, include a recommendation that particularly sensitive methodologies be omitted from article manuscripts prior to publication. This would not necessarily stifle scientific inquiry; colleagues with a legitimate wish to repeat a given experiment can be advised to contact the authors directly.

The Agency might also suggest adjustments to a particular study design. This could, for example, involve the use of a less pathogenic virus or a synthetically constructed microorganism that is weakened in such a way that it cannot survive outside a laboratory. In addition, the Agency may wish to restrict participation in the project to a few, trusted persons.

If your country has decided to have licensing procedures for dual-use technology, the Agency can also decide whether the technology in question needs to be licensed. Such a license could require adherence to specific biosecurity requirements that are set up by the Agency.

#### OTHER TYPES OF AGENCY INTERVENTIONS MAY ALSO BE NEEDED

---

If the situation requires it, other interventions may also be necessary. Apart from the above-mentioned actions, The Danish Executive Order, for example, empowers the Agency to:

- require background and security checks of persons involved in a particular project
- require a security plan that specifically states how sensitive information will be protected
- withdraw a license and close the project altogether
- take police action that could involve fines and imprisonment



## EDUCATION MUST REACH BEYOND THE LICENSED COMMUNITY

---

Education is necessary to achieve the cooperation described above between the Agency and the licensed scientific community. But this type of awareness-raising is also key to solving the dilemma of unregulated activities mentioned earlier in this chapter.

We have previously indicated that biosecurity education should reach beyond the licensed scientific community. In the context of dual-use technology, it should include relevant student groups, unregulated facilities and even amateur scientists that might one day work with dual-use technology.

By aiming broadly, the Agency can reach out and raise awareness of dual-use problems and dangers among persons with whom it would not otherwise be in contact. If the education is effective, then these persons will hopefully come to the Agency of their own accord if they ever need advice and help with dual-use technology.

The Agency should not necessarily be the only provider of this type of biosecurity education.

Universities and other educational institutions could also include it in relevant areas of their own instruction. The Agency could of course suggest this to the educational institution and assist in designing the course.

We will return to the issue of educational outreach in Chapter 19, 'Future challenges'.



## NEW TECHNOLOGICAL CHALLENGES ARE ON THE HORIZON

---

In 2008 – seven years after the mousepox story created an international furor – the two scientists who led the project pointed out in an interview that there had been no one to advise them about dual-use issues when they published their work. Their article had of course been peer-reviewed, but no biosecurity problems had been flagged during this process.

This situation is beginning to change as worldwide awareness of dual-use risks increases. But as one of the Australian researchers pointed out, the world is facing even greater challenges today, thanks to such emerging technologies as synthetic biology.

Instead of modifying a natural virus to make it more virulent, scientists are now developing capabilities that could allow them to design and make their own.

In the next chapter, we will discuss this and other future challenges to biosecurity.

## DUAL-USE CONTROVERSY HALTED SCIENTIFIC DEVELOPMENT

---

In January 2012, a group of the world's most prominent virologists took the highly unusual step of halting their own work with the avian flu virus H5N1. Their self-imposed moratorium – which lasted for an entire year – was the result of a public controversy about dual-use technologies that showed how the 'bird flu' could be mutated into an airborne virus that affects mammals.





The technologies had been developed by two scientific teams – one Dutch and one American. Both were trying to gain knowledge that could help prevent the spread of the mutated virus, which is fatal in 60% of all cases affecting humans.

The fact that their technologies could possibly be used to create a biological weapon did not become an issue until they submitted their research for publication in *Science* and *Nature*, respectively. Both magazines insisted on risk assessments by the US-based National Science Advisory Board for Biosecurity (NSABB) before publication.

When this requirement became publicly known, the community of virologists mentioned above decided to send a dramatic signal about the need for public discussion and reflection: they simply stopped their project.

In the end, the NSABB decided that slightly revised versions of both studies could safely be published. At the same time, however, the Board underscored an “urgent need for the further development of processes for the responsible communication of dual use research of concern.”

---

**Sources:**

David Malakoff et.al., *In Dramatic Move, Flu Researchers Announce Moratorium on Some H5N1 Flu Research* (ScienceInsider, 20 January 2012)

David Malakoff, *H5N1 Researchers Announce End of Research Moratorium* (ScienceInsider, 23 January 2013)

---







## CHAPTER 19:

# FUTURE CHALLENGES

*Synthetic biology, the wide availability of biological building blocks and a new subculture of unregulated 'garage laboratories' pose special challenges to the future of biosecurity.*



**F**or a number of years now, a worldwide community of amateur biologists has begun to grow and flourish in the wake of emerging and increasingly accessible biotechnologies. Community members describe themselves as ‘citizen scientists’, ‘bio-hackers’ or simply ‘do-it-yourself biologists’.

For some, their chosen hobby is an amusing combination of entertaining experiments and personal curiosity. Others pursue a more goal-oriented path and have developed some surprising capabilities within the emerging field of synthetic biology.

We will return to the subject of amateur biologists later in this chapter.

### SYNTHETIC BIOLOGY PRESENTS A NEW DUAL-USE CHALLENGE

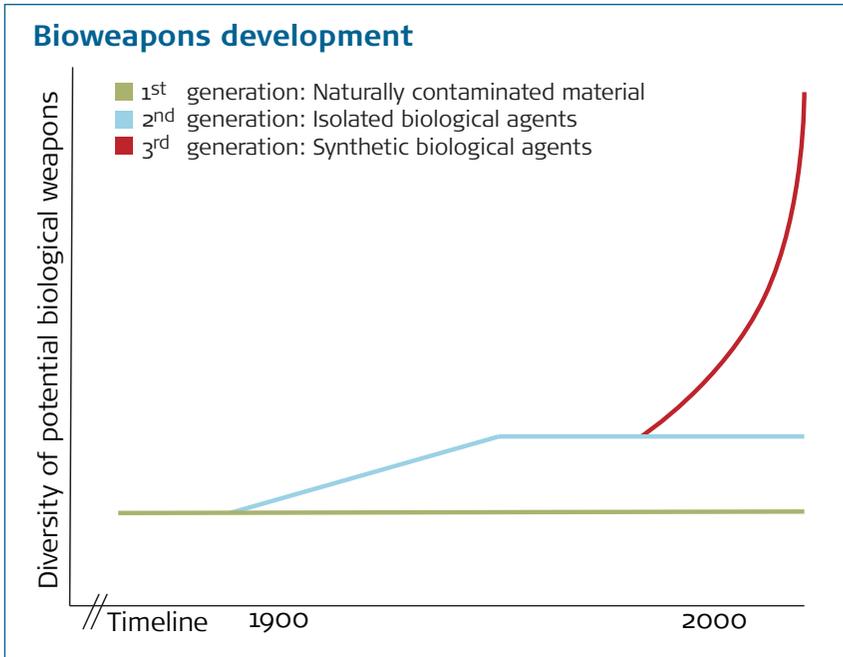
---

Synthetic biology is in itself a biosecurity challenge. In essence, it is an emerging technology that reaches beyond genetic engineering: instead of merely modifying a naturally-occurring genome, scientists are now beginning to synthesise their own strings of DNA.

These sequences are then used as building blocks from which ‘designer cells’ can be created.

The goal of synthetic biology is to create new life forms that perform useful functions. From a biosecurity point of view, however, the same technology could be put to extremely destructive use. A bioweapons manufacturer with the necessary materials and know-how could create a completely custom-made arsenal.





**Fig. 9** A third generation of biological warfare agents could in future dramatically increase the number of available bioweapons.

### A THIRD GENERATION OF BIOWEAPONS IS NOW EMERGING

Concerns have been expressed that a third generation of bioweapons, created with the help of synthetic biology, could exponentially increase the number, type and effectiveness of the biological weapons available to rogue governments and terrorist cells (see fig. 9). Such weapons could be designed with more frightening characteristics than anything seen to date.

It should be remembered, however, that it is still no simple matter to create a new type of virus or bacteria that is capable of surviving outside the laboratory. It is a technique that will probably not become 'ordinary' until some point in the distant future.



Synthesising an existing virus such as smallpox, for example, could pose a more immediate danger because it is 'naturally' viable. Moreover, the entire DNA sequence for smallpox has already been published – and the world's population is no longer vaccinated against the disease.

### MATERIALS AND KNOWLEDGE ARE BECOMING MORE ACCESSIBLE

---

At this point in time, creating a weapon with synthetic biology would still require financial resources equivalent to that of a state-funded weapons programme. In recent years, however, the basic materials and knowhow of synthetic biology have become both less expensive and more accessible.

Thanks to Internet sites such as [biobrick.com](http://biobrick.com), the standardised DNA sequences that are the building blocks of synthetic biology can be ordered online. The Internet can also provide a good deal of know-how through published articles and web-based communities.

### THE BUILDING BLOCKS OF SYNTHETIC BIOLOGY SEEM HARMLESS

---

In this book we have described a variety of steps that can be taken to prevent biological substances and know-how from ending up in the 'wrong' hands.

Laws can be enacted; employees can be security-trained; facilities can be physically protected. Exports of controlled substances and technology from professional facilities can be regulated, and potential customers can be screened. Members of



the scientific community can exercise caution with regard to how they share their knowledge.

With synthetic biology, however, there are special challenges. While the destructive potential of 'natural' viruses and bacteria is easy to spot, the individual building blocks of synthetic biology are completely harmless. So even the most cautious retailer may find it difficult to determine whether a potential buyer plans to use these substances for peaceful or destructive purposes.

### SPECIAL PROTECTIONS ARE NEEDED TO PREVENT ABUSE

---

One way in which synthetic biology can be protected from abuse is for retailers to screen all orders for DNA sequences and match them against a list of critical gene sequences in microorganisms that are known to be suitable for weaponisation. At the same time, retailers can keep customer records that make it possible to trace all orders.

Most professional retailers of biological building blocks already use this system – but there are still some who do not.

Another method of protection is to construct synthetic gene sequences that contain a unique signature sequence – a so-called 'watermark'. If the watermark should later turn up in an illegal product, it can help investigators discover the source of the misuse.

Scientists who work with synthetic biology can also help prevent misuse by ensuring that the organisms they create and work with are not viable outside a laboratory environment.



## NEW TECHNOLOGIES CAN ALSO IMPROVE BIOSECURITY

---

Some new technologies are not a challenge to biosecurity – on the contrary, they can actually improve it.

A good example of this is culture-independent diagnostics – an emerging technology that bypasses the need to culture organisms as part of the diagnostic process. Newer and faster molecular methods are used instead.

This can entirely eliminate the need for many diagnostic facilities to work with controlled substances. From a biosecurity standpoint, this is good news, insofar as it also lowers the statistical risk of theft, accidents and misuse of these dangerous biological agents.

## NON-PROFESSIONAL BIOLOGISTS CAN CHALLENGE BIOSECURITY

---

Like the other biosecurity systems described in this book, the above procedures are designed for use by scientific professionals who work with controlled biological substances and related materials.

In the future, however, we must also consider individuals and groups who are not members of the professional community and who are not covered by the legislation and controls we have recommended. As mentioned at the beginning of this chapter, there is now a growing, worldwide community of amateur biology enthusiasts, some of whom have begun to work with relatively advanced biological materials and technologies.



The question is: can this group undermine the biosecurity system we have presented in this book?

### AMATEUR BIOLOGISTS ARE A HIGHLY DIVERSE GROUP

---

'Citizen biologists' contribute to the amateur biology subculture in a variety of ways. Some work alone in basements and garage laboratories; others pursue their hobby in community workspaces or 'labitats' where they can share ideas and view each others' experiments.

Their projects range from creating synthetic life forms out of standardised DNA sequences to building inexpensive yet surprisingly sophisticated laboratory equipment. Some projects are valued at least as much for their entertainment value (glow-in-the-dark plant life) as for their usefulness.

Knowledge is freely shared in laboratories, online, at conventions and through competitions (including an event known as 'The iog Mad Science Contest'). Biological materials are sometimes exchanged through the ordinary postal system.

### A CULTURE OF BIOSAFETY SHOULD BE NURTURED

---

Whether or not the amateur biology trend represents a threat to biosecurity is debatable. The openness of the movement could make it a prime target for theft. On the other hand, it has been argued that amateur biology projects are not something that a terrorist would find worth stealing.

Still, it is probably wise not to underestimate the capabilities that may be found in this highly di-



verse group of enthusiasts. Among other things, we believe the established scientific community should nurture and encourage a culture of safety and security among these amateur groups.

**See page 259, 'Lessons learned: Reaching out to the 'labitats'.**

And at some point, governments may have to consider whether it is possible to introduce some form of official biosecurity regulation within the subculture of amateur biologists.

### FUTURE CHALLENGES REQUIRE NEW APPROACHES TO BIOSECURITY

---

Synthetic biology may be regarded as an enabling technology that will make other advanced biotechnologies more reliable, easier, cheaper and faster. Over time, this will probably lower the bar for the use of these technologies – for legitimate as well as malicious purposes.

In other words, advanced biological weapons that today seem out of reach for all but a national weapons programme may one day be accessible to a much broader range of players. Before this happens, new approaches to biosecurity must be developed to deal with this trend.

### WE MUST FOSTER AN INTERNATIONAL BIOSECURITY CULTURE

---

One possibility would be to establish an international authority to deal with future biosecurity challenges.

Rather than providing an extra layer of legally bind-



ing regulation, such a body could work to foster a voluntary, international biosecurity culture among governments as well as laboratories, retailers and other non-political stakeholders.

This effort could include working with the above stakeholders on issues related to:

- outreach, education and awareness-raising
- science and technology monitoring
- good practices in biosafety and biosecurity
- laws and regulations
- international harmonisation issues

### MODERN THREATS MUST BE MET WITH INTERNATIONAL COOPERATION

---

The above considerations underscore once again the importance of biosecurity culture – now in a context of international cooperation. They also open the possibility of involving a wider community that includes lawmakers as well as amateur biologists and any other type of stakeholder that seems relevant.

Cross-border cooperation should in fact be regarded as a necessary supplement to any national biosecurity regulation. Criminal activities involving potentially dangerous biological substances do not respect national boundaries; substances and materials may be stolen in one country, weaponised somewhere else and then used on a completely different continent.

Extensive international cooperation is also needed so that suspicious players who are denied access to controlled materials in one country cannot turn around and find a new supplier somewhere else.



## EMERGING BIOTECH NATIONS MUST BE MOTIVATED FOR BIOSECURITY

---

If international cooperation is to be truly effective, it must encompass every nation with a biotech industry. This includes countries with emerging economies, for which the biotech business – with all its exciting new technologies and potential for growth – can be an attractive and job-creating development option.

These countries must also be drawn into the international biosecurity culture. To this end, the international scientific community should make its biosecurity expertise and experience available to countries with a budding biotech industry.

At the political level, meanwhile, governments could make the establishment of an effective biosecurity and biopreparedness system a prerequisite for any foreign aid or loan packages related to the biotech industry.

## RESPONSIBLE ACTION IS KEY TO THE FUTURE OF BIOSECURITY

---

If all responsible governments, laboratories, companies, retailers, researchers and even ‘hobbyists’ can successfully create an international culture of safety, security and vigilance, it will make life infinitely more difficult for the thieves, merchants and users of bioweapons.

This, in turn, will pave the way for a future in which the world can stay ahead of the biosecurity curve instead of running behind it.



**Lessons learned:**

## REACHING OUT TO THE 'LABITATS'

We believe it is important to encourage a sense of responsibility among the growing number of unregulated amateur biologists who have begun to experiment with synthetic biology and other new technologies.

To this end, the Danish Agency has begun to visit the workshops and 'labitats' of Danish do-it-yourself (DIY)biologists; our goal is to draw them into the biosecurity culture that is present at professional facilities. DIYers have also been invited to visit the Agency, and have been asked along to meetings and conferences about dual-use research of concern.

By making them feel part of a larger community of responsible scientists, we hope to make it clear that today's new biological building blocks not only represent an exciting scientific frontier – they carry with them an array of practical and ethical obligations.





## CHAPTER 20:

# DILEMMAS FOR DISCUSSION

*In our final chapter, we will present a few scenarios, some thought-provoking questions – and the opportunity to reflect and discuss.*



**B**y now we hope we have made it clear that biosecurity issues are not always cut and dried. Security risks must be weighed against scientific benefits, and sometimes compromise is the only answer to a difficult question.

In this concluding chapter, we will present you with three dilemma scenarios, each of which raises a number of questions. We hope these questions will inspire you to use your knowledge of biosecurity and engage in some useful discussions.

Our first and third dilemmas are real-life case stories; the first is an example of how dual-use technology (in this case, the details of an experiment) can be reviewed for risks before being made publicly available. The third dilemma illustrates how a biosecurity evaluation can result in the exclusion of certain information from a published article.

Our second dilemma is not an actual case. It is an imagined, but realistic scenario designed to provoke some reflections and discussion about employee security.

#### **DILEMMA 1:** **THE 'RESURRECTION' OF THE SPANISH FLU**

---

In 2005, a group of scientists decided to investigate why the so-called 'Spanish flu' virus that killed more than 50 million people in 1918 was so much deadlier than the seasonal H<sub>1</sub>N<sub>1</sub> variant that usually disappears after a few days in bed.

Using material from a Spanish flu victim whose body had been preserved in permafrost, they managed to reconstruct all eight of the viral gene sequences in the killer virus. These were then



installed in a modern flu virus, and the illness it caused in test monkeys was much more serious than an ordinary flu virus would have caused. The Spanish flu had apparently been 'resurrected'.

Before this experiment was published in Science, it was evaluated by the US-based National Science Advisory Board for Biosecurity. The Board decided that the scientific value of this research outweighed the biosecurity risk of publishing all the details of the experiment.

- Do you agree with the Board's decision?
- Do you think the evaluation was necessary?
- What are the risks in this case?
- What are the benefits?

#### DILEMMA 2: THE CARD-CARRYING EXTREMIST

---

Imagine this: a trusted scientist at a private research facility is found to be the member of a legal but highly extremist organisation. The scientist has independent access to controlled pathogens and can work with this material without supervision.

There are no complaints about the work that is performed by this person. He is in fact a highly competent employee and would be an attractive addition to the staff of competing facilities, both national and international.

- Do you think this person poses a security risk?
- Does the value of his work outweigh any risk?
- Should potential employees at high-risk facilities be screened for their beliefs and attitudes?
- Does the fact that the above-mentioned organisation is legal affect your opinion? Why?



### DILEMMA 3: A DISEASE WITHOUT A CURE

---

In 2013, US scientists published an article in the *Journal of Infectious Diseases* about a naturally-occurring strain of *Clostridium botulinum* – the bacteria that causes botulism. What made this strain unique was the fact that it produced a new kind of toxin on which existing antiserums had no effect.

The group had, in effect, discovered a disease without a cure. Based on their own risk evaluation, the scientists decided not to publish the DNA sequence for the new toxin until an effective antiserum had been found. The article did, however, alert health authorities to the existence of the new toxin.

Doubts were later raised as to the scientific validity of the study that identified the new toxin. At the time of this writing, however, the DNA sequence had still not been published, so it has not been possible for others to formally validate the study.

- Do you agree with the scientists' decision?
- Do you think their risk evaluation was necessary?
- What are the risks in this case?
- Would there have been any benefits to publishing the DNA sequence?
- Should scientific information ever be suppressed from publication?
- Does the validity issue in this case affect your opinion? Why?







# GLOSSARY OF TERMS USED IN THIS BOOK



**Analysis**

A methodical study of an area in order to characterise it or create a better understanding of it.

**Application form**

A form to be filled out facilities that wish to obtain licenses from the Agency to possess, use, produce or store controlled materials listed in a biosecurity-related Executive Order.

**Biological agents**

Microorganisms (viruses, bacteria, fungi), parasites or toxins (from living organisms) which can be used offensively.

**Biosafety**

A set of preventive measures, including procedures and proper use of laboratory containment facilities, to prevent unintentional infection of facility personnel and the general population.

**Biosecurity**

A set of preventive measures to protect humans, animals and plants against the malicious use, directly or indirectly, of biological agents, parts thereof, or their toxins.

**Biosecurity Officer**

An employee appointed by the facility to be in charge of implementing and updating biosecurity at the site after having attended a training course offered by the Agency.

**Biosecurity Dossier**

A collection of biosecurity-related documents at a facility, including, for example, its license



application, Security Plan, inventory lists and other documentation relevant to the facility's license. All facilities with a license issued by the Agency should have a Biosecurity Dossier.

**Biological weapon**

A harmful biological substance combined with a delivery system.

**Controlled biological substances**

Human pathogens, zoonoses and toxins in the form of viruses, rickettsiae, bacteria, toxins or sub-units of toxins, some fungi and specific genetic elements and genetically modified organisms which are regulated by the Agency because of their potential for use in biological attacks.

**Controlled materials**

Biological agents, delivery systems and related materials listed the control list.

**Control list**

A list of all biological substances, delivery systems and related materials that must be regulated by law and kept secure in order to prevent theft and malicious misuse. The list should be included in the Executive Order which regulates national biosecurity.

**Decontamination**

The process by which a contaminant is inactivated or converted to a harmless substance.

**Delivery systems**

Spraying equipment and other unmanned systems capable of disseminating biological substances.



**Dispersal analysis**

An assessment of contaminant dispersion in an area that has been exposed to an accidental release or an intentional attack involving a controlled biological substance. Field investigators from the Agency or biopreparedness authority determine the extent of the contamination, demarcate the contaminated area and identify potentially exposed individuals.

**Dual use material**

A biological substance, a delivery system or related material that can be used for both legitimate and offensive purposes.

**Facility**

A legal entity or department thereof that is subject to biosecurity regulation – for example a hospital, an educational institution or a production unit.

**Form for changes to a license**

An Agency form which must be filled out by a facility that is planning any changes to its current license. The form is submitted to the Agency for approval before any change is implemented.

**Forms for inventory reporting**

Agency forms used by facilities to inform the Agency of any changes in their inventory of controlled materials. These forms include annual or quarterly stocktaking forms as well as forms for reporting the purchase, sale, transfer or destruction of controlled materials.



**Inspection visit**

The announced or unannounced inspection of a facility by Agency representatives. The aim of the visit is to ensure that the facility complies with all provisions in a national Biosecurity Law and Executive Order.

**Intentional biological attack**

An intentional and harmful act involving controlled biological substances.

**Inventory list**

A list of a facility's stock of a controlled material, specifying type and quantity.

**License**

A license issued by the Agency stating the terms and conditions with which a facility must comply in order to work with or possess specifically listed controlled material.

**Loss**

A disappearance of controlled material which cannot be explained by theft or normal use.

**Medical countermeasures**

Methods and procedures to counteract diseases – for example, quarantine, isolation and the use of vaccines, antitoxins and antibiotics.

**Misuse**

The use of controlled materials without an appropriate license from the Agency.

**Personnel list**

A list of specifically-named facility personnel



with access to a specifically-named controlled biological substance.

**Possession**

To own or have custody of controlled biological substances, delivery systems or related materials.

**Related materials**

Materials, equipment and technology which are listed in international biosecurity treaties and agreements or included in national control lists and which can be used in the design, development, production, or use of biological weapons and their delivery systems.

**Response team**

A team that provides clinical advice on immediate actions, including medical countermeasures, that must be taken in case of a suspected or actual biological accident or attack. The team collects on-site information and samples, conducts rapid laboratory analyses, and provides expert medical advice in order to identify any biological warfare agent and determine the dispersion area.

**Security Plan**

A plan for security measures or precautions to be implemented at a facility to prevent, detect and respond to the theft or misuse of controlled biological substances, delivery systems and related materials.

**Storage unit**

A unique unit for storage of biological substances, for example a closed sample tube containing a bacterial culture.



**Substance codes**

Unique numbers that are used instead of the names of specific controlled biological substances. The codes enable unclassified communication about these substances between a licensed facility and the Agency. Only the license holder and the Agency have access to these codes.

**Technology**

Non-public information that is necessary for the development, production or use of a product.

**Terrorism**

Unlawful acts with the intent to cause death, serious injury or hostage-taking. The aim is to create fear in the population or compel a government or an international organisation to perform or refrain from performing a particular action.

**Theft**

The removal, without permission, of controlled material from a facility that is licensed by the Agency.

**Vulnerability Assessment**

An identification of the threats and shortcomings of a facility's security measures regarding the possession, production, use, storage, purchase, sale, transport, transfer and disposal of controlled biological substances, delivery systems and related materials.

**Weaponisation**

A technical process by which a biological agent is made suitable for use in a biological attack.



**Published by:**

Centre for Biosecurity and Biopreparedness  
Statens Serum Institut  
Artillerivej 5  
2300 Copenhagen S  
Denmark

[www.biosikring.dk/eng](http://www.biosikring.dk/eng)

© Centre for Biosecurity and Biopreparedness

No part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

**Text:**

Anne Nielsen, Language Arts

**Editorial team:**

Nina Ruth Steenhard, DVM, PhD  
*Head of Laboratory Division*

Jeanne Lind Christiansen, MA  
*Information Officer*

Katja Nyholm Olsen, MSc, PhD  
*Special Advisor*

Robert Petersen, MA, PhD  
*Analyst*

John-Erik Stig Hansen, MD, DMSc  
*Director*

**Graphic Design and Layout:**

Britt Friis Grafisk Design

**Printed by:**

Pekema, Denmark

1st edition, 2015  
ISBN 978-87-998137-0-4





