Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science
Volume 5, Number 1, 2007 © Mary Ann Liebert, Inc.
DOI: 10.1089/bsp.2006.0026

BIOSECURITY IN SCANDINAVIA

Kristian H. Bork, Vibeke Halkjaer-Knudsen, John-Erik Stig Hansen, and Erik D. Heegaard

This article investigates the extent to which biosecurity measures are recognized and have been implemented in the Nordic countries, in the absence of formalized security standards and legislation. Two trials were undertaken: first, a broad combined biosafety and biosecurity questionnaire survey of the Nordic countries, and, second, a focused on-site audit of 22 facilities, with 94 laboratories, in Denmark. Both trials indicated that external security had been partially implemented but that little attention had been paid to internal security and the establishment of biosecurity. It was demonstrated that the backgrounds and identities of insiders were rarely checked and that they could have gained access to both pathogen inventory lists and freezers in many facilities. In 81% of pathogen-containing facilities, pathogens were not routinely and centrally accounted for. The authors recommend the establishment of a legal framework congruent with international standards and obligations; novel governmental national biosecurity authorities, requiring a fusion of both microbiological and technical expertise and legislative powers; and the formulation of a new code of conduct termed "Good Biosecurity Practice."

BIOSAFETY INCLUDES SAFETY measures to prevent accidental exposure to infectious agents. The aim of biosafety is to prevent unintentional exposure leading to casualties or disease outbreaks. All Scandinavian countries have a longstanding tradition in this area and have passed and implemented internationally based regulations to prevent accidents in work with microbial pathogens. Several international organizations, including the World Health Organization, are actively engaged in developing and reviewing existing biosafety regulations in laboratories, microbial research, and the biotech industry.

In contrast, the rapidly developing concept of biosecurity includes measures to protect against the malicious use of pathogens, or parts of them, or their toxins, in direct or indirect acts against humans, livestock, or crops.[1] Natural outbreaks of infectious disease may have significant consequences for public health, agriculture, infrastructure, and economy, but if the outbreak is deliberately caused, the consequences for national and international security may be even greater. The aim of biosecurity is to prevent proliferation of dangerous or dual-use pathogens, toxins, sensitive production equipment, and knowledge, through the international application of codes of conduct, or Good Biosecurity Practice, and regulations. Dual-use research encompasses knowledge, products, or technologies that could be directly misapplied by others to pose a threat to public health, agriculture, plants, animals, the environment, or materiel.[2] The basic elements of biosecurity are:

- Physical security of material
- Security management of personnel
- Security management of visitors
- Incident response plans
- Staff training to raise biosecurity awareness

Kristian H. Bork, MD, is an Analyst; Vibeke Halkjaer-Knudsen, PhD, is Director of the Environmental Safety Department; John-Erik Stig Hansen, MD, DMSc, is Director of the Centre; and Erik D. Heegaard, MD, PhD, DMSc, is Deputy Director of the Centre; all are at the Centre for Biological Defence, Statens Serum Institut, Copenhagen, Denmark.

- Security of information
- Transport security
- Material control and accountability[3]

National implementation of biosecurity is important for international security as emphasized by the newly adopted UN Security Council resolution 1540.[4] Nonproliferation is essential in order to reduce the risk of criminals, terrorists, or rogue states acquiring dangerous pathogens, toxins, or even a biological weapons capacity. Producing a biological weapon may involve acquiring elements from several sources and countries, which may be distant from the area where the weapon is intended to be deployed, and therefore biosecurity is both a national and an international responsibility. Development of biological agents and delivery vehicles for hostile purposes is banned by the Biological and Toxin Weapons Convention,[5] which in many countries, including Denmark, is augmented by national laws.

While some European countries are in the process of formulating comprehensive national biosecurity strategies or legislation against, for example, unauthorized possession of dangerous pathogens, most European countries have not yet begun this process.

The aim of the present survey was to investigate the extent to which biosecurity measures are recognized and have been implemented in Nordic laboratories, research institutions, and biological production facilities—in Denmark in particular—in the absence of formalized security standards and legislation. The results that were obtained may serve as guidelines and support for outlining relevant components for future legislation, biosecurity implementation, and enforcement of security measures in the Nordic countries.

Material and Methods

Two trials were undertaken in this study. First, a broad combined biosafety and biosecurity questionnaire survey of the Nordic countries (Iceland, Norway, Finland, Sweden, and Denmark) was conducted; it served as an indicator of the general compliance with and recognition of the biosecurity elements (listed above). Second, a focused on-site benchmarking audit was taken of facilities in Denmark in order to provide detailed knowledge of awareness and compliance with biosecurity in different types of institutions and possibly to identify areas in which improvement of security might be advantageous.

Trial One – Nordic Questionnaire

Participants

An internet-based questionnaire was sent to 109 biosafety representatives engaged in biotechnology research and microbial diagnostics in the Nordic countries. All were members of the Nordic Biosafety Network, the largest nongovernmental biosafety organization in the Nordic countries, a subcommittee of the European Biosafety Association.[6] The institutions represented in the network are both public and private laboratories working at biosafety levels (BSL) 1 through 4.

Questionnaire

A questionnaire was developed, composed of 33 questions of which 16 were biosecurity related (Tables 1 and 2): 2 questions focused on biosecurity awareness, 8 on accessibility, 4 on accountability and transferals, and 2 concerned biosecurity-related procedures that had been implemented. Twelve questions were biosafety related, and 5 provided descriptive data such as biosafety level, country, and location of laboratory. The questionnaire was developed, tested, and improved through a number of trial runs. Participants were allowed to answer anonymously, and the survey was open for participation for 48 days (February–March 2006). Participants were able to enter only once via mailed invitation.

Analysis of results

Results were collected and analyzed using software from Defgo (Copenhagen, Denmark). A follow-up was conducted in June 2006 through telephone calls and email correspondence with specific laboratories in order to identify reasons and considerations for refusing external requests for pathogens.

Trial Two – Danish Audit

Identification

Thirty-six institutions and microbial processing companies in Denmark were identified and invited to an on-site inspection. The units were identified through web searches (Google.dk) using search strings of the following categories:

- Pathogens (Bacillus research; foot, mouth disease research; plaque research; etc.)
- Biotechnology research institutions
- Publications (spray-drying of biological material, vaccine research)
- Pharmaceutical/veterinary production capacity and type

Units also were found through personal communication with more than 50 researchers at key facilities in the private and public research and production sectors.

Categorization

The facilities that agreed to an audit were characterized and subdivided according to their line of work and their status (public or private) into the following categories:

- universities;
- public research institutions (i.e., institutions conducting

Table 1. Web Questionnaire Results on Biosecurity-related Questions

	%	Number (*N* = 35)
Biosecurity awareness		
1. Relevant biohazard level signs posted		
Never	2.9	1
Generally or always	85.7	30
N/A (not applicable)	8.6	3
Unanswered	2.9	1
2. Biohazard signs indicate pathogens used or studied		
Never	25.7	9
Generally or always	62.9	22
N/A (not applicable)	8.6	3
Unanswered	2.9	1
3. Institution or company has an appointed biosecurity officer		
No	25.7	9
Yes	68.6	24
N/A (not applicable)	2.9	1
Unanswered	2.9	1
Physical security		
4. Laboratory doors closed during work hours		
Always open or unlocked	45.7	16
Always closed and locked	42.9	15
N/A (not applicable)	2.9	1
Other, please specify	8.6	3
5. Laboratory doors locked after work hours		
Never, only outside area access restrictions	11.4	4
Generally or always	85.7	30
N/A (not applicable)	2.9	1
6. Windows secured with alarms after work hours[a]		
No alarms	28.6	10
Windows cannot open	22.9	8
Alarms present but not in use	0	0
Alarms are generally activated	11.4	4
Alarms are always activated	31.4	11
N/A (not applicable)	2.9	1
Other, please specify	17.1	6
Personal security		
7. Personal identification equipment restricting access to the facility		
None	20.0	7
In use, but only after work hours	8.6	3
Generally in use (can be deactivated)	2.9	1
Always in use	57.1	20
N/A (not applicable)	2.9	1
Other, please specify	8.6	3
Accountability		
8. Pathogen freezer		
No lock	22.9	8
Lock present, but often unlocked	22.9	8
Always locked	40.0	14
N/A (not applicable)	5.7	2
Other, please specify	8.6	3
9. Hazardous biological material storage room locked		
Never or rarely	22.9	8
Generally	51.4	18
N/A (not applicable)	11.4	4
Other, please specify	14.3	5

Table 1. Web Questionnaire Results on Biosecurity-related Questions (*Cont'd*)

	%	Number (*N = 35*)
10. Hazardous biological material storage access is restricted[a]		
No restrictions	14.3	5
Locks	37.1	13
Alarm	14.3	5
Card reader	20.0	7
Card reader and pin code	40.0	14
Fingerprint recognition	0	0
N/A (not applicable)	11.4	4
Other, please specify	8.6	3
11. Hazardous biological material inventory list specifying agent and number of samples[a]		
None available	14.3	5
Only agent types	11.4	4
List available, but not updated every month	34.3	12
List available and updated regularly (at least once/month)	14.3	5
List available and updated regularly (at least once/month) by responsible officer/employee	17.1	6
N/A (not applicable)	8.6	3
Other, please specify	11.4	4
12. Pathogen freezer key kept[b]		
Employees hold keys to freezer/storage	11.1	3
Responsible employee holds key	29.6	8
Everybody has access to key during work hours	44.4	12
Maintenance and cleaning personnel have access to key after work hours	7.4	2
N/A (not applicable)	11.1	3
Other, please specify	7.4	2
Transport security		
13. Standard operational procedure for transport of biological material		
No	11.4	4
Yes	85.7	30
N/A (not applicable)	2.9	1
14. Number of incidents during the last 5 years where packages with biological material were lost		
0	74.3	26
1–5	20.0	7
6–10	0	0
11–20	0	0
21–40	0	0
>40	0	0
N/A (not applicable)	5.7	2
Incident response plans		
15. Standard operational procedure manual for theft of material		
Yes	34.3	12
No	62.9	22
N/A (not applicable)	2.9	1

[a] Multiple answers were allowed from 35 respondents; responses total more than 35.
[b] Multiple answers were allowed from 27 respondents.

research under direct government management and funding);
- private research companies (i.e., private companies conducting research without production capability);
- pharmaceutical industry (i.e., private companies conducting research with a production capability);
- public pharmaceutical/veterinary institutions (i.e., state-controlled companies conducting research with a production capability);
- laboratory supply chain (i.e., private companies selling laboratory supplies, not conducting laboratory research and development); and

Table 2. Questionnaire Results for External Requests for Pathogens

No. of incidents during last 5 years where external requests for pathogens were refused	0	1–5	6–10
Percentage of 25 laboratories	64%	24%	12%
Number of laboratories	16	6	3

External demands for pathogens were rejected in a number of cases. The results from the web questionnaire are from BSL-2 and BSL-3 laboratories grouped.

- public diagnostic facilities (i.e., laboratories conducting diagnostic procedures, state or county controlled).

The aim was to identify potential differences among the groups with regards to the biosecurity elements listed on pages 62 and 63.

Preparing for inspection

The invitation letter contained a nondisclosure agreement concerning sharing of facility-specific results. Before the audit, a notification was sent about the purpose of the survey and the background of one of the authors (KHB, medical doctor with special CBRN [chemical, biological, radiological, and nuclear] training and experience) conducting the survey.

A 15-minute oral biosecurity presentation was developed that outlined the scope and purpose of the audit. The presentation was to be followed by a 1–2-hour physical inspection of the institutions and their laboratories, production facilities, and storage areas using an inspection protocol developed for this purpose. For larger institutions, only critical parts of their research departments and production facilities were to be audited. An interview questionnaire technique combined with a personal standardized inspection routine for a uniform collection of data was developed and tested.

Sensitive objects

Sensitive objects and materials were defined beforehand, using the Australia Group export control lists for export, as:

- Presence of bioterror-relevant agents (live or killed) or DNA/RNA;[7]
- Presence of agroterror-relevant agents (live or killed) or DNA/RNA;[8] and
- Possession of dual-use biological equipment and related technology.[9]

Biosecurity benchmarking

Forty-four questions were developed, pretested, and evaluated for an on-site inspection protocol. We selected 19 questions as key markers for evaluating awareness and compliance with biosecurity-relevant factors, scored accordingly (Table 3).

Results

Trial One – Nordic Questionnaire

Participants

Forty-six institutions (46/109 = 42%) responded to the questionnaire; 8 of the 46 completed fewer than three questions, and 3 declined to participate because of security considerations. Thus, 35 persons (35/109 = 32%) completed the questionnaire, and the results were the subject for the subsequent analysis. The number of participating Nordic laboratories and their distribution according to the highest BSL is illustrated in Table 4.

Questionnaire

Responses on biosecurity-related questions for all BSLs are summarized in Tables 1 and 2, and specific results for BSL-3 laboratories, where the likelihood of encountering sensitive agents of the Australia Group lists is increased, are summarized and compared below.

Analysis of results

Physical Security: Two BSL-3 laboratories out of 14 (14%) reported that their laboratory doors were generally closed but unlocked during work hours, and 1 of 14 (7%) left doors unlocked after work hours, relying on outside area access restrictions alone.

Personnel Security: Approximately half of all BSLs reported that personal identification equipment (pin code display or card readers) restricted access to laboratory areas at all times, but 20% had no such security measures (Table 1, item 7). Ten of the BSL-3 laboratories (71%) were equipped with the security measures mentioned.

Accountability: Pathogen storage was reported to be secured by card-reader and pin code by 57% (8/14) of BSL-3 laboratories, but 2 relied on locks alone (14%). One BSL-3 laboratory (7%) kept keys to pathogen storage accessible to cleaning and maintenance personnel, and 3 out of 14 (21%) BSL-3 laboratories had no locks on their pathogen storage freezers. Half of the BSL-3 laboratories had an available pathogen inventory list that was checked against the actual inventory at least once a month by an employee or a responsible officer. For all BSLs, 31% (11/35) used these procedures (Table 1, item 11).

Staff Training to Raise Biosecurity Awareness: External requests for pathogens were reported to be rejected in a number of cases (Table 2). A follow-up to determine the reason for not complying with requests revealed factors such as uncertainty about the exact identity of the recipient, economic considerations, or uncertainty about the recipient's compliance with biosafety standards.

Trial Two – Danish Audit

Identification

Of the 36 invited institutions, 22 facilities (61%) were audited; two declined to participate (one had moved to a location outside Denmark, and one was moving their facility and was temporarily shut down). Fourteen units (39%) indicated an interest in participating but failed to report back, and requests for audits were unsuccessful.

Categorization

In the 22 facilities visited, a total of 94 laboratories were examined (Table 5). The distribution of institutions ac-

Table 3. Audited Institutions in Denmark: Compliance with 19 Biosecurity Relevant Factors

	Public Research Institutions	Universities	Public Diagnostic Institutions	Public Pharma/ Veterinary Institutions	Public Total		Private Research Companies	Pharma-ceutical Companies	Laboratory Supply Companies	Private Total		Total	
					No.	%				No.	%	No.	%
Number of facilities	5	7	3	1	16		1	3	2	6		22	
Number of laboratories	26	36	14	3	79		1	14	0	15		94	
Facilities holding sensitive pathogens	4 (80%)	1 (14%)	3 (100%)	1 (100%)	9	56	1 (100%)	0 (0%)	N/A	1	25	10	50
Facilities holding sensitive technology	1 (20%)	1 (14%)	0 (0%)	0 (0%)	2	13	0 (0%)	2 (66%)	1 (50%)	3	50	5	23
Biosecurity awareness													
1. Appointed biosecurity officer	0	0	0	1	1	6	0	1	0	1	17	2	9
Security of information and transport security													
2. Established policy for export of pathogens	1	1	0	0	2	13	0	2	1	3	50	5	23
Security management of personnel													
3. Identities of new employees are checked	0	0	0	0	0	0	0	3	0	3	50	3	14
4. Identities of new service, cleaning, and security personnel are checked	0	0	0	0	0	0	0	2	0	2	33	2	9
5. Employees are required to have no criminal record	0	0	0	0	0	0	1	1	0	2	33	2	9
6. Personal identification equipment on lab/technology department doors	0	1	0	0	1	6	0	1	1	2	33	3	14
Physical security													
7. Perimeter security established	2	0	0	1	3	19	0	2	0	2	33	5	23
8. Alarms on outer doors	2	1	0	1	4	25	1	3	2	6	100	10	46
9. Alarms on windows on all floors	0	0	0	1	1	6	1	1	1	3	50	4	18
10. Alarms on lab/technology dept. doors after work hours	0	1	0	1	2	13	1	2	1	4	66	6	27
Security management of visitors													
11. Reception desk	5	2	0	1	8	50	1	3	1	5	83	13	59
Accountability													
12. List of agents available	0	6	2	1	9	56	1	3	N/A	4	100	13	65
13. Agents accounted for mon. once/2 months	0	0	0	0	0	0	1	0	N/A	1	25	1	5
14. List of agents stored at secure place or coded	2	1	1	0	4	25	0	2	N/A	2	50	6	30
15. Freezers locked under audit	0	2	1	0	3	19	0	2	N/A	2	50	5	25
16. Freezers equipped with personal identification equipment	0	0	0	0	0	0	0	1	N/A	1	25	1	5
17. Pathogen storage locked during audit	1	2	1	0	4	25	0	2	N/A	2	50	6	3
18. Service, maintenance, cleaning, and security personnel not allowed to access pathogen storage after work hours unaccompanied	0	1	0	1	2	13	0	2	N/A	2	50	4	20
Incident response plans													
19. Established policy concerning thefts or attempted theft of pathogens	1	0	0	0	1	6	0	1	N/A	1	25	2	10
Positive grouped responses	14	18	5	8	45		7	34	7	48		93	
Maximum positive responses	19*5	19*7	19*3	19*1	19*16		19*1	19*3	11*2	11*6, 7*4		402	
Score percentage	15	6	9	42		14	37	60	32		51		21

Table 4. Web Questionnaire Participants, BSL, and Country Distribution

	Denmark	Sweden	Finland	Norway	Total
BSL-1	1	2	0	0	3
BSL-2	6	7	0	2	15
BSL-3	3	6	2	3	14
BSL-4	0	0	0	0	0
N/A	1	2	0	0	3
Total	11	17	2	5	35

cording to the categories mentioned above is illustrated in Table 3.

Inspection

The majority of audits were conducted along with the safety officer of the institutions, but in many cases several additional employees (1–5 persons) took part in the inspection. The average time of inspection was approximately 75 minutes. The facilities were located in four of the six Danish county regions, and the audits were conducted from June to August 2006. Inspection may not encompass the entire organization, especially in larger institutions. Findings cover only a particular department.

Sensitive objects

Sensitive agents or technology were identified in 55% (12/22) of all facilities through inspection and interview. Sensitive agents were identified in 45% (10/22) of all facilities. They were found at all three public diagnostic facilities, of which two were unclassified according to the BSL terminology, and in four out of five (80%) public research institutions. One of seven universities had sensitive agents, but none of the pharmaceutical companies stored sensitive pathogens. Dual-use biological equipment was found in two of three (66%) pharmaceutical companies, in one of five (20%) public research institutions, in one of seven (14%) universities, and in none of the public diagnostic facilities (Table 3).

Biosecurity benchmarking

Compliance with 19 key measures, within the 8 biosecurity elements listed on pages 62 and 63, was evaluated for each group and analyzed (Table 3).

Physical Security: Perimeter security (Table 3, item 7) was established in a minority of facilities by fencing (4/22, 18%); one was secured by remote location on a dedicated island. Of the ten facilities holding sensitive agents, six (60%) had no perimeter security. Two of three pharmaceutical companies (66%) and none of the ten public diagnostic institutions and universities had perimeter security. Eighty-seven percent of public institutions (14/16), compared to 34% of private companies (2/6), had no burglar alarms in their laboratories and technical departments (Table 3, item 10), although some had implemented building access restriction and alarms against forced entry on external doors. Eight of the ten (80%) facilities holding sensitive agents had neither installed alarms on laboratory doors nor installed alarms inside their laboratories. None of the eight public research and diagnostic institutions had alarms. Five facilities (23%) had no security personnel patrolling regularly after working hours, and 13 of 16 public facilities (81%) had no alarms on windows at ground level or external doors.

Accountability: Sixty-six storage freezers for pathogens were examined at 18 facilities. One pharmaceutical facility had locks requiring personal identification (Table 3, item 16), but most freezers were secured with easily breakable standard locks, and 50 freezers (76%) were unlocked despite locks being present. Thirty-five freezers were located in the ten laboratories where sensitive agents were identified, and 33 (94%) of those were either unlocked or had no locks.

In 14 of 16 pathogen-storage areas (88%) of the public sector, cleaning and service personnel had unaccompanied access after working hours on a daily basis (Table 3, item 18), but in two pharmaceutical companies and in two public institutions, the access was monitored by members of the staff. Nine of the ten institutions (90%) holding sensitive pathogens left cleaning and service personnel to work unaccompanied and with no security clearance. The sharing of technological, production, or diagnostic equipment with research communities outside the facility was not allowed in 4 of 22 private facilities (18%). These regulations were empowered by policies and procedures and were, in all four cases, motivated by protection of corporate and intellectual property.

Pathogens were not routinely and centrally accounted for in 9 out of 10 (90%) of the facilities holding sensitive biological material. Control, if implemented, accounted for

Table 5. Audited Laboratories in Denmark According to Their Biosafety Levels (BSLs)

Classification	Count
BSL-3	3
BSL-3 Ag	2
BSL-2	18
BSL-2 GMO	3
BSL-1	23
BSL-1 GMO	38
Unclassified	7
Total	94

Note. BSL-3 Ag = agricultural laboratory, BSL GMO = laboratory containing genetically modified organisms.

pathogens annually or less frequently. Among the 20 pathogen-containing facilities (sensitive and nonsensitive pathogens), agent inventory lists (Table 3, item 14) were not secured in 14 facilities (70%), and in 11 of the facilities (55%) agent inventory lists were kept uncoded in ring binders. In five of the eight (63%) public research and diagnostic facilities, which in almost all cases had sensitive pathogens, the pathogen lists were freely accessible to the auditor and all people in the laboratory.

Security of Information and Transport Security: Procedures and policies are necessary to avoid unintentional, potentially illegal export of selected pathogens and equipment to countries outside Australia Group Member States.[10] Five of 22 facilities (23%) had formulated and implemented such precautions as part of their company policy (Table 3, item 2). Of the ten facilities holding sensitive pathogens, seven (70%) had no such policy. None used material transfer agreements (verifying end-user and purpose).

Security Management of Personnel and Biosecurity Awareness: In 2 of the 22 facilities, both involved with production (9%), a biosecurity officer was identified (Table 3, item 1); the rest had no appointed person responsible for implementing and maintaining biosecurity. One out of ten (10%) facilities holding sensitive pathogens had a biosecurity officer.

All pharmaceutical companies performed a check on the background of staff members before employment (Table 3, item 3), whereas none of the public institutions systematically confirmed the identities of their new employees. Two private companies (9%) had an extended application procedure that requires a clean criminal record before employment (Table 3, item 5). Several facilities, primarily universities, had PhD students from numerous countries outside Australia Group member states and made no checks on background and identity before granting access.

Security Management of Visitors: None of the 22 facilities checked the auditor's background or identity by confirmatory phone calls to the Danish National Centre for Biological Defence or by demands for personal identity papers or the equivalent. Nine facilities (41%) had no reception desk or checkpoint for registering visitors (Table 3, item 11). One facility had written brochures concerning security regulations for visitors, external craftsmen, service personnel, and the like.

DISCUSSION

No comprehensive law or formal set of rules covers all aspects of biosecurity in Scandinavia. Biosafety regulations overlap with biosecurity requirements to some extent. Biosecurity, however, requires additional measures, involving both restricting access from intruders as well as ensuring that only authorized personnel, with checked backgrounds, have access to pathogens or sensitive equipment and technology.

In our opinion, access and handling of sensitive material and technology (as defined above) in selected laboratories should be documented and in special situations even monitored. Security violations should result in a rapid assessment of degree of damage and theft; the latter is possible only if all pathogens are accounted for. For that and other purposes, such as suspicious external demands for dangerous pathogens, frequently updated standard operational procedures as well as material transfer agreements and accountability methods will be necessary. The U.S. and UK have developed and implemented regulations concerning work with selected microbial substances. Since 2001 some of their most sensitive laboratories have been secured, but a comprehensive solution requires an international security strategy and standardized regulations.

Trial One – Nordic Questionnaire

The majority of the facilities in Scandinavia responding to the web questionnaire have an appointed biosecurity officer, indicating a general willingness to implement biosecurity. This interest is further illustrated by the fact that most BSL-2 and BSL-3 laboratories have personal identification equipment installed, rather than simple locks, thus restricting external access to laboratory buildings; the purpose is either to ensure biosecurity or to protect against sabotage or industrial espionage. However, one fourth of the participants reported that hazardous material storage areas were rarely or never locked, and approximately half of the facilities kept storage freezers mostly unlocked. Furthermore, approximately half of the laboratories reported that the keys necessary for unlocking pathogen storage freezers were accessible to everybody in the laboratory during work hours.

Taken together, these results indicate that the focus has been on implementing external rather than internal or personnel security. The chance of discovering a theft of pathogens by an insider, who may bypass implemented external security measures, is low, since the majority of laboratories have no standard operational procedure in case of thefts and they have no system for regularly and systematically controlling the amounts and presence of pathogens in the laboratory.

Trial Two – Danish Audit

The benchmarking of facilities revealed significant differences between public and private institutions and further revealed that none of the facilities could fulfill all 19 requirements for a maximum score. The two facilities with the highest scores, both large pharmaceutical companies, were in compliance with 12 of 19 key biosecurity measures. On the other hand, some of the overall least secured institutions were public, and, given the high incidence of sensi-

tive agents in these facilities, this points to an area where improvement of biosecurity is imperative.

The majority of audited facilities were easily accessible, especially after working hours, and potential security violations would likely go unnoticed, especially since the number of facilities having alarms installed was low. Insiders whose backgrounds and identities are rarely checked could gain access to both pathogen inventory lists and freezers in many facilities. The auditor gained both access to sensitive areas and knowledge without anyone checking his background, his employment by the National Centre for Biological Defence, or even his personal identity papers upon arrival at the facilities. Almost half of the facilities did not even have a reception desk that could be used for checking visitor appointments and identity.

It seems that private institutions have formulated policies on safety and security in order to comply with various international standards and expectations of customers, commonly formulated under the term "good corporate governance"—that is, corporate or institutional policies and standards concerning ethical, environmental, safety, and security issues. Public research institutions are probably less inclined to do so, as the results clearly indicate.

Several findings in the questionnaire were not confirmed by the audit, which monitored facilities in Denmark only. The bias of results observed can be explained by the fact that the facilities in the Danish audit were smaller research institutions than the ones generally represented in the Nordic Biosafety Network. Furthermore, some of the differences may be explained by the drop-out variance, misinterpretation of the questionnaire contents, and methodological differences. Exchanging even high-risk pathogens is part of laboratory and scientific practice. Exporting pathogens internationally may conflict with European export regulations, but the risk of unintentionally violating regulations can be managed by the implementation of simple standardized procedures. National transfer of pathogens must be evaluated in the context of biosecurity, which is even of more concern if the recipient is unknown.

Conflicts between safety measures and biosecurity regulations need to be solved—for example, biohazard signs that display the name and type of pathogens in laboratories may help prevent unintentional exposures but may also aid intruders in their search for specific pathogens. Access to sensitive laboratories was sometimes restricted by the use of access code displays, while at the same time directions were given to aid the access of emergency personnel in case of an accident (Figure 1).

Implementing biosecurity should be part of a global strategy as emphasized by the UN.[11] Biosecurity is not only a matter of physical and personnel security but also requires awareness about the dangers involved if certain pathogens and technology fall into the hands of criminals or terrorists. Only through awareness of the potential for misuse and the establishment of codes of conduct for scientists can compliance with biosecurity regulations be expected. The apparent lack of procedures that both trials demonstrated should be corrected, and this will, in combination with risk assessments, provide an initial significant improvement of biosecurity before the more costly external security measures are considered.

Figure 1. Biosecurity and safety measures collide at BSL-3 laboratory entrance. Safeguarding against access from intruders is ensured by the use of codes. The knob overrides the keypad, aiding access of rescue personnel in case of an emergency situation. The knob override is required to comply with safety regulations from Danish authorities.

The need for a new government-approved standard based on the WHO Biorisk Management guideline for "Good Biosecurity Practice" is evident.[12] A national au-

thority may execute "Good Biosecurity Practice" certification and include this as an element of Good Corporate Governance or Good Laboratory Practice, whenever applicable. A standardized measuring unit for "Good Biosecurity Practice" needs to be developed and accepted, such as counting the number of security barriers from publicly accessible areas to sensitive areas in order to evaluate and compare institutions of different types. Sensitive materials and classified agents were identified in unclassified laboratories in our study. Therefore, the process of implementing biosecurity should not only focus on BSL-classified institutions but rather be based on the presence of agents and technology.

One of the authors conducting the audit encountered elements that, although not included in the definition of critical materials and technology and therefore not included in the results, still could be characterized as critical: laboratories conducting de-novo synthesis of DNA/RNA. It is suggested, therefore, that the implementation and maintenance of regulations for biosecurity be supported by highly specialized technical expertise that includes knowledge about the dual-use potential of material and technology not formulated on the Australia Group list for export control. As biotechnology and the potential for misuse evolve rapidly, biosecurity regulations and procedures need to be rapidly adaptable to meet threats such as those from upcoming pathogens like SARS. Future national biosecurity organizations will have to meet these requirements to ensure both a sufficient reduction of proliferation risk as well as being in compliance with UN Security Council Resolution 1540.

The authors recommend the establishment of a legal framework coherent with international standards and obligations; novel governmental national biosecurity authorities, requiring a fusion of both microbiological and technical expertise and legislative powers; and the formulation of a new code of conduct termed "Good Biosecurity Practice."

REFERENCES

1. Organization for Economic Cooperation and Development (OECD). *Glossary of Terms.* OECD International Futures Programme; 2006. Available at: http://www.biosecuritycodes.com/gloss.htm#biosec. Accessed January 17, 2007.
2. National Science Advisory Board for Biosecurity. *Draft Guidance Documents.* Bethesda, Md: National Science Advisory Board for Biosecurity; 2006. Available at: http://www.biosecurityboard.gov/pdf/NSABB%20Draft%20Guidance%20Documents%2027Sep06%20(12%2011%202006).pdf. Accessed January 17, 2007.
3. Sandia National Laboratories. *Biosecurity—Elements of Biosecurity.* Albuquerque, NM: Sandia National Laboratories; 2006. Available at: http://www.biosecurity.sandia.gov/biosecurity. Accessed January 17, 2007.
4. UN Security Council. UN Security Council Resolution 1540: Non-proliferation of weapons of mass destruction. Adopted at the 4956th meeting. New York: UN Security Council; April 28, 2004. Available at: http://daccessdds.un.org/doc/UNDOC/GEN/N04/328/43/PDF/N0432843.pdf?OpenElement
5. Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction; 1975.
6. European Biosafety Association (EBSA). EBSA; 2006. Available at: http://www.ebsa.be. Accessed January 17, 2007.
7. Australia Group. *List of Biological Agents for Export Control.* Commonwealth of Australia; June 1, 2005. Available at: http://www.australiagroup.net/en/control_list/bio_agents.htm. Accessed January 17, 2007.
8. Australia Group. *List of Animal Pathogens for Export Control.* Commonwealth of Australia; April 2005. Available at: http://www.australiagroup.net/en/control_list/animal.htm. Accessed January 17, 2007.
9. Australia Group. *Control List of Dual-Use Biological Equipment and Related Technology.* Commonwealth of Australia; April 2005. Available at: http://www.australiagroup.net/en/control_list/bio_equip.htm. Accessed January 17, 2007.
10. Australia Group. *Australia Group Member States.* Commonwealth of Australia; 2006. Available at: http://www.australiagroup.net/en/agpart.htm. Accessed January 17, 2007.
11. UN Secretary General. Uniting against terrorism: recommendations for a global counter-terrorism strategy. Sixtieth session, Agenda items 46 and 120. New York: United Nations; April 27, 2006. Available at: http://daccessdds.un.org/doc/UNDOC/GEN/N06/330/88/PDF/N0633088.pdf?OpenElement
12. World Health Organization. *Epidemic and Pandemic Alert and Response. Biorisk Management, Laboratory Biosecurity Guidance.* Geneva: WHO; 2006.

Manuscript received September 29, 2006;
accepted for publication December 18, 2006.

Address reprint requests to:
Kristian Hveysel Bork, MD
Centre for Biological Defence
Statens Serum Institut
Artillerivej 5, 334/106
Copenhagen S
DK-2300 Denmark

E-mail: khb@ssi.dk