MMWR™

Morbidity and Mortality Weekly Report

Recommendations and Reports | December 6, 2002 / Vol. 51 / No. RR-19

Laboratory Security and Emergency Response Guidance for Laboratories Working with Select Agents

Centers for Disease Control and Prevention

safer • healthier • people™

The *MMWR* series of publications is published by the Epidemiology Program Office, Centers for Disease Control and Prevention (CDC), U.S. Department of Health and Human Services, Atlanta, GA 30333.

SUGGESTED CITATION

Centers for Disease Control and Prevention. Laboratory security and emergency response guidance for laboratories working with select agents. MMWR 2002;51(No. RR-19):[inclusive page numbers].

Centers for Disease Control and Prevention

Julie L. Gerberding, M.D., M.P.H.
Director

David W. Fleming, M.D.
Deputy Director for Science and Public Health

Dixie E. Snider, Jr., M.D., M.P.H.
Associate Director for Science

Epidemiology Program Office

Stephen B. Thacker, M.D., M.Sc.
Director

Office of Scientific and Health Communications

John W. Ward, M.D.
Director
Editor, MMWR *Series*

Suzanne M. Hewitt, M.P.A.
Managing Editor

C. Kay Smith-Akin, M.Ed.
Project Editor

Malbea A. Heilman
Beverly J. Holland
Visual Information Specialists

Quang M. Doan
Erica R. Shaver
Information Technology Specialists

CONTENTS

Laboratory Security and Emergency Response Guidance for Laboratories Working with Select Agents

Prepared by
Jonathan Y. Richmond, Ph.D.[1]
Shanna L. Nesby-O'Dell, D.V.M.[2]
[1]*Office of the Director*
Office of Health and Safety (Retired)
[2]*Office of the Director*
Office of Health and Safety

Summary

In recent years, concern has increased regarding use of biologic materials as agents of terrorism, but these same agents are often necessary tools in clinical and research microbiology laboratories. Traditional biosafety guidelines for laboratories have emphasized use of optimal work practices, appropriate containment equipment, well-designed facilities, and administrative controls to minimize risk of worker injury and to ensure safeguards against laboratory contamination.

The guidelines discussed in this report were first published in 1999 (U.S. Department of Health and Human Services/CDC and National Institutes of Health. Biosafety in microbiological and biomedical laboratories [BMBL]. Richmond JY, McKinney RW, eds. 4th ed. Washington, DC: US Department of Health and Human Services, 1999 [Appendix F]). *In that report, physical security concerns were addressed, and efforts were focused on preventing unauthorized entry to laboratory areas and preventing unauthorized removal of dangerous biologic agents from the laboratory. Appendix F of BMBL is now being revised to include additional information regarding personnel, risk assessments, and inventory controls. The guidelines contained in this report are intended for laboratories working with select agents under biosafety-level 2, 3, or 4 conditions as described in Sections II and III of BMBL. These recommendations include conducting facility risk assessments and developing comprehensive security plans to minimize the probability of misuse of select agents.*

Risk assessments should include systematic, site-specific reviews of 1) physical security; 2) security of data and electronic technology systems; 3) employee security; 4) access controls to laboratory and animal areas; 5) procedures for agent inventory and accountability; 6) shipping/transfer and receiving of select agents; 7) unintentional incident and injury policies; 8) emergency response plans; and 9) policies that address breaches in security. The security plan should be an integral part of daily operations. All employees should be well-trained and equipped, and the plan should be reviewed annually, at least.

Introduction

Traditional laboratory biosafety guidelines have emphasized use of optimal work practices, appropriate containment equipment, well-designed facilities, and administrative controls to minimize risks of unintentional infection or injury for laboratory workers and to prevent contamination of the outside environment (*1*). Although clinical and research microbiology laboratories might contain dangerous biologic, chemical, and radioactive materials, to date, only a limited number of reports have been published of materials being used intentionally to injure laboratory workers or others (*2–7*). However, recently, concern has increased regarding possible use of biologic, chemical, and radioactive materials as terrorism agents (*8,9*). In the United States, recent terrorism incidents (*10*) have resulted in the substantial enhancement of existing regulations and creation of new regulations governing laboratory security to prevent such incidents.

The Public Health Security and Bioterrorism Preparedness and Response Act of 2002* (the Act) required institutions to notify the U.S. Department of Health and Human Services (DHHS) or the U.S. Department of Agriculture (USDA) of the possession of specific pathogens or toxins (i.e., select agents†), as defined by DHHS, or certain animal and plant pathogens or toxins (i.e., high-consequence pathogens), as defined by USDA. The Act provides for expanded regulatory oversight of these agents and a process for limiting access to them to persons who have a legitimate need to handle or use such agents. The Act also requires specified federal agencies to

The material in this report originated in the Office of Health and Safety, Robert H. Hill, Jr., Ph.D., Acting Director.

* Public Law 107–188, June 12, 2002.

† Throughout this report, the term *select agent* refers to specifically regulated pathogens and toxins as defined in Title 42, Code of Federal Regulations (CFR), Part 73, including pathogens and toxins regulated by both DHHS and USDA (i.e., overlapping agents and toxins). The reader should note that 42 CFR Part 73 has not been published yet, and is still under federal review with anticipated publication in December 2002.

withhold from public disclosure, among other requirements, site-specific information regarding the identification of persons, the nature and location of agents present in a facility, and the local security mechanisms in use. In addition, the Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001[§] prohibits restricted persons from shipping, possessing, or receiving select agents. Violation of either of these statutes carries criminal penalties.

Appendix F of the 4th edition of the CDC/National Institutes of Health, Biosafety in Microbiological and Biomedical Laboratories (BMBL) was the first edition to address laboratory security concerns (*1*). However, that publication primarily addressed physical security concerns (e.g., preventing unauthorized entry to laboratory areas and preventing unauthorized removal of dangerous biologic agents from the laboratory). The guidelines presented here are provided to assist facility managers with meeting the regulatory mandate of 42 Code of Federal Regulation (CFR) 73 and, therefore, include information regarding personnel, risk assessments, and inventory controls. These guidelines are intended for laboratories where select agents are used under biosafety levels (BSL) 2, 3, or 4 as described in Sections II and III of BMBL. Appendix F of BMBL is being revised to include consideration of the following biosecurity policies and procedures:

- risk and threat assessment;
- facility security plans;
- physical security;
- data and electronic technology systems;
- security policies for personnel;
- policies regarding accessing the laboratory and animal areas;
- specimen accountability;
- receipt of agents into the laboratory;
- transfer or shipping of select agents from the laboratory;
- emergency response plans; and
- reporting of incidents, unintentional injuries, and security breaches.

Definitions

Biosafety: Development and implementation of administrative policies, work practices, facility design, and safety equipment to prevent transmission of biologic agents to workers, other persons, and the environment.

Biosecurity: Protection of high-consequence microbial agents and toxins, or critical relevant information, against theft or diversion by those who intend to pursue intentional misuse.

Biologic Terrorism: Use of biologic agents or toxins (e.g., pathogenic organisms that affect humans, animals, or plants) for terrorist purposes.

Responsible official: A facility official who has been designated the responsibility and authority to ensure that the requirements of Title 42, CFR, Part 73, are met.

Risk: A measure of the potential loss of a specific biologic agent of concern, on the basis of the probability of occurrence of an adversary event, effectiveness of protection, and consequence of loss.

Select agent: Specifically regulated pathogens and toxins as defined in Title 42, CFR, Part 73, including pathogens and toxins regulated by both DHHS and USDA (i.e., overlapping agents or toxins).

Threat: The capability of an adversary, coupled with intentions, to undertake malevolent actions.

Threat assessment: A judgment, based on available information, of the actual or potential threat of malevolent action.

Vulnerability: An exploitable capability, security weakness, or deficiency at a facility. Exploitable capabilities or weaknesses are those inherent in the design or layout of the biologic laboratory and its protection, or those existing because of the failure to meet or maintain prescribed security standards when evaluated against defined threats.

Vulnerability assessment: A systematic evaluation process in which qualitative and quantitative techniques are applied to arrive at an effectiveness level for a security system to protect biologic laboratories and operations from specifically defined acts that can oppose or harm a person's interest.

Risk Assessment

Recommendation: Conduct a risk assessment and threat analysis of the facility as a precursor to the security plan.

Background: In April 1998, the General Accounting Office issued a report regarding terrorism (*11*). A key finding of that report was that threat and risk assessments are widely recognized as valid decision-support tools for establishing and prioritizing security program requirements. A threat analysis, the first step in determining risk, identifies and evaluates each threat on the basis of different factors (e.g., the capability and intent to attack an asset, the likelihood of a successful attack, and the attack's probable lethality). Risk management is the deliberate process of understanding risk (i.e., the likelihood that a threat will harm an asset with certain severity of

[§] Public Law 107–56, October 26, 2001.

consequences) and deciding on and implementing actions to reduce that risk. Risk management principles are based on acknowledgment that 1) although risk usually cannot be eliminated, it can be reduced by enhancing protection from validated and credible threats; 2) although threats are possible, certain threats are more probable than others; and 3) all assets are not equally critical. Therefore, each facility should implement certain measures to enhance security regarding select agents. The following actions should assist decision-makers in implementing this recommendation:

- Each facility should conduct a risk assessment and threat analysis of its assets and select agents. The threat should be defined against the vulnerabilities of the laboratory to determine the necessary components of a facility security plan and system (*12,13*).
- The risk assessment should include a systematic approach in which threats are defined and vulnerabilities are examined; risks associated with those vulnerabilities are mitigated with a security systems approach (*12,13*).
- Ensure the security plan includes collaboration between senior management, scientific staff, human resource officials, information technology (IT) staff, engineering officials, and security officials. This coordinated approach is critical to ensuring that security recommendations provide a reasonable and adequate assurance of laboratory security without unduly impacting the scientific work.

Facility Security Plans

Recommendation: Establish a facility security plan.

- Each facility should develop a comprehensive security plan that complies with 42 CFR Part 73 and reviews the need for policies in
  - — physical security;
  - — data and IT system security;
  - — security policies for personnel;
  - — policies for accessing select agent areas;
  - — specimen accountability;
  - — receipt of select agents into the laboratory;
  - — transfer or shipping of select agents from the laboratory;
  - — emergency response plans; and
  - — reporting of incidents, injuries, and breaches.
- Develop security policies based on site-specific assessments. Security plans should include measures that address physical security of building and laboratory areas. Policies should also address concerns associated with access, use, storage, and transfer of sensitive data. If sensitive electronic data are present, IT specialists should assess the security of hardware and software products in addition to the security of local area networks.
- Review safety, security, and IT policies and procedures at least annually for consistency and applicability. These procedures should also be reviewed after any incident or change in regulations. Necessary changes should be incorporated into the revised plans and communicated to all.
- Laboratory supervisors should ensure that all laboratory workers and visitors understand security requirements and that all employees are trained and equipped to follow established procedures. The security plan should be an integral part of daily operations. New employees should receive training when they first begin work, and all employees should receive training at least annually thereafter. Training should be updated as policies and procedures change. All training should be documented by maintaining records of training schedules and employee attendance.
- Security plans should receive periodic performance testing to determine their effectiveness. Test procedures can vary from a simple check of keys, locks, and alarms to a full-scale laboratory or facility exercise.

Security Policies for Personnel

Recommendation: Establish security-related policies for all personnel.

- Honest, reliable, and conscientious workers represent the foundation of an effective security program. Facility administrators and laboratory directors should be familiar with all laboratory workers.
- Establish a policy for screening employees who require access to select agent areas to include full- and part-time employees, contractors, emergency personnel, and visitors. Additional screening might be necessary for employees who require access to other types of sensitive or secure data and work areas. These screening procedures should be commensurate with the sensitivity of the data and work areas (e.g., federal security clearances for government employees and contractors).
- Ensure that all workers approved for access to select agents (e.g., students, research scientists, and other short-term employees) wear visible identification badges that include, at a minimum, a photograph, the wearer's name, and an expiration date. Facility administrators should consider using easily recognizable marks on the identification badges to indicate access to sensitive or secure areas.

Access Control

Recommendation: Control access to areas where select agents are used or stored.

- Consolidate laboratory work areas to the greatest extent possible to implement security measures more effectively. Separate select agent areas from the public areas of the buildings. Lock all select agent areas when unoccupied. Use keys or other security devices to permit entry into these areas.
- Methods of secure access and monitoring controls can include key or electronic locking pass keys, combination key pad, use of lock-boxes to store materials in freezers or refrigerators, video surveillance cameras, or other control requirements. Protocols for periodically changing combination keypad access numbers should be developed.
- Assess the need for graded levels of security protection on the basis of site-specific risk and threat analysis. This security can be accomplished through card access systems, biometrics, or other systems that provide restricted access.
- Lock all freezers, refrigerators, cabinets, and other containers where select agents are stored when they are not in direct view of a laboratory worker.
- Limit access to select agent areas to authorized personnel who have been cleared by the U.S. Department of Justice as indicated in 42 CFR Part 73. All others entering select agent areas must be escorted and monitored by authorized personnel.
- Record all entries into these areas, including entries by visitors, maintenance workers, service workers, and others needing one-time or occasional entry.
- Limit routine cleaning, maintenance, and repairs to hours when authorized employees are present and able to serve as escorts and monitors.
- Establish procedures and training for admitting repair personnel or other contractors who require repetitive or emergency access to select agent areas.
- Ensure visitors are issued identification badges, including name and expiration date, and escorted and monitored into and out of select agent areas. Such visits should be kept to a minimum.
- Ensure procedures are in place for reporting and removing unauthorized persons. These procedures should be developed through collaboration among senior scientific, administrative, and security management personnel. These procedures should be included in security training and reviewed for compliance at least annually.

Select Agent Accountability

Recommendation: Establish a system of accountability for select agents.

- Establish an accounting procedure to ensure adequate control of select agents and maintain up-to-date inventory of seed stocks, toxins, and agents in long-term storage. Records should include data regarding the agent's location, use, storage method, inventory, external transfers (sender/receiver, transfer date, and amount), internal transfer (sender/receiver, transfer date, amount), further distribution, and destruction (method, amount, date, and a point of contact).
- Establish procedures that maintain accurate and up-to-date records of authorizations for entry into limited access areas (i.e., a current list of persons who possess door keys and those who have knowledge of keypad access numbers or the security system).

Receiving Select Agents

Recommendation: Develop procedures for bringing select agent specimens into the laboratory.

- A centralized receiving area for select agents is recommended to maximize safety and minimize security hazards associated with damaged or unknown packages.
- Facilities should establish procedures for inspecting all packages (i.e., by visual or noninvasive techniques) before they are brought into the laboratory area. Suspicious packages should be handled as prescribed by federal and state law enforcement agencies.
- Biologic safety cabinet or other appropriate containment device should be used when opening packages containing specimens, bacterial or virus isolates, or toxins. Packages should be opened by trained, authorized personnel.

Transfer or Shipping of Select Agents

Recommendation: Develop procedures for transferring or shipping select agents from the laboratory.

- Package, label, and transport select agents in conformance with all applicable local, federal, and international transportation and shipping regulations, including U.S. Department of Transportation (DOT) regulations.[¶] Materials that are transported by airline carrier should also comply with packaging and shipping regulations set by

[¶] U.S. Department of Transportation, Research and Special Programs Administration, 49 CFR, Parts 171–180.

the International Air Transport Association (IATA). Personnel who package, handle, and ship these agents (including import and export) should be subject to all applicable training. The responsible facility official should be notified of all select agent transfers, internal or external.
- Ensure required permits (e.g., granted by the U.S. Public Health Service, USDA, DOT, U.S. Department of Commerce, and IATA) are obtained before select agents are prepared for transport. Standard operating procedures should be in place for import and export activities.
- Decontaminate contaminated or possibly contaminated materials before they leave the laboratory area.
- Avoid hand-carrying select agents when transferring them to other external facilities. If select agents are to be hand-carried on common carriers, all applicable packaging, transport, and training regulations should be followed.
- Develop and follow a protocol for intrafacility transfer of all select agents.

Emergency Response Plans

Recommendation: Implement an emergency response plan.
- Limiting access to select agent laboratory and animal areas can make implementing an emergency response more difficult. This should be considered as emergency plans are developed.
- Evaluate select agent laboratory and animal areas for safety and security concerns before an emergency plan is developed.
- Develop and integrate laboratory emergency plans with facilitywide plans. These plans should also include such adverse event assessments as bomb threats, severe weather (e.g., hurricanes or floods), earthquakes, power outages, and other natural or man-made disasters.
- Include facility administrators, scientific directors, principal investigators, laboratory workers, maintenance and engineering support staff, facility safety officers, and facility security officials in emergency planning.
- Include provisions for immediate notification of and response by laboratory and animal directors, laboratory workers, safety office personnel, or other knowledgeable persons when an emergency occurs.
- Establish advance coordination with local police, fire, and other emergency responders to assist community emergency responders in planning for emergencies in select agent laboratory and animal areas. Discussion should address security concerns associated with sharing of sensitive information regarding secure work areas.
- Consider circumstances that might require the emergency relocation of select agents to another secure location.
- Reevaluate and train employees and conduct exercises of the emergency response plan at least annually.

Incident Reporting

Recommendation: Establish a protocol for reporting adverse incidents.
- Ensure that laboratory directors, in cooperation with facility safety, security, and public relations officials, have policies and procedures in place for reporting and investigating unintentional injuries, incidents (e.g., unauthorized personnel in restricted areas, missing biologic agents or toxins, and unusual or threatening phone calls), or breaches in security measures.
- DHHS or USDA should be notified immediately if select agents are discovered to be missing, released outside the laboratory, involved in worker exposures or infections, or misused. Additionally, all incidents involving select agents (e.g., occupational exposure or breaches of primary containment) should be reported to local and state public health authorities.

Acknowledgments

CDC is grateful to the members of the Select Agent Interagency Workgroup, Biosecurity Subcommittee, and recognizes the contributions of Rachel E. Levinson, M.A., Chairman Biosecurity Subcommittee and Jonathan Y. Richmond, Ph.D., Assistant Chairman, Biosecurity Subcommittee.

References

1. US Department of Health and Human Services/CDC and National Institutes of Health. Biosafety in microbiological and biomedical laboratories. Richmond JY, McKinney RW, eds. 4th ed. Washington, DC: US Department of Health and Human Services, 1999.
2. Török TJ, Tauxe RV, Wise RP, et al. Large community outbreak of salmonellosis caused by intentional contamination of restaurant salad bars. JAMA 1997;278:389–95.
3. Kolavic SA, Kimura A, Simons SL, Slutsker L, Barth S, Haley CE. Outbreak of *Shigella dysenteriae* type 2 among laboratory workers due to intentional food contamination. JAMA 1997;278:396–8.
4. US Nuclear Regulatory Commission. Report to Congress on abnormal occurrences July–September 1995; dissemination of information. Federal Register 1996;61:7123–4.
5. US Nuclear Regulatory Commission. Incident investigation report: ingestion of phosphorus-32 at Massachusetts Institute of Technology, Cambridge, Massachusetts, identified on August 19, 1995 [NUREG-1535]. Washington, DC: US Nuclear Regulatory Commission, 1995.
6. US Nuclear Regulatory Commission. Preliminary notification of event or unusual occurrence PNO-1-98-052. Subject: intentional ingestion of iodine-125 tainted food (Brown University), November 16, 1998. Washington, DC: US Nuclear Regulatory Commission, 1998.

7. US Nuclear Regulatory Commission. National Institutes of Health issuance of director's decision under 10 CFR Sec. 2.206. Federal Register 1997;62:50018–33.
8. Atlas RM. Biological weapons pose challenge for microbiology community. ASM News 1998;64:383–9.
9. Ruys T. Laboratory design principles. In: Handbook of facilities planning. Ruys T, ed. New York, NY: John Wiley & Sons, 1990;257–64.
10. CDC. Update: investigation of anthrax associated with intentional exposure and interim public health guidelines, October 2001. MMWR 2001;50:889–93.
11. US General Accounting Office. Combating terrorism: threat and risk assessments can help prioritize and target program investments. Washington, DC: US General Accounting Office, 1998. Publication no. GAO/NSIAD-98-74.
12. Johnson B. Understanding, assessing, and communicating topics related to risk in biomedical research facilities [Chapter 10]. In: Richmond JY, ed. Anthology of biosafety: IV. Issues in public health. Mundelein, IL: American Biological Safety Association, 2001;149–166.
13. Royes C, Johnson B. Security considerations for microbiological and biomedical facilities [Chapter 6]. In: Richmond JY, ed. Anthology of biosafety: V. BSL–4 laboratories. Mundelein, IL: American Biological Safety Association, 2002;131–148.

All *MMWR* references are available on the Internet at http://www.cdc.gov/mmwr. Use the search function to find specific articles.

Use of trade names and commercial sources is for identification only and does not imply endorsement by the U.S. Department of Health and Human Services.

References to non-CDC sites on the Internet are provided as a service to *MMWR* readers and do not constitute or imply endorsement of these organizations or their programs by CDC or the U.S. Department of Health and Human Services. CDC is not responsible for the content of these sites. URL addresses listed in *MMWR* were current as of the date of publication.

The *Morbidity and Mortality Weekly Report (MMWR)* series is prepared by the Centers for Disease Control and Prevention (CDC) and is available free of charge in electronic format and on a paid subscription basis for paper copy. To receive an electronic copy each week, send an e-mail message to *listserv@listserv.cdc.gov*. The body content should read *SUBscribe mmwr-toc*. Electronic copy also is available from CDC's Internet server at *http://www.cdc.gov/mmwr* or from CDC's file transfer protocol server at *ftp://ftp.cdc.gov/pub/publications/mmwr*. To subscribe for paper copy, contact Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402; telephone 202-512-1800.

Data in the weekly *MMWR* are provisional, based on weekly reports to CDC by state health departments. The reporting week concludes at close of business on Friday; compiled data on a national basis are officially released to the public on the following Friday. Address inquiries about the *MMWR* series, including material to be considered for publication, to Editor, *MMWR* Series, Mailstop C-08, CDC, 1600 Clifton Rd., N.E., Atlanta, GA 30333; telephone 888-232-3228.

All material in the *MMWR* series is in the public domain and may be used and reprinted without permission; however, citation of the source is appreciated.

☆U.S. Government Printing Office: 2003-533-155/69076 Region IV