Material control and accountability for laboratory biosecurity

George T. Baldwin*, Susan B. Rivera and Reynolds M. Salerno

Sandia National Laboratories,
Albuquerque, NM 87185, USA
E-mail: gtbaldw@sandia.gov
E-mail: srivera@miox.com
E-mail: rmsaler@sandia.gov
*Corresponding author

Abstract: Laboratory biosecurity refers to a suite of measures to protect legitimate stocks of dangerous pathogens and toxins from being acquired by individuals with malicious intent. Intentional misuse presents a different problem than accidental misuse, which is the subject of laboratory biosafety. In particular, the material control and accountability (MC&A) component of laboratory biosecurity addresses an insider threat. MC&A directly involves the personnel who work with pathogens and toxins that could be attractive to bioterrorists. Control of material comprises both procedural and physical measures for both material and MC&A-relevant information. Accountability requires a one-to-one correspondence between materials and people, together with a system of records, reporting and audit. Key elements of MC&A should be understood intellectually, rather than being applied simply as a prescriptive list of security measures. MC&A measures reflect an additional stewardship responsibility that technical people accept in working with material that could harm others if used improperly.

Keywords: accountability; biosecurity; control; laboratory; material; pathogen; security; stocks; toxin.

Reference to this paper should be made as follows: Baldwin, G.T., Rivera, S.B. and Salerno, R.M. (2009) 'Material control and accountability for laboratory biosecurity', *Int. J. Risk Assessment and Management*, Vol. 12, Nos. 2/3/4, pp.368–379.

Biographical notes: George T. Baldwin, PhD, is a member of the technical staff in Global Security Programs at Sandia National Laboratories. His major professional interests involve technical verification and confidence building measures for non-proliferation, including international nuclear safeguards, the Additional Protocol, fissile material cutoff, disposition of excess materials and related issues. His principal expertise is in radiation detection, nuclear instrumentation and measurements applied to reactors, particle accelerators and inertial fusion machines. He worked previously for the Safeguards Department at the International Atomic Energy Agency in Vienna, Austria. He is a member of the American Physical Society and the Institute for Nuclear Materials Management. He holds a BA in physics from Kalamazoo College and PhD in nuclear engineering from the University of Michigan.

Susan B. Rivera, PhD CPO, is the Manager of Research and Development at MIOX Corporation. MIOX Corporation is helping to provide innovative, sustainable, energy efficient and practical solutions to the world water crisis, an

Copyright © 2009 Inderscience Enterprises Ltd.

endeavour which requires partnerships with industry leaders, government oversight agencies, NGOs and federal/state/local governments. She interfaces with these sector representatives and water science experts and plays a key role in MIOX's international point-of-use and point-of-entry water purification initiatives. She earned her Doctorate in Biochemistry from the University of Utah. She commenced Postdoctoral work at Sandia National Laboratories in bionanomechanical system characterisation and assembly. She next worked on International Biological Threat Reduction and Homeland Security at Sandia, participating in security assessments at US government bioscience facilities and contributing to the development of international biosecurity guidelines. In her current position at MIOX, she assists stakeholders in the area of water security.

Reynolds M. Salerno, PhD, is the Manager of International Biological Threat Reduction in the Global Security Programs at Sandia National Laboratories. Recognised as a leading expert on laboratory biosecurity in the United States, he and his team have worked extensively in laboratory biosafety, biosecurity, and disease surveillance and diagnostics internationally. In the last five years, he and his team have visited biocontainment laboratories in more than 20 countries, specifically to consult on biosafety and biosecurity issues. They have also presented major biosafety and biosecurity workshops in ten different countries since 2004 and have many more international workshops currently planned. He has published widely in the biological threat reduction and counter-bioterrorism field. He received his PhD from Yale University in 1997.

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

1 Introduction

Bioterrorism, the intentional and malicious use of pathogens or toxins to cause harm, is a widely recognised threat. Preparing to respond to a bioterrorist act is clearly critical to any comprehensive strategy to counter the threat. In the US alone, between 2001 and 2004, over $10 billion was invested for biodefence to improve disease surveillance, vaccines and therapeutics, detection capability, and emergency response (Biodefense for the 21st Century, 2004). Preparations for detection and response are important, but so too are steps that would prevent or complicate the acquisition of pathogens or toxins for bioterrorist use in the first place. Public health and medical research necessarily involve maintaining stocks of pathogens and toxins for legitimate purposes. Although such research and diagnostic stocks are not an exclusive source for bioterrorist material, they are organisms that have been isolated and whose viability and virulence have often already been characterised – important technical hurdles that any bioterrorist would have to overcome. Thus, dangerous pathogens and toxins in legitimate laboratories could represent attractive sources unless precautions are taken. Laboratories must take appropriate measures to reduce the risks of such materials being stolen and misused.

Laboratory biosecurity (or pathogen security) refers to a suite of measures that help to protect legitimate stocks of dangerous pathogens and toxins from being acquired by individuals with malicious intent. For example, legitimate facilities must be secured so that outsiders cannot easily break in: thus, physical protection is one obvious element of

laboratory biosecurity. Access control limits those who can enter to only trusted people with an acknowledged, legitimate reason for access. Personnel management determines exactly who can and should be trusted with access. These and other elements of laboratory biosecurity have been described at greater length elsewhere (Tucker, 2003).

If laboratory biosecurity is to be at all effective, those who work with dangerous pathogens and toxins must appreciate the security issues and requirements of their work. Especially in the aftermath of the anthrax attacks in the United States in late 2001, many legislative and regulatory steps have been imposed on the biotech, pharmaceutical, medical and public health communities, but without commensurate explanations that would assist in the understanding and acceptance of these security measures.

In this article, we discuss the rationale for and the role of material control and accountability ('MC&A') in laboratory biosecurity. MC&A measures directly involve the personnel who work with the pathogens and toxins that could be attractive to bioterrorists. The overview of key elements of MC&A that follows is not meant to provide a prescriptive list of security measures, but rather to establish an intellectual and philosophical understanding of what MC&A is, what it seeks to accomplish and why it is necessary.

2 The rationale for material control and accountability

Even if all other aspects of laboratory biosecurity are implemented – physical facilities have been protected, only authorised people are granted access to the facilities, and management ensures that those authorised people truly warrant public trust – the security is not complete. There remain two principal concerns, both examples of an 'insider threat'.

1 The professional or personal situation of a trusted individual with authorised access could change in a way that might provoke or enable malicious behaviour.

2 An individual with malicious intent could under false pretences become a trusted member of the workforce with authorised access.

If applied correctly, the MC&A component of laboratory biosecurity can help mitigate the insider threat.

Most people react defensively to the notion of an insider threat: 'That would never happen here'. Nevertheless, can one be certain that somewhere, someone in a similar position of responsibility is always acting with noble intentions? The possibility of malicious intent, however small, does exist. The object of MC&A measures is to create an environment that discourages such misbehaviour. MC&A seeks to establish practices and culture that systematically prevent and deter misuse scenarios, rather than relying exclusively on individual ethics and behaviour.

3 Relationship to biosafety

The biotech, pharmaceutical, medical and public health communities are well aware of the need for safety precautions in working with hazardous materials, and in particular, with pathogens and toxins (BMBL, 1999; Laboratory Biosafety Manual, 2004). Laboratory biosafety measures have existed for many years. Clearly, a technical person

has a vested interest in taking such measures to heart. Not doing so could risk personally suffering direct consequences. Biosafety measures protect not only occupational workers; but also they protect the public and the environment from accidents involving pathogens and toxins. Laboratory biosecurity is similar, but has subtle differences.

Laboratory biosecurity is a recognition of an additional stewardship responsibility that technical people accept in working with material that could harm others if used improperly. It is the assurance that an individual will not deliberately use material maliciously, and will take every reasonable precaution to prevent others from doing so. While biosafety is concerned with accidental misuse, biosecurity is concerned with intentional misuse.

4 The role of material control and accountability

MC&A measures enhance laboratory biosecurity by establishing exactly what biological material is present at a facility, how and where the material is stored and handled, and who is responsible for it. MC&A combines policies, procedures and technologies to augment other elements of laboratory biosecurity during the use, storage and transfer of material. Control ensures that material is confined to known, legitimate use, while accountability ensures oversight by formally associating material with people and information records. We discuss each of these elements of MC&A in turn.

4.1 Material

The first issue for MC&A is to define 'material' precisely. Material could include any infectious or toxic biological agent, capable of causing harm to human, animal or plant populations. From the laboratory biosecurity perspective, material includes those agents – pathogens and toxins – deemed to be potentially attractive to diversion for deliberate misuse.

CDC list of bioterrorism agents/diseases[2]

Category A

Pose a risk to national security: easily disseminated or transmitted; high mortality; potential for major public health impact including panic and social disruption. Require special action for public health preparedness.

Anthrax (*Bacillus anthracis*)

Botulism (*Clostridium botulinum toxin*)

Plague (*Yersinia pestis*)

Smallpox (*variola major*)

Tularemia (*Francisella tularensis*)

Viral hemorrhagic fevers (filoviruses [e.g. Ebola, Marburg] and arenaviruses [e.g. Lassa, Machupo]).

Category B

Moderately easy to disseminate; moderate morbidity and low mortality rates. Require enhanced diagnostic capacity and disease surveillance.

- Brucellosis (Brucella species)
- Epsilon toxin of *Clostridium perfringens*
- Food safety threats (*e.g. Salmonella species, Escherichia coli* O157:H7, Shigella)
- Glanders (*Burkholderia mallei*)
- Melioidosis (*Burkholderia pseudomallei*)
- Psittacosis (*Chlamydia psittaci*)
- Q fever (*Coxiella burnetii*)
- Ricin toxin from *Ricinus communis* (castor beans)
- Staphylococcal enterotoxin B
- Typhus fever (*Rickettsia prowazekii*)
- Viral encephalitis (alphaviruses [e.g. Venezuelan equine encephalitis, eastern equine encephalitis, western equine encephalitis])
- Water safety threats (*e.g. Vibrio cholerae, Cryptosporidium parvum*).

Category C

Emerging pathogens that could be engineered for mass dissemination due to availability, ease of production and dissemination, and potential for high morbidity, mortality and major health impact.

- Emerging infectious diseases such as Nipah virus and hantavirus

Commonly, material is defined by externally imposed regulation (Agricultural Bioterrorism Protection Act of 2002; possession, use, and transfer of biological agents and toxins final rule, 2005; Possession, use, and transfer of select agents and toxins final rule, 2005). Given the rapid progress of biological and medical development, such lists are necessary, but not sufficient. Those who work with biological agents ultimately need to take responsibility for identifying laboratory biosecurity-relevant material.

Ideally, material subject to MC&A should be identified by a rigorous risk assessment. Risk assessment, the basis for an overall implementation of risk management, is essential to ensure that security resources are applied effectively. Protecting all assets against all possible threats is clearly impossible, so judgments need to be made that help optimise MC&A.[1] The risk assessment methodology should further be specific for biological facilities and agents (Gaudioso, Salerno and Barnett, 2006).

Not all harmful biological material is equally attractive to bioterrorists (Casadevall and Pirofski, 2004). Although there is often significant overlap between material of biosafety concern and laboratory biosecurity concern, they are not always the same. The safety risks associated with *Bacillus anthracis*, for example, are typically mitigated through the use of 'BSL-2' laboratory conditions. Nevertheless, a variety of other

properties of *B. anthracis* makes it especially attractive as a bioterrorism weapon. A corresponding laboratory biosecurity index, were it to exist, would certainly rate *B. anthracis* to be of serious concern from a security perspective (Gaudioso and Salerno, 2004).

The difficulty in defining material subject to MC&A is in the details. The starting and ending points for capturing material must be clear. For example, the virulence sequences of pathogen DNA alone could qualify. Clinical, diagnostic or unknown samples suspected of containing an infectious substance need to be considered. From a laboratory perspective, material is sometimes distinguished between working stocks and seed stocks, but such categorisation does not by itself indicate different MC&A significance. Control measures likely differ for the two categories.

4.2 Control

Control is the core of MC&A practice. It is the overall effect of many separate measures, taken together, that ensure material stays (or in the case of transfer, goes) where it is supposed to, and that it is used for legitimate purpose by the right people.

Control must deal with all activities involving material, such as storage, use, transfer and disposal. Control should be effective under both normal conditions and anticipated abnormal conditions wherever possible, such as accidents, power failures or emergencies. Otherwise, covert diversion of material could be attempted under the cover of some abnormal condition (perhaps intentionally caused).

The application of control measures should be 'graded' such that material of greatest concern is subject to the most stringent control, while that of lesser concern is subject to correspondingly lesser control. The reason is to allocate resources sensibly and effectively, while minimising intrusiveness of control measures. For example, control may seek only to detect (and thus deter) misuse, or it may be intended to prevent misuse. Detection might be implemented periodically, randomly or promptly.

Fundamentally, material exists in a 'bulk' state, and often is capable of replicating from an arbitrarily small amount. To set certain *de minimus* amounts of material that can be exempt from MC&A is largely unrealistic, except for toxins. Bulk material cannot be dependably quantified to determine whether any has gone missing.

Thus to facilitate control, material is best aggregated – at some level – into discrete 'items'. Items can be counted, identified and labelled. They may be 'distinguishable' (i.e. identified uniquely) or 'indistinguishable'. Material in solution in a test tube, or sealed in an ampoule is aggregated as an item, for example. Similarly, material in an animal carcass might be an item, but better if the carcass itself were confined in a sealed box; the box would then become the item.

Control measures should:

1 assure the integrity of each material item

2 assure that no item is missing

3 minimise the opportunity for misuse during activities that necessarily involve bulk material.

Item integrity means establishing a complete boundary around an item, so that material within the item cannot easily cross that boundary without detection.

'Containment and surveillance' measures can be useful for control. Containment, here not the same as biosafety containment, often entails tamper indication, the use of an enclosure ('seal') that would reveal the possible loss of item integrity. Seals require inspection and verification – possibly periodically, or before intended, legitimate use. Surveillance might be done directly by other people, or assisted with cameras (video surveillance is not usually easy to implement: it requires attention to many details and issues, can be quite expensive, and may not be effective).

Defining items at the most detailed level possible may not be necessary. An item could be a cabinet or freezer, or even a restricted-access laboratory, provided that control measures can assure item integrity. If able to be done, such higher-level aggregation would obviate any need to count vials.

Ideally, the particular set of controls devised should be developed by those most closely connected to the work itself. By taking stock of laboratory material and activities from a laboratory biosecurity perspective, and being informed by an impartial risk assessment, laboratory managers should be able to develop a workable collection of procedural and physical measures that would improve the security of material subject to MC&A.

4.2.1 Procedural measures

Procedures, designed in advance and explicitly considering their laboratory biosecurity implications, are central to the effective control of pathogens and toxins. Procedures are important for many other reasons besides laboratory biosecurity, such as for quality control or worker safety. They are not something new. What is new, however, is the need to re-examine existing practices to ensure that procedures reflect laboratory biosecurity concerns. MC&A procedures can be developed in concert with mindful, site-specific work planning by responsible and qualified individuals.

Ideally, MC&A procedures would be integrated with currently existing, standard laboratory procedures. In some cases, additional procedures could be required, whether dictated by externally imposed regulations, or because they intuitively make sense. Special attention should be given to procedures associated with potentially dual-use equipment like a large fermenter, where its legitimate purpose could also be subverted easily to an illegal use.

The kinds of activities that will require procedures likely include:

- working with material
- inactivating and disposing of material
- conducting periodic inventory checks
- removing material from, and returning it to, storage
- labelling sample containers.

In addition to procedures for routine activities, unexpected conditions should be anticipated wherever possible. What is the course of action if a sample is discovered missing?

Certain general requirements should be recognised for procedures to be effective:

- all procedures should be written
- corresponding training, with associated testing, should be provided
- procedures should be reviewed periodically and updated as necessary
- any relevant contributing discussion should be documented, which will help to clarify the reasoning behind procedural decisions.

4.2.2 Physical measures

Physical controls are engineered solutions to help prevent misuse. They use technology to assist or complement the procedural measures.

For example, a locked freezer or vault can provide additional control in laboratory spaces that are shared among more individuals than actually work with a particular material. Automated systems can log events such as lab access (in and out) or freezer opening/closing. Such systems can record both time of the event and personal identification. Barcode labels or radiofrequency tags are engineered measures that can facilitate inventory-taking.

4.2.3 Information control

The information produced in the course of implementing MC&A itself introduces a concern for laboratory biosecurity. Combinations to locks on freezers or vaults, or the precise locations of specific material, illustrate the sensitivity of MC&A information: security would be compromised if the information is divulged to, or accessible by, anyone who does not need that information. Thus, establishing and enforcing a 'need to know' requirement – even for otherwise authorised people – is essential to information control.

MC&A-relevant information is not the same as laboratory research results or the scientific content of publications. Classification of research findings, methods and techniques is an entirely separate question. The laboratory biosecurity consideration here is limited specifically to avoid the release of information about

1. Where particular material is and how one might obtain it for malicious use;
2. What specific laboratory biosecurity measures are in place at specific facilities to protect material.

Publications should be reviewed to prevent unnecessary release of such MC&A-relevant information.

Examples of measures to control MC&A sensitive information include limiting access to computer networks and databases, using secure e-mail, marking and physically securing sensitive electronic and hardcopy documents, and restricting distribution. Once again, details create the difficulties. How can the need to limit access be reconciled with the need for backup (e.g. for a freezer combination)? How can management be prevented from exercising authority to extract MC&A information from subordinates illegitimately?

4.3 Accountability

4.3.1 Accountable person

Accountability involves ensuring that for every item of material subject to MC&A, there is an associated individual who is responsible for its oversight. This 'accountable person' should be qualified, authorised and able to carry out the oversight function. Oversight includes the maintenance of records, reporting and ensuring control of the material. The accountable person is responsible for knowing how, when, where and why particular material has been used, transferred or destroyed.

The basis for such personal accountability is simply to ensure that no material is 'orphaned', i.e. permitted to exist within a laboratory without someone being held accountable for it. Someone must both recognise the need for stewardship responsibility of the material and be willing to accept it.

Enforcing a system of accountability will likely mandate decisions on whether or not to retain stocks of MC&A-subject material. Considering its security liability, certain dangerous material should not be retained 'casually'. There is an overhead cost that MC&A entails, which must be weighed against the perceived benefits of retaining that material.

Personal accountability for material should be integrated with the standard management practice of the organisation itself. For example, management would assign responsibility for accountability, training and auditing; plan and evaluate implementation; and ensure the continuity of accountability as people transfer or leave the organisation.

4.3.2 Accountability records

Information records are a critical part of the accountability aspect of MC&A. They are often dictated externally by regulations, but any laboratory should do its own assessment of information records from a laboratory biosecurity perspective.

Most records exist for the institution to retain historical knowledge about MC&A-subject material. Exactly how such knowledge is recorded may vary considerably according to the particular circumstances. The object is to be able to describe both the existence and use of material accurately and completely, so that an accountable person is able to answer questions that could arise later. Laboratory notebooks, inventory as manual ledgers or electronic files and databases, and shipping/receiving receipts are all examples of material records that serve accountability purposes. The information record should indicate unambiguously the specific material and the associated accountable person.

Decisions must be made about several aspects of record keeping:

- When must information be recorded?
- What information must be kept?
- How long must information be kept?
- Where should information records be kept?
- What security is required for these records?

4.3.3 Reporting and audit

A final element of the accountability aspect of MC&A is reporting and audit. Otherwise an institution would have no assurance that any of its best intentions were actually happening.

Routine reports incur extra administrative overhead, so their frequency and detail will be limited. Nevertheless, they assure management that continuing attention is being paid to MC&A practice, and may be required for compliance with external regulations.

Anything out of the ordinary should not rely on routine reporting, however. In that case, a mechanism for non-routine reporting can ensure timeliness and facilitate response. Fostering an environment that encourages anyone to report anomalies like unjustified access is essential.

Reporting must also be viewed as a potential information control issue. Management has a need to know at some level, but it is unlikely that an upper level manager needs to know a particular freezer combination, for example. MC&A-relevant information must necessarily be abstracted as it is passed on to higher-levels of management.

5 Discussion

The focus for MC&A (and laboratory biosecurity in general) is specifically the security of legitimate stocks of dangerous pathogens and toxins. The concern here is not with everything considered valuable, *per se.* Clearly, there is also a need for security in a broader sense, which preserves the overall ability of an institution to carry out its mission.

Will a system of MC&A measures ever be perfect? No, but a system that includes MC&A measures should be substantially better than one without such measures. What MC&A cannot control entails a residual risk. The efficacy of MC&A needs to be balanced against cost to assess just what risks can be tolerated.

Several issues are involved when implementing MC&A initially. Usually, there will be a legacy of stored materials that calls for laboratory house-cleaning, a luxury for which there is never enough time or an ideal time. Stored samples may need to be identified and characterised if information has been lost. The laboratory may either decide to diagnose a sample or simply destroy it. In most cases, retaining an unknown for unspecified reasons entails too great a risk.

How an institution utilises its laboratory space may need to change. Work may need to be consolidated and compartmentalised. Work with dangerous pathogens and toxins (e.g. 'select agents' in the United States) would best be separated from work with other materials that do not require such overhead. Reducing the amount of readily available 'working material', and the number of places where it exists, together with applying better control of long-term storage, will involve conscious decisions that may involve changes from previous practice.

Substantial benefits can be realised from a conscientious implementation of MC&A practice. The primary one is of course reducing the opportunity for misuse of material held by legitimate facilities, which alone would be sufficient reason for MC&A. MC&A may accomplish this directly, through effective control of dangerous pathogens and toxins, but also indirectly, by deterring misuse. Another significant benefit is that effective MC&A will enable research and operation to continue, and may even lessen the chance for suffering increased regulation. By transparently assuring that conditions are in

place so that misuse of material is unlikely, an institution strengthens its legitimacy to continue work. Finally, MC&A measures are fully compatible with good research practice, quality and accreditation standards (ISO 15189:2003, 2003).

Measures may already be implemented in various institutions that appear to be (and may in fact be called) MC&A, but they may have been developed for reasons other than laboratory biosecurity. In such cases those measures should be reviewed explicitly from a laboratory biosecurity perspective, rather than merely assuming that existing measures suffice.

Institutional management must not only ensure that all who have access to material understand their MC&A responsibilities, but also they must promote a supportive work environment. Individual technical people should embrace laboratory biosecurity as an unavoidable response to newly recognised threats, and help to find ways to ensure that it is not merely tolerated, but consciously integrated as standard practice. Ultimately, the most powerful guarantor of effective MC&A will be the attitudes and behaviour of those who are responsible for it.

References

Agricultural bioterrorism protection act of 2002; possession, use, and transfer of biological agents and toxins final rule (2005) US Department of Agriculture, 7 CFR Part 331 and 9 CFR Part *121, Federal Register*, Vol. 70, pp.13242–13292, March 18.

Biodefense for the 21st Century (2004) Available at: http://www.whitehouse.gov/news/releases/2004/04/20040428-6.html.

Biosafety in Microbiological and Biomedical Laboratories (BMBL) (1999) (4th ed.) *US Department of Health and Human Services*, Centers for Disease Control and Prevention, and National Institutes of Health, May.

Casadevall, A. and Pirofski, L. (2004) 'The weapon potential of a microbe', *Trends in Microbiology*, Vol. 12, pp.259–263.

Gaudioso, J. and Salerno, R. (2004) 'Science and government: biosecurity and research: minimizing adverse impacts', *Science*, Vol. 304, p.687.

Gaudioso, J., Salerno, R. and Barnett, N. (2006) 'Developing a risk assessment and management approach to laboratory biosecurity', *Applied Biosafety*. Vol. 11.

ISO 15189:2003 (2003) 'Medical laboratories – particular requirements for quality and competence', *International Organization for Standardization*.

Laboratory Biosafety Manual (2004) (3rd ed.), World Health Organization.

Possession, use, and transfer of select agents and toxins final rule (2005) *US Department of Health and Human Services, 42 Code of Federal Regulations Part 73, Federal Register*, Vol. 70:52, pp.13294–13325, March 18.

Tucker, J. (2003) 'Limiting terrorist access to deadly pathogens', *Peaceworks 52*, United States Institute of Peace, November; Salerno, R. and Estes, D. (2005) 'Biosecurity: protection of high consequence pathogens and toxins against theft and diversion', in R. Pilch and R. Zilinskas (Eds), *Encyclopedia of Bioterrorism Defense*. Hoboken: Wiley-Liss.

Notes

[1] The US Government Accountability Office endorses a risk management approach to security, i.e. an approach that

1. establishes which assets should be protected against which threats
2. ensures that the amount of protection provided to a specific asset, and the cost for that protection, is proportional to the risk of the theft or destruction of that asset.

See 'Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts', US Government Accountability Office, GAO-02-208T (Washington, DC: October 2001), and 'Combating Bioterrorism: Actions Needed to Improve Security at Plum Island Animal Disease Center', GAO-03-847, (Washington, DC: September 2003).

[2] US Department of Health and Human Services, Centers for Disease Control and Prevention, Nov 19, 2004, http://www.bt.cdc.gov/agent/agentlist-category.asp.