International
BIOLOGICAL THREAT REDUCTION

Biological Risks and Risk Management: Lab Biosafety and Biosecurity

Reynolds M. Salerno, Ph.D., Manager
International Biological Threat Reduction
Sandia National Laboratories
Albuquerque, NM USA

National Training Seminar on Biosafety and Biosecurity, Pakistan, June 2007

www.BEPstate.net

www.biosecurity.sandia.gov

Sand No. 2006-2174C, 2007-1747P 2005-7121C, 2005-7122C, 2005-7039C
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.

BIOSECURITY ENGAGEMENT PROGRAM

Evolution of the Biological Threat

- The biological threat has evolved in concert with
  - Increasing emergence and re-emergence of highly infectious disease
  - Advance of biotechnology globally
  - Rise of transnational, asymmetric terrorism
- This recent "globalization" of the biological threat has broadened the availability of materials, technologies, and expertise needed to maliciously disseminate infectious disease

Mt. Merapi, Yogyakarta, Indonesia

2

Infectious Disease

- Global outbreaks of emerging and re-emerging infectious disease present a growing threat to international security
- Most dangerous infectious diseases are often tropical diseases that emerge in developing countries
- Infectious diseases now spread across borders as never before
- Natural outbreaks represent unpredictable sources of dangerous pathogens for terrorists

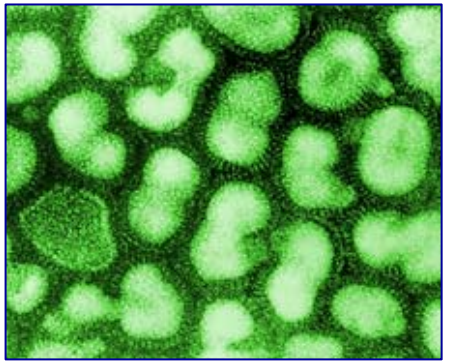
SARS virus

FMD outbreak UK

3

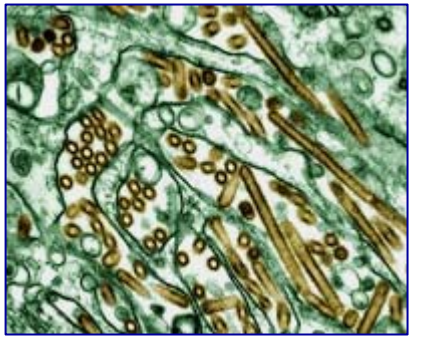
Highly Pathogenic Avian Influenza

- **H5N1 strain of highly pathogenic avian influenza first emerged in 1997 and has spread to 59 countries**
  - **Officially 306 people infected, and 185 fatalities**
  - **Has also infected other mammals**



Avian influenza virus

- **Sequencing of the 1918 pandemic influenza virus revealed that H5N1 is very similar *(Taubenberger 2005)***
  - **Unlike the strains of the 1958 and 1967 pandemics**



- **The virus is evolving**
  - **Strain in Turkey had mutations that made it more adaptable to humans than birds**
  - **Strain in Vietnam resistant to Tamiflu®**
  - **Confirmed human-to-human transmission in Indonesia**

4

Biotechnology and the Life Sciences

- Rapid expansion of bioscience worldwide is perhaps the most significant influence on the biological threat
- Viable and virulent organisms are stored and used in more legitimate bioscience facilities across the globe than ever before
- Individuals with the expertise necessary to misuse biology can be found in nearly all areas of the life sciences internationally
- The tools necessary to develop and disseminate a low-grade biological weapon are ubiquitous

5

Double-Edge Sword of Biotechnology

- **Genetic modification**
  - **2001 – IL-4 and mousepox (Australia)**
  - **2003 – IL-4 and mousepox (St. Louis)**
- **Chemical synthesis**
  - **2002 – polio virus (Stony Brook)**
  - **2003 – phi-X174 virus (Venter)**
  - **2005 – 1918 influenza virus (Taubenberger)**

- **Advance of biotechnology will ease**
  - **Acquisition barriers**
  - **Production barriers**
  - **Dissemination barriers**

6

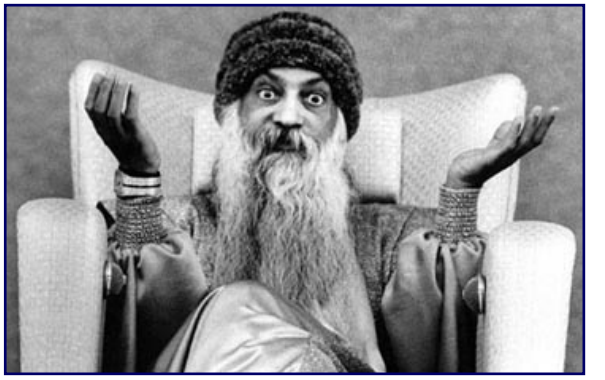
Origins of Bioterrorism

- In 1910, the Pancho Villa guerillas used shards of pottery and obsidian laced with botulinum toxin to attack federal sentries

- In 1952, the Kenyan Mau Mau separatist group used African milk brush toxin to poison steer

- In 1981, Dark Harvest, an environmental extremist group in the United Kingdom, delivered anthrax-contaminated soil to a political party conference

- In 1984, Rajneeshees cult contaminated restaurant salad bars in The Dalles, Oregon with salmonella bacteria



Bhagwan Shree Rajneesh

Gruinard Island, UK

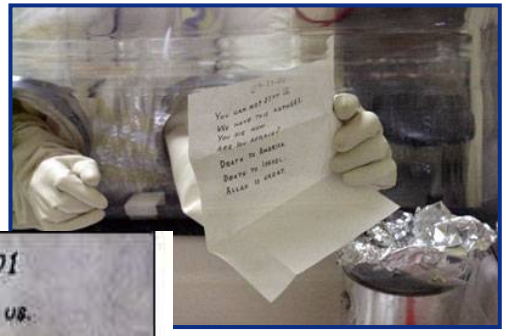
7

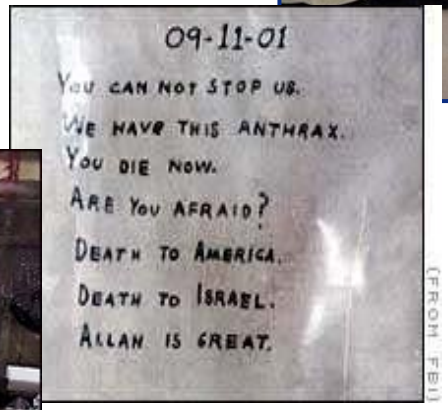
Escalation of Bioterrorism

Aerosolization of Bacillus anthracis and botulinum toxin by Aum Shinrikyo

- **Aum Shinrikyo – 1990s**
  - **Aerosolized and disseminated biological agents in Japan**
    - **Vaccine strain of *Bacillus anthracis***
    - **Inactive strain of *Clostridium botulinum***

- **US anthrax attacks – 2001**
  - **Highly refined: 4-7 letters contaminated over 60 different sites**
  - **Highly virulent: killed 5, injured 22**





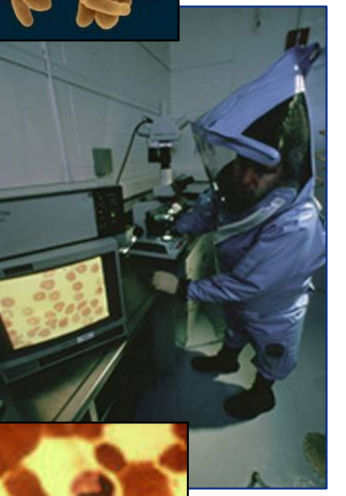
Amerithrax

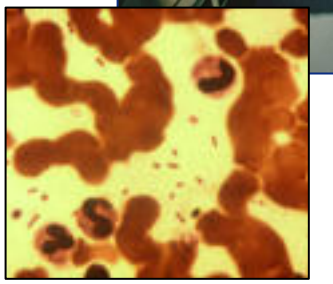
8

Laboratory Biosafety and Biosecurity

- **Laboratory biosafety**
  - **Objective: reduce or eliminate accidental exposure to or release of potentially hazardous agents**
- **Laboratory biosecurity**
  - **Objective: protect biological agents against theft by those who intend to cause harm**
- **Common strategy**
  - **Implement graded levels of protection based on a risk management methodology**
- **Control of certain biological materials is necessary, but *how* that is achieved must be carefully considered**
  - **Laboratory biosecurity and biosafety should be integrated systems that avoid compromising necessary infectious disease research and diagnostics**

Francisella tularensis





Yersinia pestis

9

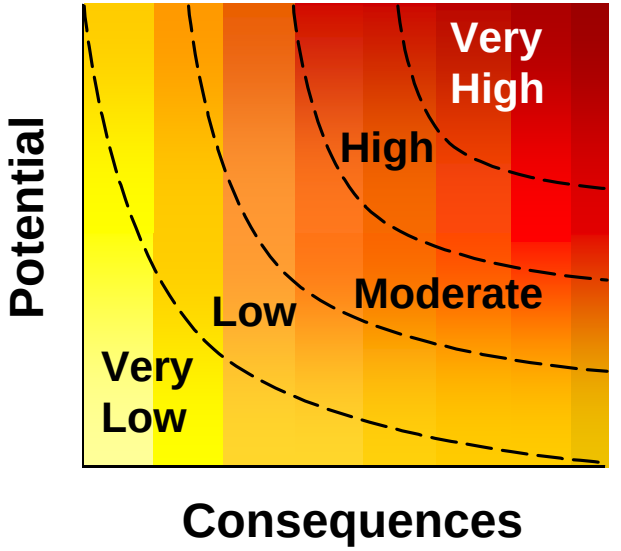
Strengthening Biological Risk Management

Vision for Integrated BioRisk Management:

- ✓ Increased focus on "awareness" to change current culture
- ✓ Clarify terminology
- ✓ Development of targeted "training strategies"
- ✓ Securing "commitment" from key stakeholders, including government officials, who must be on board
- ✓ Continue increasing "capacity" based on Regional/Country needs and establish accountability through development of Country "report cards"

Biosecurity and Biosafety Based on Risk Management

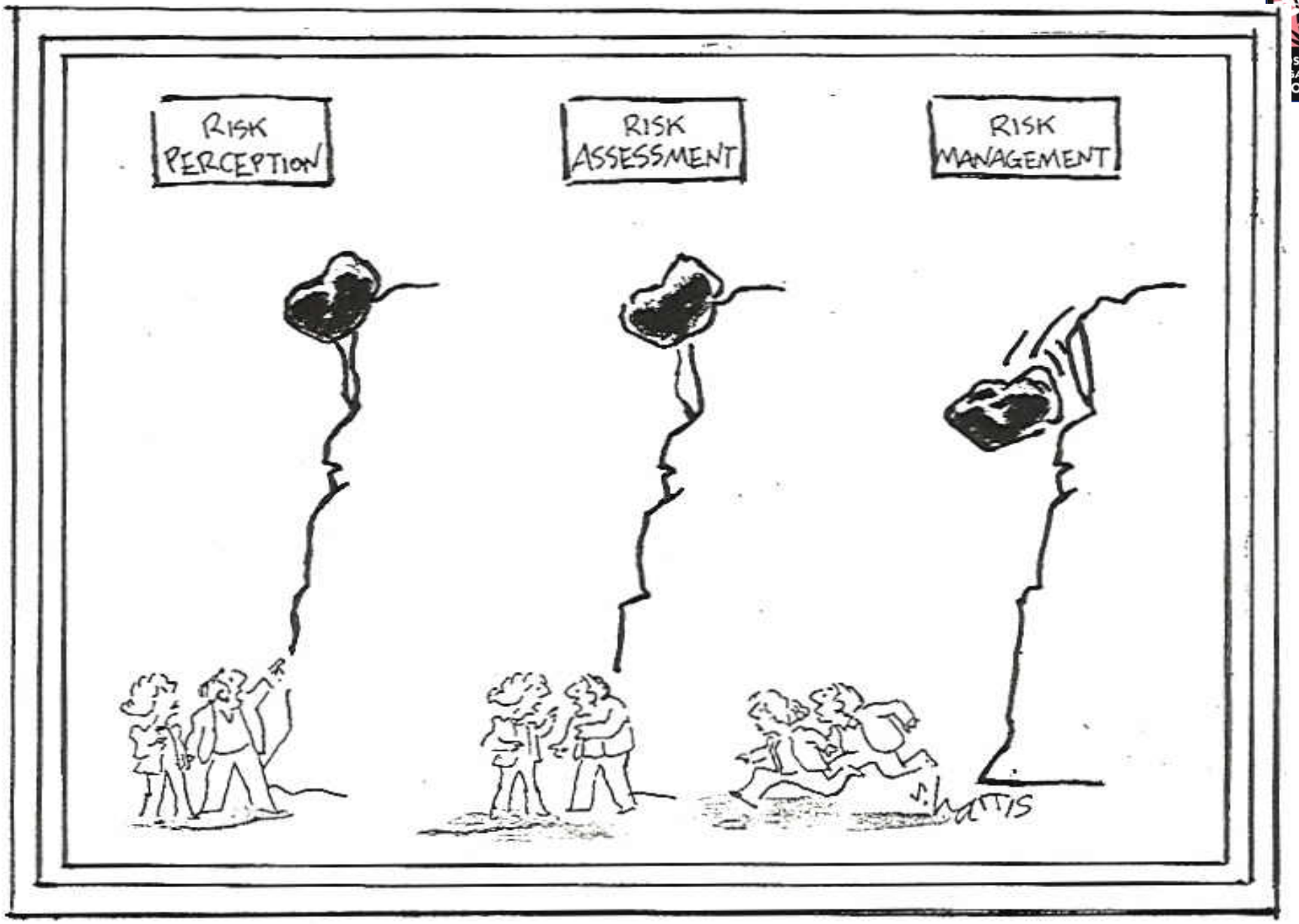
- Laboratory work with pathogens will always involve some level of safety and security risk
- Most biological materials occur in nature and can be isolated from nature
- Critical not to compromise legitimate bioscience operations
  - Systems should be designed to address unique situations
- Resources are not infinite; existing resources should be used efficiently
- Management must distinguish between "acceptable" and "unacceptable" risks
  - Ensure that protection and the cost is proportional to the risk



- Protect against unacceptable risk scenarios

- Develop incident response plans for acceptable risk scenarios

11



12

Risk Perception in Laboratories

Biosafety risks: laboratory-acquired infections

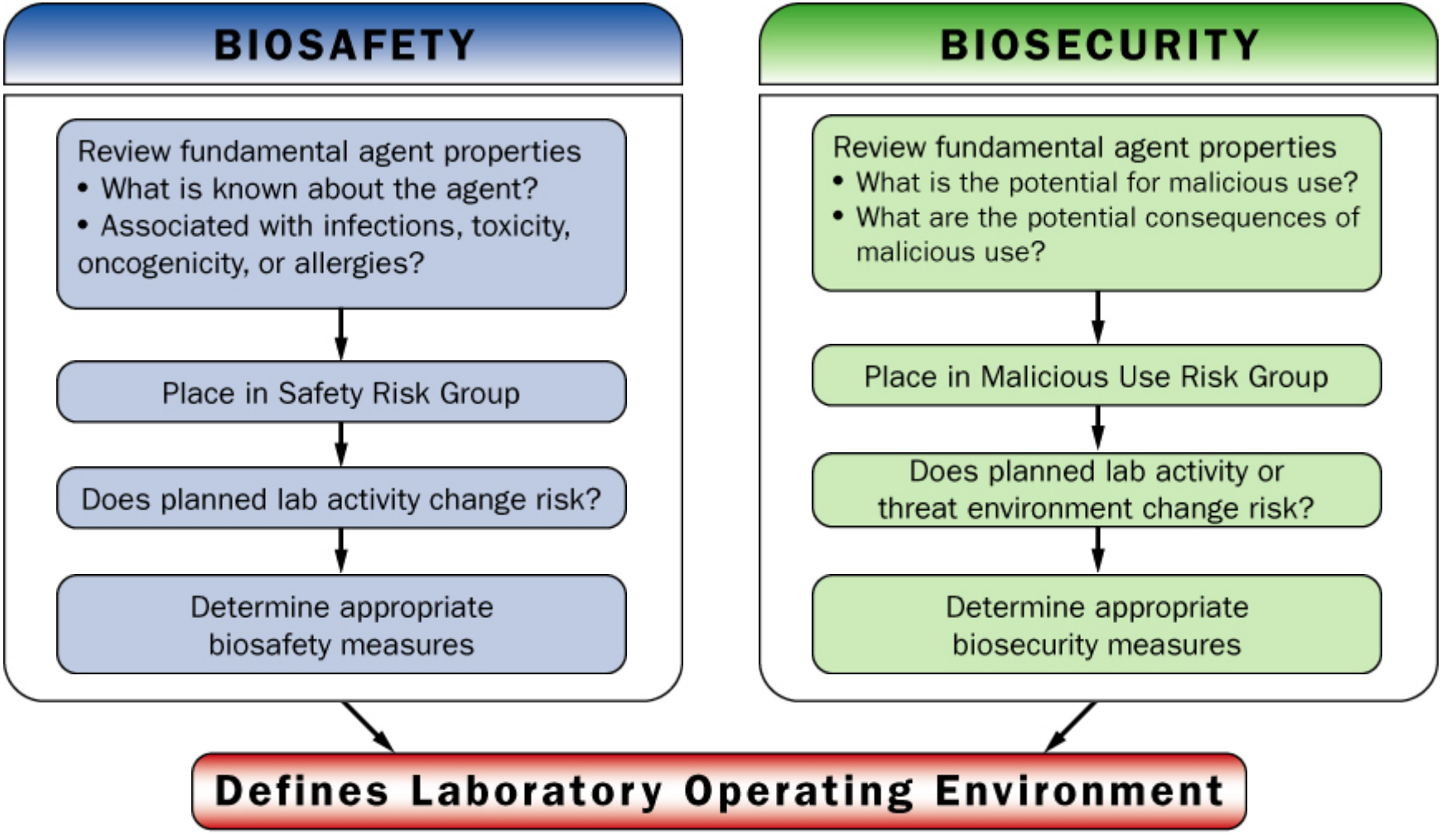
- History of lab-acquired infections
  - Often attributed to carelessness or poor technique
  - Relatively few cases can be attributed to direct accident (mouth pipetting and sharps injuries)
  - Exposure to airborne pathogens generally presumed to be most plausible cause
  - Brucellosis is most common
- Sporadic infections in community as a result
  - 1973 and 1978—England had 3 secondary cases of smallpox
  - 1950—2 cases of Q fever in household of scientist
  - 1990—1 documented case of Monkey B virus from animal handler to wife
  - SARS—including 3 generations (9 cases)

Biosecurity risks: laboratories as sources of material for malicious use

- Bioterrorism has emerged as a threat to international security
  - 1984 Rajneeshee religious cult attacks
  - 1990s Aum Shinrikyo attempts
  - 2001 Anthrax attacks in the US
- Examples of illicit acquisition
  - 1990s—Aum Shinrikyo ordered *Clostridium botulinum* from a pharmaceutical company
  - 1995—Larry Wayne Harris, a white-supremacist, ordered 3 vials of *Yersinia pestis* from the ATCC
  - 1995—Laboratory technician Diane Thompson removed *Shigella dysenteriae* Type 2 from hospital's collection and infected co-workers

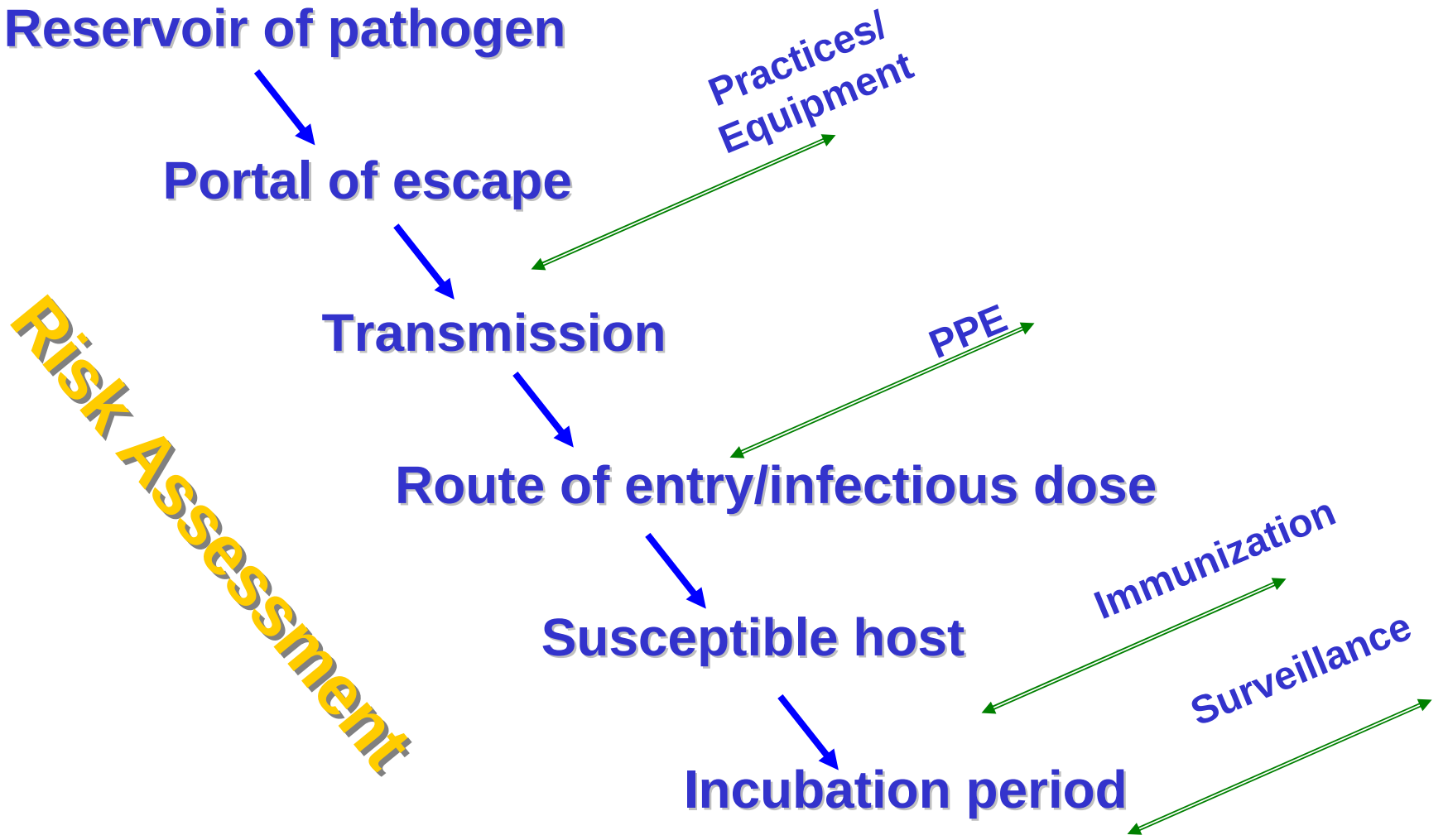
13

Risk Assessment: Integrated Biosafety and Biosecurity



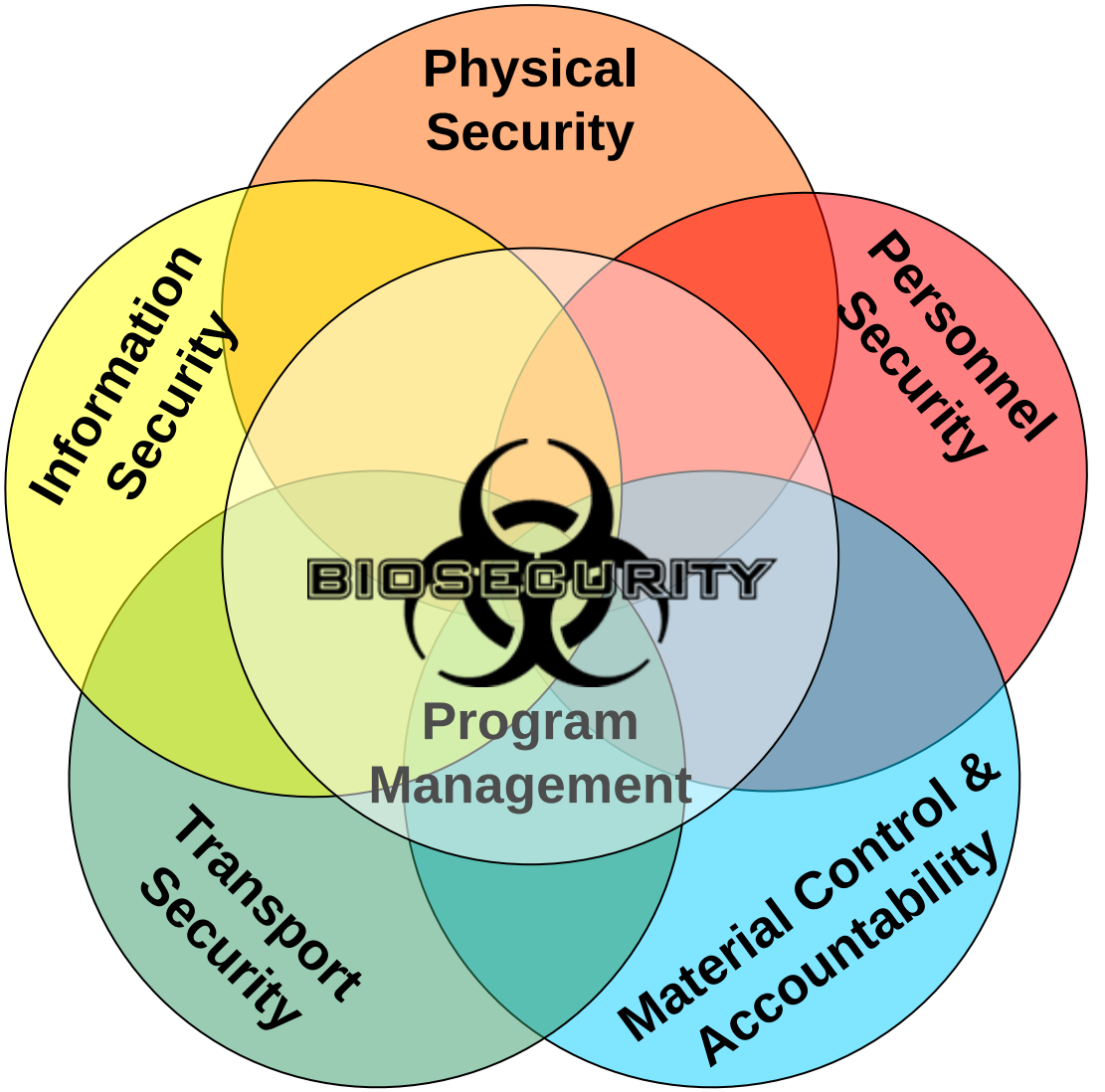
14

Risk Management: Implementation of Biosafety



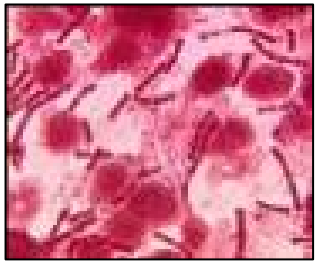
15

Risk Management: Implementation of Biosecurity



16

Biosecurity Risk Assessment



1. Evaluate assets (agent assessment)
2. Evaluate lab activity
3. Evaluate threat environment

17

Biosecurity Risk Assessment: Malicious Use Risk Group Evaluation

- **Assess value of the agents from an adversary's perspective**
  - **Consequences**
    - **Population**
      - Transmissibility
      - Mortality
      - Morbidity
    - **Economic**
    - **Psychological**
  - **Weaponization potential**
    - **Acquisition**
      - Natural
      - Laboratory
      - Synthetic biology
    - **Production**
      - R&D
      - Covert production
      - Ease of storage
    - **Dissemination**
      - Route of infection (e.g. aerosol, ingestion)
      - Environmental hardiness

REPORTS

Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template

Jeronimo Cello, Aniko V. Paul, Eckard Wimmer*

9 AUGUST 2002 VOL 297 SCIENCE www.sciencemag.org

JOURNAL OF VIROLOGY, Feb. 2001, p. 1205–1210 Vol. 75, No. 3
0022-538X/01/$04.00+0 DOI: 10.1128/JVI.75.3.1205–1210.2001
Copyright © 2001, American Society for Microbiology. All Rights Reserved.

Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox

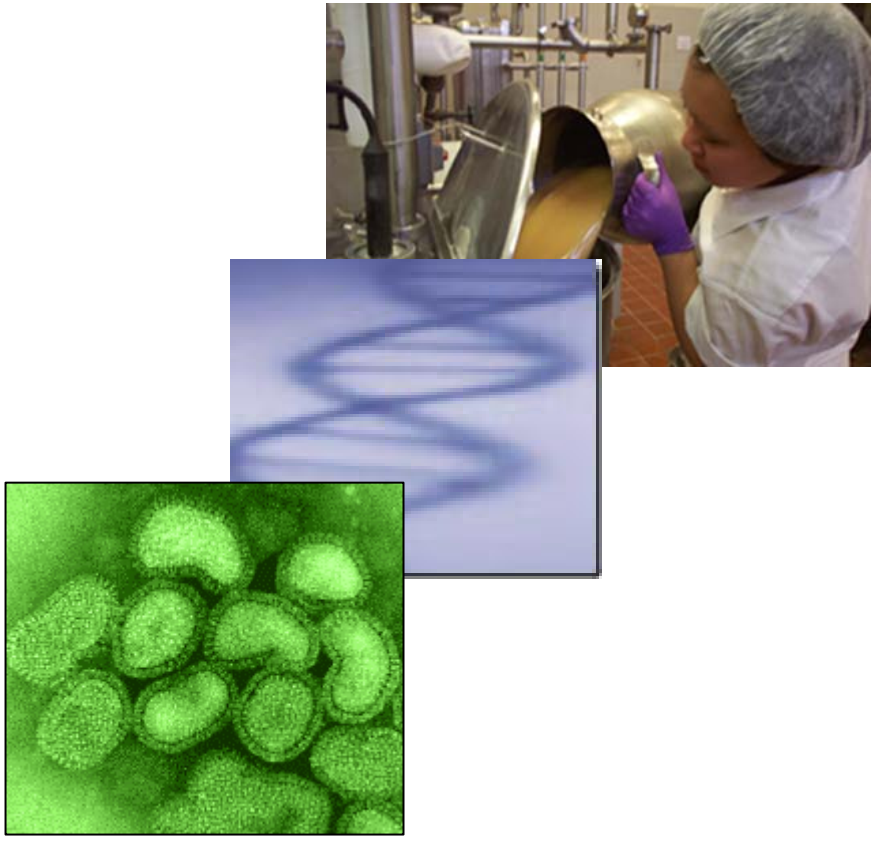
RONALD J. JACKSON,[1,2]* ALISTAIR J. RAMSAY,[2]† CARENA D. CHRISTENSEN,[2] SANDRA BEATON,[1] DIANA F. HALL,[1]‡ AND IAN A. RAMSHAW[2]

Pest Animal Control Cooperative Research Centre, CSIRO Sustainable Ecosystems,[1] and Division of Immunology and Cell Biology, John Curtin School of Medical Research, Australian National University,[2] Canberra, Australia

18

Biosecurity Risk Assessment: Elements That May Modify Risk

- **Consider lab experiments**
  - **Does planned experiment produce an agent with higher weaponization potential or higher potential consequences?**
    - **Increased stability**
    - **GMOs**
    - **Large quantities**
    - **Aerosol challenges**



19

Biosecurity Risk Assessment: Elements That May Modify Risk

- Adversary Classes
  - Terrorist
  - Extremist
  - Criminal
- Insiders
  - Authorized access to the facility, dangerous pathogens, and/or restricted information
  - Distinguish Insiders by level of authorized access
    - Site
    - Building
    - Asset
  - Facility management, site security, and local law enforcement interviews
- Outsiders
  - No authorized access
  - Local law enforcement, site security, and intelligence community interviews

20

Biosecurity Risk Assessment: Malicious Use Risk Groups

- **Nonpathogenic**
  - Malicious use would have insignificant or no consequences
- **Low**
  - Difficult to deploy, and/or
  - Malicious use would have few consequences
- **Moderate**
  - Relatively difficult to deploy, and
  - Malicious use would have localized consequences with low to moderate casualties and/or economic damage, and potentially cause pervasive anxiety
- **High**
  - Not particularly difficult to deploy, and
  - Malicious use could have national or international consequences, causing moderate to high casualties and/or economic damage, and the potential to cause mass panic and significant social disruption
- **Extreme**
  - Would normally be classified as highly attractive, except that they are not found in nature (eradicated)
  - Could include genetically engineered agents, if they would otherwise be classified as highly attractive

21

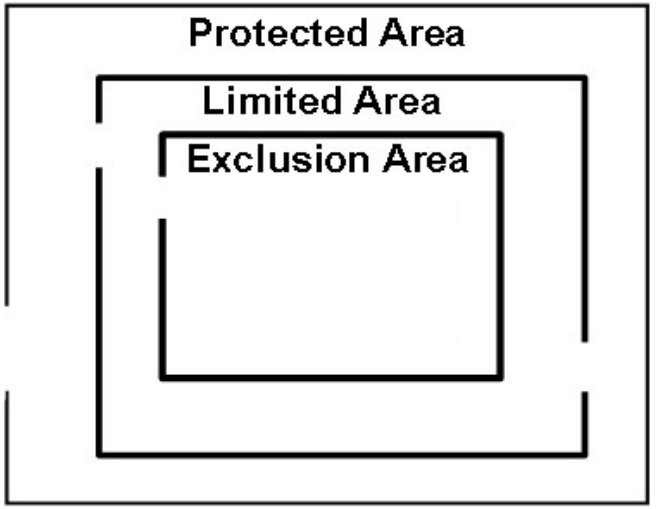
Laboratory Biosecurity System

- Biosecurity system components
  - Physical security
  - Personnel security
  - Material handling and control measures
  - Transport security
  - Information security
  - Program management practices
- Each component implemented based on results of risk assessment
- In general, biosecurity for
  - Moderate risk focuses on the insider
  - High risk focuses on both the insider and the outsider

22

Physical Security: Concentric Layers of Security

- **Property Protection Areas**
  - **Low risk assets**
    - **Grounds**
    - **Public access offices**
    - **Warehouses**



- **Limited Areas**
  - **Moderate risk assets**
    - **Laboratories**
    - **Sensitive or administration offices**
    - **Hallways surrounding Exclusion Areas**

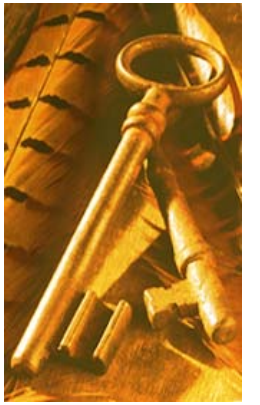
- **Exclusion Areas**
  - **High risk assets**
    - **High containment laboratories**
    - **Computer network hubs**

23

Physical Security: Access Controls

- Access control ensures that only authorized individuals are allowed into certain areas
  - Increasingly strict controls as you move toward higher risk assets
- Property Protection Areas: Fences
  - Mark the boundaries of your property
  - Announce your intention to protect the property
  - Elicit strong statement of intent from intruder
  - Terrain features can also serve this purpose
- Limited Areas
  - Unique item
  - Controlled possession
  - Electronic or physical key
- Exclusion Areas
  - Unique item
  - Unique knowledge
  - Controlled possession
  - Electronic key card <u>and</u> keypad or biometric device

  or
  - Controlled key <u>and</u> second individual to verify identity



24

Physical Security: Intrusion Detection and Response

- Intrusion Detection
  - Guards
  - Electronic sensors
- Alarm Assessment
  - Validation of violation before response
  - Can be direct (guards) or remote (video)
- Response
  - On-Site Guard Force
    - Supports electronic systems
    - Patrols or guards perimeter and buildings
    - Summons and directs local law enforcement
  - Local law enforcement (police) support
    - Reinforces or substitutes for on-site guard force
    - Memorandum of understanding

25

Personnel Security: Screening

- Conduct screening for authorized individuals
  - Degree of scrutiny commensurate with level of risk associated with the position
    - Need for unescorted access to restricted areas
    - Types of assets held in the restricted areas
    - Level of authority in association with high risk materials

- Mechanisms
  - Verify credentials
  - Check references
  - Criminal history
  - In-depth background investigation

26

Personnel Security: Badges

- **Badges should be issued to those individuals authorized to be in restricted areas**

- **Badge return**
  - **Upon employee termination**
  - **Daily or at the conclusion of a limited term for visitors**

- **Report lost or stolen badges**

27

Personnel Security: In-Processing and Out-Processing

- **In-Processing**
  - **Complete all required forms, safety training, security training and immunizations as applicable for work environment**

- **Out-Processing**
  - **Retrieve keys**
  - **Access changes or termination**
  - **Retrieve property**
  - **Deactivate computer and electronic access accounts**

28

Personnel Security: Visitor Controls

- **Types**
  - **Personal Visitors**
    - **Family members**
  - **Casual Visitors**
    - **Tours, seminars**
    - **Equipment repair technicians**
  - **Working Visitors**
    - **Visiting researchers**
    - **Facility maintenance personnel**

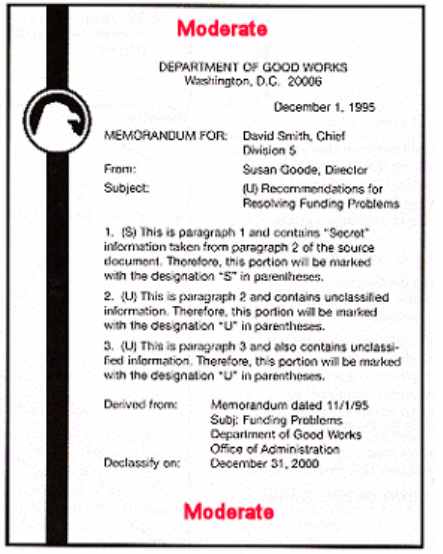
- **Controls**
  - **All visitors should have a host at the facility**
  - **Visitors should be escorted in restricted areas**

29

Information Security

- **Protect information that is too sensitive for public distribution**
  - **Label information as restricted**
  - **Limit distribution**
  - **A review and approval process aids in the identification of sensitivities**
  - **Restrict methods of communication**
  - **Implement network and desktop security**

- **Biosecurity-related sensitive information**
  - **Security of dangerous pathogens and toxins**
    - **Risk assessments**
    - **Security system design**
  - **Access authorizations**



Moderate

DEPARTMENT OF GOOD WORKS
Washington, D.C. 20006

December 1, 1995

MEMORANDUM FOR: David Smith, Chief
Division 5

From: Susan Goode, Director

Subject: (U) Recommendations for Resolving Funding Problems

1. (S) This is paragraph 1 and contains "Secret" information taken from paragraph 2 of the source document. Therefore, this portion will be marked with the designation "S" in parentheses.

2. (U) This is paragraph 2 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

3. (U) This is paragraph 3 and also contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

Derived from: Memorandum dated 11/1/95
Subj: Funding Problems
Department of Good Works
Office of Administration

Declassify on: December 31, 2000

Moderate

30

Information Security: Communication and Network Security

- **Communication Security**
  - **Mail, email, or fax security is required**
  - **Limited discussions in open areas**
  - **Information should only be reproduced when needed and each copy must be controlled as the original**

- **Network Security**
  - **Firewalls**
  - **User authentication**
  - **Virus protection**
  - **Layered network access**
  - **Desktop security**
  - **Remote and wireless access controls**
    - **Encryption**
    - **Authentication**

31

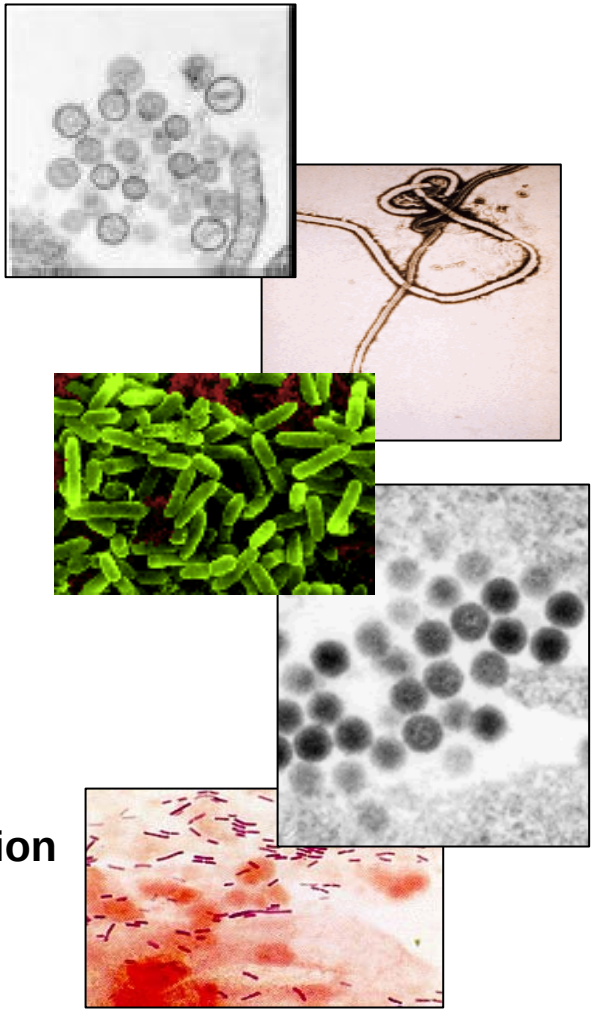
Material Control & Accountability: Objectives

- Ensure the complete and timely knowledge of:
  - What materials exist
  - Where the materials are located
  - Who is accountable for them
- Operating procedures associated with the materials
  - Location of storage and use
  - Identification
  - Inventory
- Documentation and reporting requirements
- Purpose is NOT to detect whether something is missing

32

Material Control and Accountability

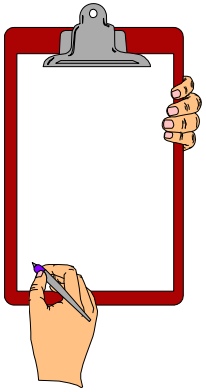
- Agent
  - What agents are high risk?
  - Viable? Whole organism or DNA?
- Quantity
  - Any amount can be significant
  - A threshold amount for toxins
- Form
  - Repository stocks, working samples, in host, contamination
- Detail—what level is adequate for MC&A?
  - Material as *items*
  - Each vial as a separate inventory record?
- When does MC&A start & stop?
  - Naturally occurring; clinical samples; disposition



33

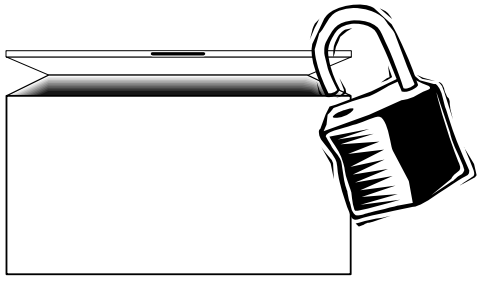
Material Control and Accountability

- **Control is either…**
  - **Engineered / Physical**
  - **Administrative**



- **Containment is part of material control**
  - **Containment Lab / Freezer / Ampoule**

- **Procedures are essential for material control**
  - **For both normal and abnormal conditions**



34

Material Control and Accountability

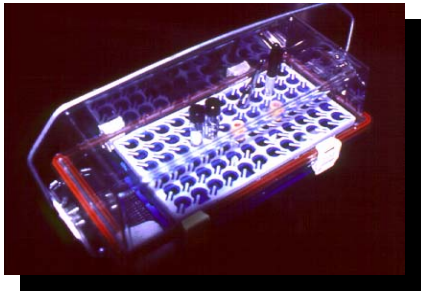
- **All material should have an associated "accountable person"**
  - **The person best in a position to answer questions about the associated material**
  - **Not someone to blame!**
  - **Ensure that no material is "orphaned"**

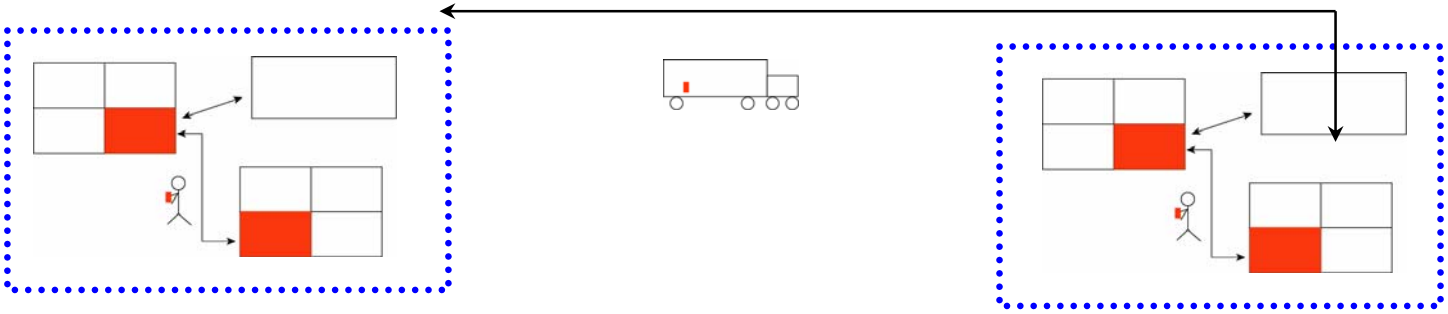
- **Procedures should ensure accountability**
  - **Experimental work: laboratory procedures**
  - **Inventory: know what you have**
  - **Reporting: document routine MC&A practices**
  - **Audit/ assessment: is this working?**
    - Ensures effective *implementation* of MC&A
  - **Training: personnel understand requirements**

35

Transport Security: Internal Transport

- Movement of materials to and from restricted areas within a facility
- May involve personnel from
  - Labs
  - Shipping areas
  - Receiving areas
  - Disposal areas (e.g. autoclave and incinerator rooms)
- Move materials safely and securely
  - Standard Operating Procedures
  - Leak-proof containers
  - Pre-approval?
  - Tracking?

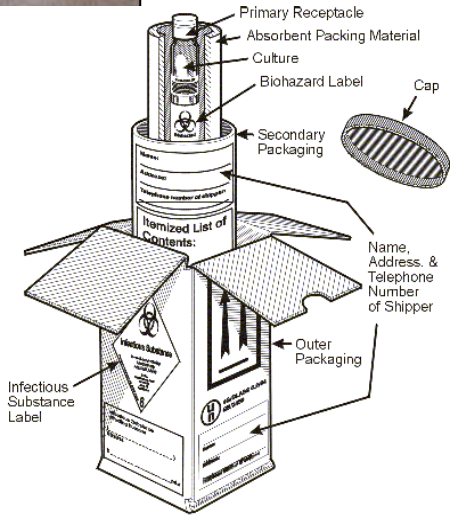




36

Transport Security: External Transport

- Movement of materials from one facility to another facility
- May involve commercial carriers
- Occur within a wide array of international and state regulations and standards
- Must be able to move frozen materials efficiently
- Need to be cost-effective
- International transport of infectious materials is regulated



37

Transport Security: Facility Responsibilities

- **Personnel security**
  - **For people who have access to dangerous pathogens and toxins or information during transfers**
- **Establish chain of custody (tracking)**
  - **Record all individuals who have contact with the dangerous pathogens and toxins**
- **Provide physical security**
  - **For packages that need temporary storage**
- **Protect transport documentation**
- **Determine who is able to authorize, transport, and receive dangerous pathogens and toxins**

38

Carrier Security

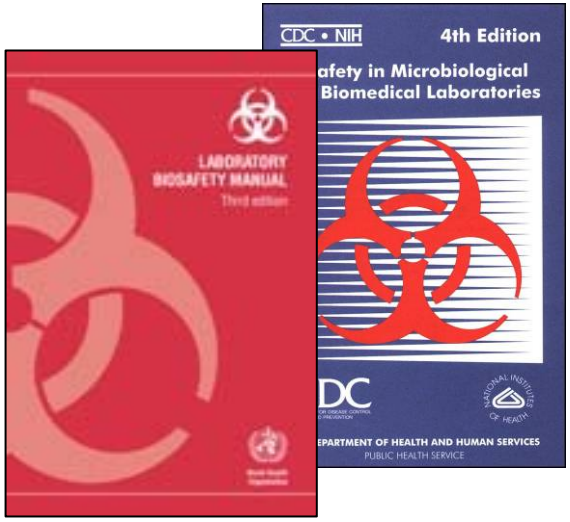
- Carriers should provide security by
  - Ensuring reliable and trustworthy people handle the package
  - Controlling access to transport facilities, docks, and vehicles
  - Tracking shipping progress
  - Providing ongoing security training for employees

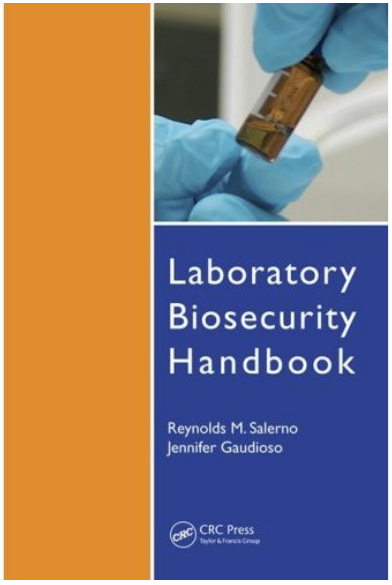
39

Laboratory Biosecurity Supports Laboratory Biosafety

- Laboratory biosecurity supports the laboratory biosafety agenda of preventing disease in people, animals, and plants and minimizing the risk of worker injury

- Safe and secure laboratories help
  - Ensure the containment of hazardous infectious substances in laboratories
  - Maintain citizens' confidence in the activities of the bioscience research community
  - Increase transparency to investors in the biomedical and biotechnology industries
  - Protect valuable research and commercial assets
  - Reduce the risks of crime and bioterrorism





40

Similar Physical Aspects of Biosafety and Biosecurity

Biosafety

- Physical protection
  - Increasing levels of physical containment to prevent the accidental release of dangerous biological agents
    - BSL-1
    - BSL-2
    - BSL-3
    - BSL-4
  - Examples: negative air pressure, cabinets and hoods

Biosecurity

- Physical protection
  - Graded protection designed to secure dangerous biological agents from adversaries
    - Property Protection Area
    - Limited Area
    - Exclusion Area
  - Examples: access controls, intrusion detection

41

Similar Procedural Aspects of Biosafety and Biosecurity

Biosafety

- Material control and accountability
  - Handling procedures to prevent accidental infection
  - Use of personal protective equipment
- Personnel reliability
  - Background checks to ensure proper credentials to handle dangerous organisms
  - Policies to prevent untrained individuals from working with materials that pose a biosafety risk

Biosecurity

- Material control and accountability
  - Basic inventory procedures to limit opportunities for illicit acquisition
  - Designation of laboratory workers responsible for specific material
- Personnel reliability
  - Background checks to ensure personnel are reliable and trustworthy
  - Procedures to remove unauthorized personnel from secure areas

42

Similar Procedural Aspects of Biosafety and Biosecurity, cont.

Biosafety

- **Transport**
  - **Requirements to ensure the safe transport of materials within a lab**
  - **Federal and international regulations governing the transport of infectious substances outside the lab**

Biosecurity

- **Transport**
  - **Best practices to ensure the secure transport of materials both inter-facility and intra-facility**
  - **Chain of custody where appropriate**

Biosafety and Biosecurity share a variety of components

43

Potential Conflicts between Biosafety and Biosecurity

- Emergency alarm – electronic locks
  - Safety – doors fail open
  - Security – doors fail secure
- Emergency egress
  - Safety – move people into the safest location as quickly as possible
  - Security – prevent people from moving into or through restricted areas
- Emergency response
  - Safety – provide emergency responders with locations of hazards and responsible individuals
  - Security – control distribution of sensitive information only to those with a need to know
- Signage
  - Safety – identify hazardous substances and responsible parties
  - Security – avoid identification of target materials or individuals with access
- Keys required inside laboratory areas
  - Safety – contamination concern
  - Security – multiple layers of access

44

Thank You!

Reynolds M. Salerno, Ph.D., Manager
International Biological Threat Reduction
Sandia National Laboratories
PO Box 5800, MS 1371
Albuquerque, NM 87185 USA
Tel. 505-844-8971
Fax. 505-284-8870
Cell. 505-440-6387
Email. rmsaler@sandia.gov
www.biosecurity.sandia.gov

45