BIOSECURITY IN THE LABORATORY

Maureen Sullivan
Biosecurity

• Why is biosecurity important
• History of biosecurity field
• Definitions
• Laboratory Biosafety verses Biosecurity
• Principles and Practice
  – Concepts of Biosecurity
  – Biosecurity Risk Assessment
• Regulatory issues with Select Agent Program
• Clinical laboratory security issues
• Developing a Biosecurity Plan
Why is Biosecurity Important?

• 2001 Anthrax attacks
  – 5 deaths/17 ill
  – Worst biological attacks in US History
  – FBI names suspect
    • Anthrax researcher at USAMRIID
Why is Biosecurity Important?

- Biological attack in Oregon
  - *Salmonella typhimurium* sprayed on 8 salad bars in attempt to influence a local election
  - 751 citizens affected
  - Originally looked like a normal naturally occurring outbreak
  - Over a year later the outbreak was linked to the Rajneesh Foundation
  - Two members of Rajneesh were convicted (one is nurse with access to Salmonella)
Why is Biosecurity Important?

How well do you know your co-workers?

- *Shigella dysenteriae* type 2 among laboratory workers
  - Disgruntled laboratory technician spikes donuts with *Shigella dysenteriae* type 2
  - Email sent out to lab staff to come enjoy the donuts
  - 12 people become ill
  - Laboratorian is convicted and gets 20 years in prison
Biosecurity Incident List

By Dr Ananya Mandal, MD

- In 1966, Dr. Mario Jascalevich from New Jersey was accused of poisoning five patients with a plant-derived poison called tubocurarine.
- Between 1964 and 1966, a Japanese doctor called Mitsuru Suzuki contaminated sponge cakes and other sources of food with shigella dysenteriae (causes diarrhea) and salmonella typhi (causes typhoid), leading to 200 to 400 illnesses and four deaths.
- Between May 1977 and November 1980, a nursing home worker called Arnfinn Nesset killed 27 residents using a substance called curacit.
- In 1984, religious cult members held attacks in Dalles, Oregon using salmonella typhimurium in an attempt to affect the election and gain control of the Wasco County Court. The restaurant salad bars were used as the dissemination points and the attack led to 751 illnesses. A cult member was arrested on an unrelated charge and confessed later to being involved in the event.
- In the 1990s, Aum Shinrikyo tried to disseminate bacillus anthracis (anthrax - the vaccine strain), Clostridium botulinum and the Ebola virus in Tokyo, Japan to fulfil the apocalyptic prophecy.
- In 1995, Larry Wayne Harris ordered 3 vials of Yersinia pestis (causing plague) from the ATCC and in the same year laboratory technician Diane Thompson took Shigella dysenteriae Type 2 from a hospital and infected her co-workers.
- In 1995, a neurologist in Virginia called Dr. Ray W. Mettetal was found with ricin on his person after being arrested for something else.
- In 1998, a gastroenterologist in Louisiana called Richard Schmidt infected nurse Janice Allen with HIV by injecting her with blood from a patient who had AIDS.
- In 1999, a phlebotomist called Brian T. Stewart was sentenced to life imprisonment for deliberately infecting his baby with HIV-infected blood to avoid the cost of child support.
- In 2001, there were a series of anthrax attacks in the United States.
- In 2003, Professor Thomas Butler was arrested for removing 30 vials of Yersinia pestis from a laboratory.

Reviewed by Sally Robertson, BSc

Sources
1. www.who.int/foodsafety/fs_management/No_01_Biosecurity_Mar10_en.pdf
3. www.americanprogress.org/.../CURITY_A_COMPREHENSIVE_ACTION_PLAN.pdf
5. www.forestry.gov.uk/.../FC_Biosecurity_Guidance.pdf
History of Biosecurity

• First described in the agricultural and environmental industries
  – Biosecurity is the protection of agricultural animals from any type of infectious agent—viral, bacterial, fungal, or parasitic. People can spread diseases as they move within a facility and from one to another.
Laboratory Biosafety vs Biosecurity

- **Biosafety**: development and implementation of administrative policies, work practices, facility design, and safety equipment to prevent transmission of biological 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.
Laboratory Biosafety vs Biosecurity

**Biosafety**
- Reduce or eliminate exposure
- Laboratory design and access restrictions
- Personnel expertise and training
- Containment equipment
- Safe methods of managing infectious materials

**Biosecurity**
- Prevent loss, theft, misuse of microorganisms, biological materials and research related information
- Limit access to facilities, research materials and information

Goals of Biosafety and Biosecurity

• Biosafety goal: Protect people from dangerous pathogens.

• Biosecurity goal: Protect pathogens from dangerous people.
Biosecurity AND Biosafety

**Biosafety**
- Risk Assessment
  - Exposures
  - Aerosol production
  - Facility issues
  - Lack of training
  - Improper PPE use
  - Poor management practices

**Biosecurity**
- Threat Assessment
  - Crimes
  - Insiders
  - Outsiders
  - Natural hazards

**Risks**
- Dangerous pathogen, toxin or valuable biological material

**Vulnerability Assessment**
Common components of Biosafety and Biosecurity

• Good laboratory practices
• Risk assessment
• Management oversight
• Personnel qualifications
• Control and accountability of organisms
  – Inventory management
• Access control
• Training
• Emergency Planning
  (some conflicts also exist)
Conflicts Between Biosafety and Biosecurity

Emergency Response
- Rapid egress of staff
- Rapid ingress of first responders
- Ensure security of assets

Signage
- Warns of safety concerns
- Don’t divulge too much information
Concepts of Biosecurity

- Risk and threat assessment
- Facility security planning (access)
- Physical security
- Data and IT security
- Personnel security
- Specimen accountability
- Specimen receipt and transfer
- Emergency response plans
- Training
- Reporting
Elements of a Biosecurity Program

- Program management
- Physical security-access control and monitoring
- Personnel management
- Inventory and accountability
- Information security
- Transport of biological agents
- Response plans
- Reporting and communication
- Training and drills
- Security updates and re-evaluations
- Select agents
Developing a Biosecurity Program

• Collaborative process involving all stakeholders
  – Senior management (Lab director)
  – Scientific staff
  – Human Resources
  – IT staff
  – Safety officer
  – Security staff
  – Building engineering staff
What Are Some Barriers or Challenges?

- Lack of resources
- Lack of management support
- Resistance to change
- Inadequate training
- Insufficient information
- Not a personal value
Risk Assessment

• Systematic evaluation of the probability and consequences of a loss, theft or potential misuse of pathogens or toxins
  – How likely is it that a bad thing will happen?
  – If a bad thing happens, what are the consequences?

• **Goal** is to determine what you want the security system to prevent.
Biosecurity Risk Assessment and Management Process

1. Identify and prioritize biological materials
2. Identify and prioritize threat to biological materials
3. Analyze the risk of specific Security Scenarios
4. Develop an overall Risk Management Program
5. Re-evaluate the institution’s risk posture and protection objectives
Biosecurity Risk Assessment and Management Process

1. Identify and prioritize biological materials
2. Identify and prioritize threat to biological materials (assess potential threats and vulnerabilities)
3. Analyze the risk of specific Security Scenarios
4. Develop an overall Risk Management Program
5. Re-evaluate the institution’s risk posture and protection objectives
Identify and Prioritize Biological Materials: Inventory

• Identify and prioritize biological materials
  – Determine what you have in your inventory
    • May need to conduct a comprehensive inventory (MDH has over 250 thousand samples in inventory)
    • What is it, where is it stored, how much
  – Evaluate the potential for misuse of the materials
  – Determine what happens if materials are misused
Why did we do this?

• We have a very large collection, little documentation
• We are running out of freezer space
• First step in creating a specimen retention schedule to manage their collection
• Legislative requirement to know how many human specimens we have
Objectives

1. Create Plan for executing an inventory
2. Execute inventory

Deliverable

• A documented, usable, inventory of the entire specimen and isolate collection @ IDL.
How did we do this?

- Project Management Approach
- Excellent Team
- Leadership buy-in
Project Team

Planning:
- What to be inventoried
- What information to be captured
- Standardized freezer rack numbering
- Spreadsheets

Execution:
- Expectations
- Process for spreadsheets
Freezer names

- Gave “meaning” to a specific freeze
- Team Building exercise
### Execution

- **32 freezer spaces**
- **Freezer Expert**

<table>
<thead>
<tr>
<th>Slot/Box</th>
<th>Row</th>
<th>Column</th>
<th>Acc. Series</th>
<th>Accession #</th>
<th>Stock #</th>
<th>XMN #</th>
<th>S/E (R) Proj</th>
<th>Year</th>
<th>Storage Vessel</th>
<th>Comment/Description</th>
<th>Why? (R)</th>
<th>Disposal Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1 A</td>
<td>1 C</td>
<td>2003002549</td>
<td>Isolate</td>
<td>2003</td>
<td>2ml</td>
<td>MRSA</td>
<td>IDK/Because we always have</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1 A</td>
<td>2 C</td>
<td>2003002550</td>
<td>Isolate</td>
<td>2003</td>
<td>2ml</td>
<td>MRSA</td>
<td>IDK/Because we always have</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1 A</td>
<td>3 C</td>
<td>2003002551</td>
<td>Isolate</td>
<td>2003</td>
<td>2ml</td>
<td>B. PERTUSSIS</td>
<td>IDK/Because we always have</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1 A</td>
<td>4 C</td>
<td>2003002552</td>
<td>Isolate</td>
<td>2003</td>
<td>2ml</td>
<td>B. PERTUSSIS</td>
<td>IDK/Because we always have</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1 A</td>
<td>5 C</td>
<td>2003002553</td>
<td>Isolate</td>
<td>2003</td>
<td>2ml</td>
<td>SP</td>
<td>IDK/Because we always have</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1 A</td>
<td>6 C</td>
<td>2003002554</td>
<td>Isolate</td>
<td>2003</td>
<td>2ml</td>
<td>B. PERTUSSIS</td>
<td>IDK/Because we always have</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>1 A</td>
<td>7 C</td>
<td>2003002555</td>
<td>Isolate</td>
<td>2003</td>
<td>2ml</td>
<td>B. PERTUSSIS</td>
<td>IDK/Because we always have</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>1 A</td>
<td>8 C</td>
<td>2003002556</td>
<td>Isolate</td>
<td>2003</td>
<td>2ml</td>
<td>GBS</td>
<td>IDK/Because we always have</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>1 A</td>
<td>9 C</td>
<td>2003002559</td>
<td>Isolate</td>
<td>2003</td>
<td>2ml</td>
<td>MRSA</td>
<td>IDK/Because we always have</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>1 B</td>
<td>1 C</td>
<td>2003002560</td>
<td>Isolate</td>
<td>2003</td>
<td>2ml</td>
<td>MSSA</td>
<td>IDK/Because we always have</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>1 B</td>
<td>2 C</td>
<td>2003002561</td>
<td>Isolate</td>
<td>2003</td>
<td>2ml</td>
<td>SP</td>
<td>IDK/Because we always have</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>1 B</td>
<td>3 C</td>
<td>2003002562</td>
<td>Isolate</td>
<td>2003</td>
<td>2ml</td>
<td>SP</td>
<td>IDK/Because we always have</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>1 B</td>
<td>4 C</td>
<td>2003002563</td>
<td>Isolate</td>
<td>2003</td>
<td>2ml</td>
<td>MRSA</td>
<td>IDK/Because we always have</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>1 B</td>
<td>5 C</td>
<td>2003002564</td>
<td>Isolate</td>
<td>2003</td>
<td>2ml</td>
<td>MRSA</td>
<td>IDK/Because we always have</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Action plan
Team Work!

Teams decided:
- Team name
- Roles for everyone on the team
- Goal finish date
- How they were going to reach the goal
Motivation and Success

- Raffle
- Motivating e-mails and speeches
- Snack time
- Ice box detox
- Where possible, all groups have switched to barcoded labels for storage
- Excel training
- Saves time in finding isolates
The Taming of Wile E. Coyote: Before
The Taming of Wile E. Coyote: After

- 2754 stools aliquoted into 34 boxes
- All tubes are in numerical order
- Oldest stool: early 1993
The Numbers
IDL Inventory

- Isolate: 162,114
- Specimen: 58,594
- Extract: 33,830
- Glycerol Sweep: 19,958
- Other: 284

7% 12% 22% 59%
Why Are We Keeping It?

- Trend analysis
- Rare/Unique
- PT/Control Strain
- Epi Request
- Lab Research
- CDC Surveillance

0 20000 40000 60000 80000 100000
What’s next?

✓ Maintenance plan
  o Specimen retention schedule
  o Adjust specimen/isolate collection to the schedule
Potential Threats and Vulnerabilities

- Determine how undesired events might occur. What types of “insiders” pose a threat?
- Determine how unauthorized access might occur. What types of “outsiders” pose a threat?
- What are the motives, means, and opportunities of these potential threats?
- Identify protective measures in place and how they might be breached.
Definitions: Threats and Vulnerability

• Threat: someone with the intent to cause trouble, harm, etc; an expression of intention to inflict evil, injury, or damage.”

• Vulnerability: “…an opening or point of attack or damage.”
# People Threats

<table>
<thead>
<tr>
<th>Insider</th>
<th>Outsider</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Risk</td>
<td>Low Risk</td>
</tr>
<tr>
<td>Unescorted access</td>
<td>Public access to information</td>
</tr>
<tr>
<td>Non-violent</td>
<td>May be armed</td>
</tr>
<tr>
<td>Knowledge of facility</td>
<td>May carry tools</td>
</tr>
<tr>
<td>Opportunity</td>
<td>Strategy:</td>
</tr>
<tr>
<td>Strategy:</td>
<td>Detect &amp; Contain</td>
</tr>
<tr>
<td>Know employees</td>
<td></td>
</tr>
</tbody>
</table>

Insider (Internal) Threats

• Employee making direct threats
  – Workplace violence
  – Internal sabotage of research
• Employee involved in threatening behaviors or subversive activities
• Internal animosity (love triangles, bad relationships between authority lines)
Incompetence as a Hazard

- Maybe the most common form of “Insider Threat”
- Not malicious
- Complacency, laziness, indifference
- Lack of fundamental education (understanding of microbiology)
- Lack of training
Outsider (External) Threats

• Direct threats against employees: personal connection or terrorist-related
• Direct threats against employer or supervisor
• Direct threats against research or institute
Indirect Threats

• “Wrong place, wrong time”
• Inadvertent release of information
• Elicitation of information on manipulation by third parties
Environmental Threats

- Hurricane
- Tornado
- Flood
- Blizzard
- Fire
- Earthquake
- (Power /Outage or Shortage)

NOTE: Select Agent program wants you to address all of these individually!
The Incident, January 6, 2014

- Overnight temperature drops to -24° F
- Laboratory air handlers and heat wheels go down allowing cold air into the system
- Air handlers restarted in a.m. and building warms up
- Frozen heating system coils thaw and burst
  - Multiple (20) additional heating coil leaks throughout the day
  - Fire sprinkler in clean metals lab
Quick to Action
Analyze the Risk of Specific Security Scenarios

- Evaluate the likelihood of each risk scenario materializing and its associated consequences
- Protect against unacceptable risk scenarios (Prioritize)
- Develop incident response plans for acceptable risk scenarios

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>More Likely</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Moderate</td>
</tr>
<tr>
<td></td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Highest</td>
</tr>
<tr>
<td>Less Likely</td>
<td>Lowest</td>
</tr>
</tbody>
</table>

- Moderate Risk
- Low Risk
- Moderate Risk
- High Risk
- Highest Risk

- Protect against unacceptable risk scenarios (Prioritize)
- Develop incident response plans for acceptable risk scenarios
- Evaluate the likelihood of each risk scenario materializing and its associated consequences
Develop and Overall Risk Management Program

- Oversight, implementation, training, enforcement and maintenance
- Development of biosecurity risk statement
- Development of biosecurity plan
- Ensuring adequate resources

risk management = risk + mitigation
Layers of Security

- Protection Area
  - Low consequence
- Limited Area
  - Moderate consequence
- Exclusion Area
  - High consequence
Re-evaluate

Re-evaluate and modify:
• Biosecurity risk statement
• Biosecurity risk assessment process
• Biosecurity program/plan
• Biosecurity systems

Re-enforce:
• Implementation, training, annual re-evaluation of biosecurity program
Re-evaluations and Revisions

- At least annually
- Routine review
- After any biosecurity-related incident
- After Program audits
- After Drills/Exercises
- Document
Laboratory Biosafety Training Program

Mission: provide a comprehensive curriculum for biosafety and biosecurity training.

Establish a solid base of laboratory skills and application of biosafety principals.
Determine Training Needs

- Regulatory requirements
- Risk assessments
- Hazards present
- BSL2 and BSL3 training
- PPE
- Laboratory practices
Develop a Training Plan

- New employee training
- Outside training versus site specific training
- Format
- Exams
- Competencies
- Exercises
Who Should be Trained?

- Laboratory staff working in the facility
- Maintenance and cleaning staff
- External first responders
- Security staff

Training should be commensurate with the roles and responsibilities and authorities of staff.
Scope of Training

• Didactic session on theory of biosafety and biosecurity
• Hands on training demonstrating proper BSC use
• Hands on training for proper PPE usage
• Procedure specific training
• Training should NOT be a one-time event!
New Employee Safety Orientation

• Create a checklist
  – Chemical Hygiene Plan
  – Safety information (on agency website)
  – Laboratory safety equipment
  – Chemical/Biological Safety Cabinet Operation
  – PPE
  – Laboratory Hazards (chemical, bloodborne pathogens, etc)
  – Immunizations (Occupational Health Program)
  – Laboratory Emergency Procedures

• Site specific training

• Procedure specific training (part of SOP)
Annual Refresher Competency Training

- Review Procedural changes
- New procedures
- Observation
- Part of annual competency assessment
- Exercises
Biosecurity and Select Agents

• Federal Regulations 42 CFR 73
• Regulations at www.selectagents.gov
  – Risk assessment
  – Physical security
  – Personnel security
  – Tier 1 Security
• Select Agent (SA) program for Clinical labs
Clinical lab security issues

- The same as ours, but potentially greater risk because more public access
- Facilities in hospitals
- Retrofit security
- Don’t have SA program accountability
- Smaller facilities will not have the volume of samples
Resources

  Biosafety in Microbiological and Biomedical Laboratories

- [http://www.cdc.gov/mmwr/preview/mmwrhtml/rr5119a1.htm](http://www.cdc.gov/mmwr/preview/mmwrhtml/rr5119a1.htm)

- [http://www.cdc.gov/mmwr/preview/mmwrhtml/su6101a1.htm](http://www.cdc.gov/mmwr/preview/mmwrhtml/su6101a1.htm)
  Guidelines for Safe Work Practices in Human and Animal Medical Diagnostic Laboratories
THE END!

THANKS!!