Biosecurity Risk Assessment Methodology (BioRAM) applicability to the U.S. Select Agent Program

Susan Caskey, Carlos Salazar, Nikki Held, Amanda Burroughs
Software revisions by Daniel Bowen

Overview

Biosecurity risk is defined, in this context, to include the risks posed by a malicious use of a biological agent for a criminal or terrorist activity. In 2001, biosecurity became a US national concern following the malicious release of bacterial spores which cause the disease anthrax. Prior to and directly following this incident, Sandia National Laboratories begin working with international and national bioscience facilities to implement biosecurity risk mitigation measures in the form of physical, personal, transportation, material accountably, and information security. In order to define the most appropriate security measures, Sandia National Laboratories uses a structured risk assessment process. This process has been converted into a formalized model and software tool, BioRAM.

In 2011, this model and software tool was reviewed to determine the applicability of its use in conducting laboratory assessments in direct support of the US Select Agent Program. This review included two parallel technical reviews. The first of these reviews focused on the portion of the model which defines the potential for a notional adversary to steal a biological agent; this review examined the legal framework of Select Agent Regulations (42 CFR Part 73, 9 CFR Part 121, and 7 CFR Part 331) as compared to the model criteria. The second technical review focused on the criteria defining the likelihood of successful exposure/infection from a malicious release to the human community and the consequences of this malicious release. The results of these reviews have enabled direct revisions to the BioRAM software model to increase its utility in support US Select Agent laboratory risk assessments. This paper will provide a summary of a comparison of the model to the current regulations and to the results of the Federal Experts Security Advisory Panel (FESAP) recommendations regarding tiering of the agents.

The FESAP was established by Executive Order 13546 on July 2, 2010 to provide recommendations related to the security of the biological select agents and toxins as they are defined in the Select Agent Regulations. These recommendations were released on June 14, 2011 (http://www.phe.gov/Preparedness/legal/boards/fesap/Pages/default.aspx).

BioRAM

The biosecurity risk assessment model (BioRAM) was designed for use by biorisk officers at laboratories to provide visualization of the relative risks and help to identify risk mitigation measures. The BioRAM models have incorporated IBTR and international biorisk officer experience in drafting sets of criteria, prioritizing the criteria, and outlining scoring functions for the criteria. The main objectives of these models are to help strengthen risk governance in the laboratories by providing assessment methods that are standardized, systematic, and repeatable.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.
SAND# 2011-7195

Risk is defined by likelihood and consequences. For biosecurity, likelihood is defined as the likelihood of theft of a biological agent from a facility by a notional adversary, the likelihood of successful malicious release which leads to exposure/infection and the severity of the consequence of a successful malicious release with the agent.

The assessment process is broken into components:

Evaluate the biological agents that exist at the facility.
Define specific or notational adversaries which pose a threat to the agents.
Evaluate the facility processes and procedures.
Evaluate the in place biorisk mitigation measures.

Within each component are several criteria and sub-criteria that are scored independently. These scores are weighted and then rolled up to provide the overall consequence and likelihood score. This method is based on a Multi Criteria Decision Analysis (MCDA) scheme, quantifying the various aspects of biorisk using qualitative definitions.

The final results show the relative risk of agents at the given facility, and give program management a mechanism to determine risks that are unacceptable. This scheme can aid management in allocating recourses to mitigate facility biorisks; or to assess current biorisk program management effectiveness.

This model is not intended to provide a formal quantitative assessment of absolute risk but, rather provide a structured method for the comparison of the relative risks posed by laboratory practices and by biological agents. There are numerous approaches to structured risk assessment and decision analysis; multi-criteria decision analysis (MCDA) is one of these methods. MCDA has been identified as a scientifically sound method for decision analysis and has been extensively validated for use in risk analysis.

"Research on quantitative decision making has proceeded from the study of decision theory founded on single criterion decision making towards decision support for more realistic decision making situations with multiple, often conflicting, criteria, and more than one decision-maker. In particular, MCDA stands out as a promising category within decision support methods."[1]

Linkov[2] and others have advocated the use of a multi-criteria decision analysis as part of a traditional risk assessment in situations where there is a limited set of empirical data and a high level of uncertainty. MCDA is a robust discipline and is useful in illustrating and justifying decisions. MCDA has been accepted by the risk community as a process for conducting structured risk assessments, focusing on areas with limited detailed knowledge, and where information may vary with time. In addition to the structure, MCDA also offers a transparent method for conducting the risk assessment as it can help in quantifying and communicating the risks and support decision-makers choices on risk management. MCDA provides a mechanism

[1] Mona Riabacke, Mats Danielson, Love Ekenberg, and Aron Larsson "A Prescriptive Approach for Eliciting Imprecise Weight Statements in an MCDA Process" Algorithmic Decision Theory: First International Conference, 2009
[2] Igor Linkov, "Comments on the OMB Risk Assessment Bulletin", 2006

to combine multiple information sources including those based upon expert judgment to assess risks. [3]

The basic structure of MCDA models is to define the relevant criteria which define the problem(s) to be addressed, attach numerical measurements and relative importance to the criteria, and to combine the numerical values to arrive at a relative ranking.[4] In MCDA there are several mathematical models which define how the numerical measurements and relative importance rankings are determined. Likewise, combining of measurements varies from model to model. The method used in this analysis is based upon a weighted sum algorithm which is one of the most common approaches. This method combines all the criteria and weights into a single score (*A*) by summing all the weighted numerical values (*aij*,*wj*).

When using MCDA for risk analysis, the resulting score of the weighted sum is a component in the creation of the relative risk ranking. In this methodology, the weighted sum is used to define the likelihood and the consequences independently. These two values are combined to create the relative risk characterization.

Evaluation of the Biological Agents

The BioRAM model, being a risk assessment model, calculates both the likelihood of successful malicious use of a biological agent and the consequences of this use.

The BioRAM model includes criteria which evaluate an agent's biological properties as they influence the likelihood of successful use. These include the potential routes of transmission, communicability, and natural stability. These criteria are evaluated using an absolute scale, with zero being the absence of ability for successful use and four being the worst case. Consequences are modeled based on the impact of disease to a human host (for human and zoonotic agents, the consequence model for animal diseases is slightly different) and the ability to mitigate the consequences of a malicious release. Additionally, socioeconomic impacts are also captured. As with the likelihood, these criterions are scored on an absolute scale with zero being the absence of consequence and four defining the worst credible consequence.

In reviewing the use of BioRAM as a support tool for the US Select Agent Program, 49 agents from the CDC (and overlap) list were evaluated by use of open source[5] literature review. The results of evaluation highlighted several agents as having both notably higher likelihood and consequence (or overall risk) relative to the other agents. These results correlated very closely with the FESAP recommended Tier 1 agents. Specifically this group included, smallpox

---

[3] Igor Linkov, F. Kyle Satterstrom, Jerrery Steevens, Elizabeth Ferguson, and Richard C. Pleus, "Multi-Criteria decision analysis and environmental risk assessment for nanomaterials" Journal of Nanoparticles Research, 2007

[4] Evangelos Triantaphyllou, *Multi-Critera Decision Making Methods: A comparative Study*, Kluwer Academic Publishers, 2000

[5] CDC Bioterror and Chemical Threat Websites, Public Health Agency of Canada MSDS Website, Iowa State University for Food Safety Factsheets, and the World Organization for Animal Health Website

(Variola major) virus, *Burkholderia mallei*, *Bacillus anthracis*, *Burkholderia pseudomallei*, Alastricm (Variola minor) virus, *Yersinia pestis*. Additionally, the reconstituted 1918 Spanish Fluvirus, which is not included in the FESAP Tier 1 agent list, fell in to this high risk area. Both of the recommended Tier 1 hemorrhagic fever viruses (Marburg and Ebola) were on the border. These agents could have significant consequences, but the potential for successful malicious use was lower than the other agents in the top tier in this model. The main drivers for their lower likelihood, as compared to the other agents, includes their lack of environmental stability and the limited ability for transmission.

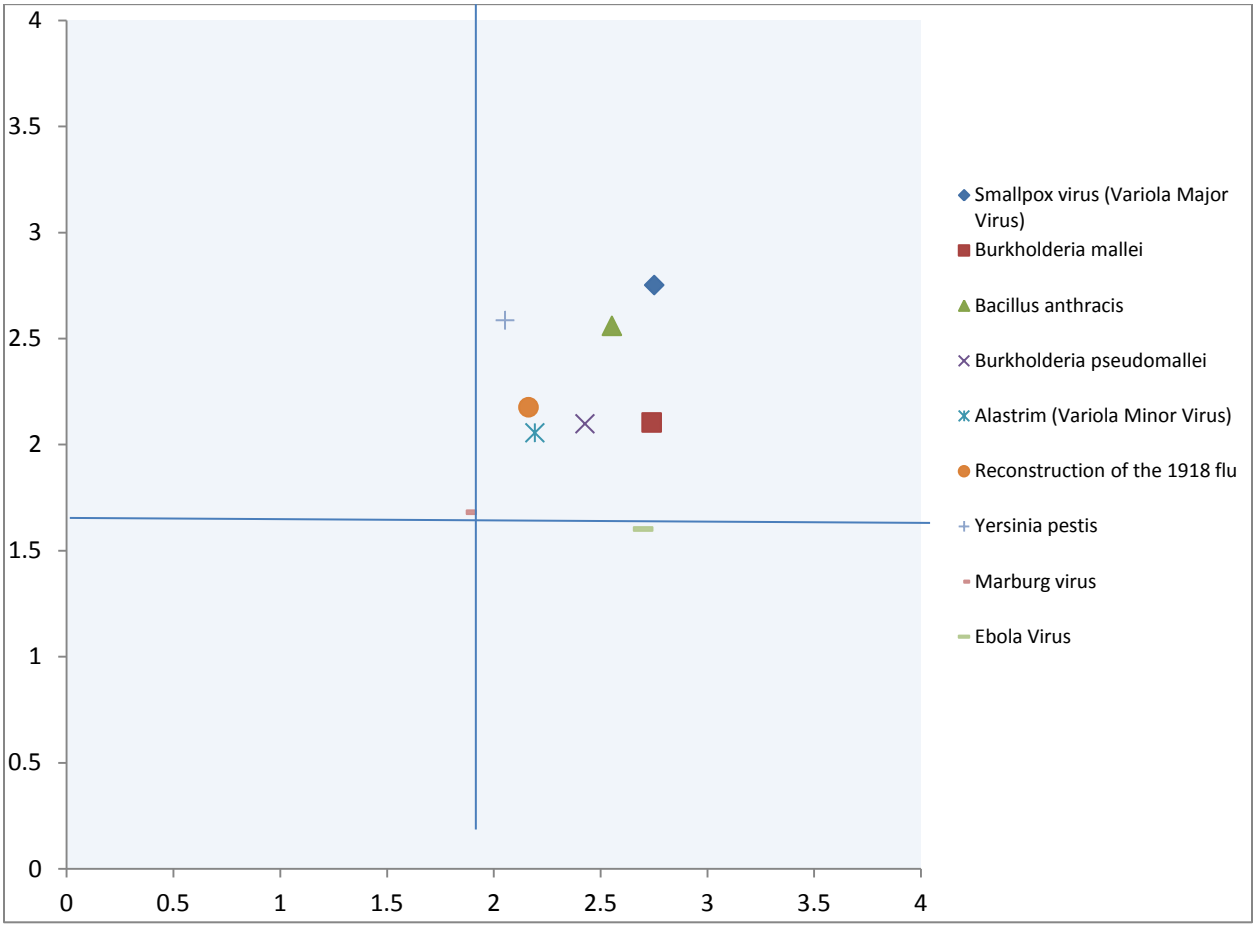

Figure 1: BioRAM Agent Model Highest Risk

This evaluation also highlighted several agents as being relatively a lower risk than the other agents on the CDC US Select Agent list. The agents which were modeled and fell into the overall lower risk characterization include: Cercopithecine herpesvirus 1 (Herpes B virus), *Coccidioides posadasii*/ *Coccidiodes immitis*, Eastern Equine Encephalitis virus, Central European Tick-borne encephalitis, Venezuelan Equine Encephalitis virus, Bovine Spongiform Encephalitis, *Clostridium perfringens* epsilon toxin, shiga toxin and the shiga-like ribosome inactivating proteins, and the T-2 toxin, several of the haemorragic fever viruses, other encephalitis viruses, toxins, the rickettsia, and monkeypox. It should be noted that the majority of these agents were clustered toward the center of the model, which when confidence intervals are added these agents would be characterized as a moderate risk and comparable to the other agents

included on the US Select Agent list. However, there are several very distinct lower risk agents; these include the T-2 toxin, Bovine Spongiform Encephalitis, the tick-borne encephalitis viruses, Menangle virus, and the Herpes B virus. All of these lower-risk agents are agents which have been recommended by FESAP for removal from the US Select Agent list.

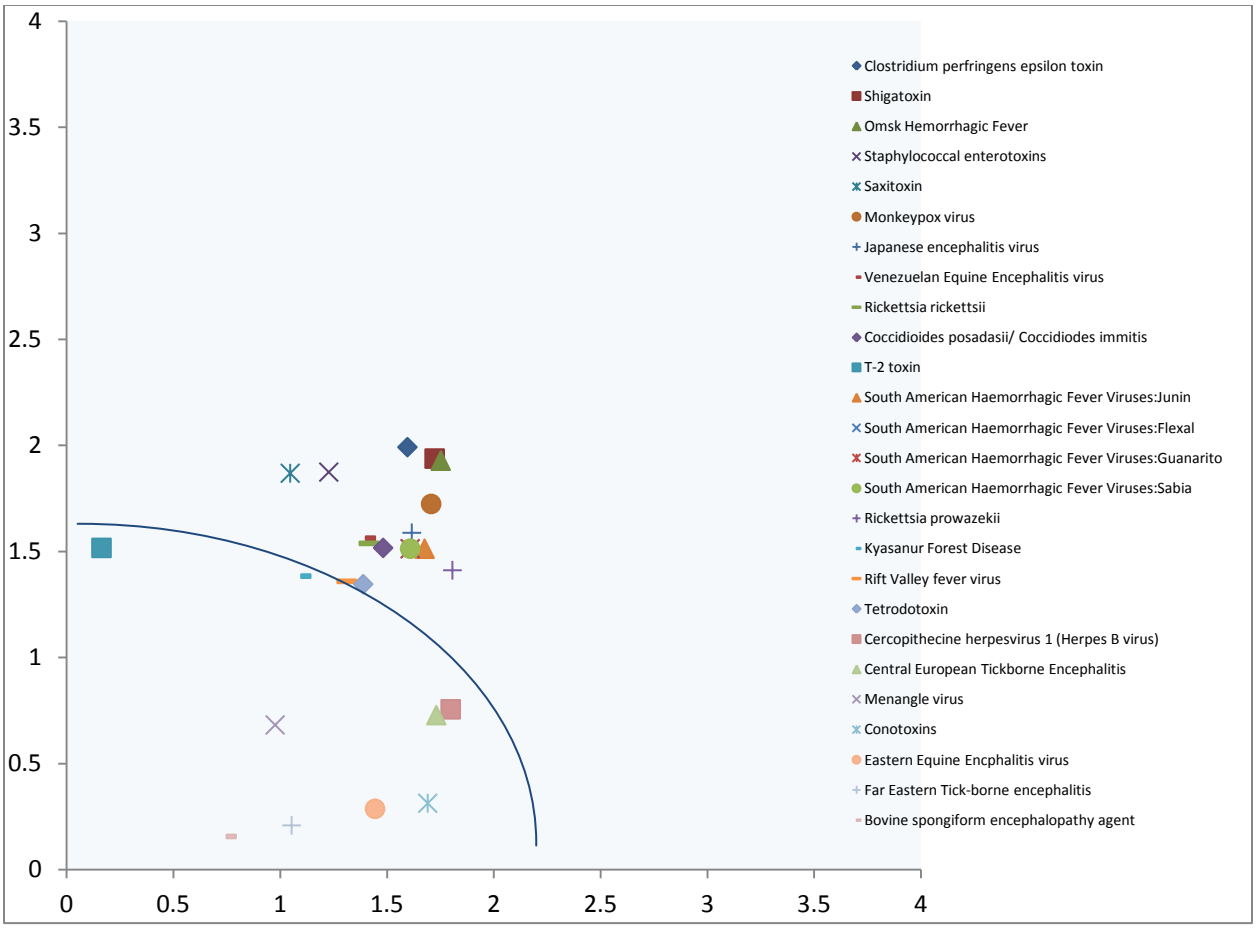

Figure 2: BioRAM Agent Model Lowest Risk

A risk analysis perspective to model the likelihood an agent can be used successfully for malicious intent and the consequences of this act creates a standardized, structured, and repeatable process for agent evaluation. This type of model can, transparently, be used in communication of the tiering process and can directly support FESAP recommendations.

Likelihood of successful theft as compared to the regulations

The BioRAM model calculates likelihood of successful theft by a notional adversary by defining the level of in place biosecurity risk mitigation measures as compared to no mitigation measures or ideal. These measures are defined by weighted criteria and defined absolute scales. In this model, the absence of a risk mitigation measure is defined as a four and ideal biosecurity risk mitigation measures by a score of zero (these are inverted absolute scales to facilitate using summations when combining scores). The criteria have been broken into a hierarchical structure which includes branches focusing on physical security, personnel security, transport security,

material control and accountability, information security, and program management. Each of these branches is weighed independently for insider threats and outsider threats and compared against each other.

Using the Select Agent Regulations, subject matter experts defined within the absolute scales for each criterion how the regulations matched with the pre-defined ideal (score of zero), specifically, the reviewers noted if the regulation was more restrictive or less restrictive than the BioRAM model ideal and if the regulation was less restrictive what score from BioRAM correlated with the regulation. From this review, a mathematically minimum accepted likelihood of theft, agent independent, could be calculated. The following lists the comparison of the regulation to the ideal pre-defining in BioRAM (the scores in bold correspond to the regulations):

Question	**Response Suggestions**
Physical Security	
What type (if any) of a facility or campus perimeter exists?	4 = Facility has no perimeter 3 = Facility has a partial perimeter **0 = Facility has a clearly defined perimeter (natural or man-made)**
Does the building housing the agent limit access through a control system?	4 = Building has no access controls **3 = Building has only procedural access controls** 2 = Building has manual access controls 1 = Building has electronic access controls based on something person has (e.g. swipe card) 0 = Building has electronic access controls tied to person, e.g. knowledge (e.g. PIN) or biometrics
Does the room housing the agent limit access through a control system?	4 = Room has no access controls **3 = Room has procedural access controls** 2 = Room has manual access controls 1 = Room has electronic access controls based on something person has (e.g. swipe card) 0 = Room has electronic access controls tied to person, e.g. knowledge (e.g. PIN) or biometrics
Do the agent storage areas (freezers, culture collection, etc) limit access through a control system?	4 = Asset has no access controls **3 = Asset has only procedural access controls** **2 = Asset has manual access controls** 1 = Asset has electronic access controls based on something person has (e.g. swipe card) 0 = Asset has electronic access controls tied to person, e.g. knowledge (e.g. PIN) or biometrics
Do intrusion detection systems exist in the areas where agents are used or stored?	4 = No intrusion detection **3 = Only detection is staff trained to report anything unusual** 2 = Detection based on observations by personnel, including roving guard patrols 1 = Local annunciation of alarms only 0 = Alarms for intrusion detection are reported to a central alarm station

Are all door and windows (or other potential entry points) alarmed?	**4 = No controls (access controls and/or intrusion detection) on any entry points** 1= Controls only on doors 0 = Controls on all possible entry paths through barrier (e.g. glass break sensors on windows)
How are alarms assessed?	**4 = No alarm assessment** 3= Only alarm assessment is staff trained to report 2= Guards sent to assess alarms 1 = Alarm assessed by camera 0 = Alarm assessed by camera that records brief time before alarm and then afterwards
How are alarms responded to?	**4 = No plans for alarm response** 2= Local law enforcement is initial response and a MOU is in place for this 1 = Local law enforcement is initial response, MOU in place, and this is exercised regularly OR Onsite guard response 0 = Onsite guard response and LLE back-up with MOU and regular exercises
Personnel Reliability	
How is personnel vetted prior to allowing them unescorted access to the agent, this should include the R.O., owner of entity is applicable, and any users?	4 = No vetting of personnel prior to granting access 3 = Vetting includes only verification of credentials (education, prior employment) and references 2 = Vetting includes verification of credentials, references, and criminal history **1 = Personnel are registered as defined by the security risk assessment process and have received their access approval** 0 = Personnel are registered as defined by the security risk assessment process and have received their access approval, in addition the facility conducts reviews credentials, past employment records, and interviews contacts and references.
How is the personnel vetted who will not have direct access of the agent, this may include persons maintaining equipment in or around laboratories, systems administrators, cleaning staff, etc?	**4 = No vetting of personnel prior to granting access** 3 = Vetting includes only verification of credentials (education, prior employment) and references 2 = Vetting includes verification of credentials, references, and criminal history 1 = Personnel are registered as defined by the security risk assessment process and have received their access approval 0 = Personnel are registered as defined by the security risk assessment process and have received their access approval, in addition the facility conducts reviews credentials, past employment records, and interviews contacts and references.

How are people escorted?	4 = Allowed unescorted access to room with asset 3 = Administrative escorting to room with asset allowed **2 = Escorting requirements in place but not defined escort ratios** 1 = Escort ratios defined 0 = Escort ratios defined, dates/times of escorted visitors recorded
Are badges worn?	**4 = Not required or routinely worn** 0 = Badges required
Do badges indicate level of access allowed by the wearer?	**4 = Badges not required or routinely worn** 4 = No indicators of the level of access by the wearer 0 = Badges indicate level of access
Does badge include a photo of the wearer (owner) and a time interval for when it is valid?	**4 = Badges not required or routinely worn** 4 = No way to identify if badge belongs to person wearing it 0 = Badges have a photo and expiration date
Are there procedures for returning badges or reporting lost badges?	**4 = Badges not required or routinely worn** 4 = No badge procedures 0 = Procedures are in place for lost badges and turning in badges when access in no longer needed
What is the level of biosecurity training provided?	4 = No biosecurity training provided **2 = Biosecurity training provided to anyone with unescorted access** 1 = Biosecurity training provided to all employees 0 = Biosecurity training provided to all employees and on-site contractors (e.g. guards)
Do employee assistance programs exist?	**4 = No support systems in place** 3 = Informal support network among personnel 2 = Formal employee assistance program in place 1 = And employees not penalized if access voluntarily suspended due to a temporary situation 0 = And anonymous whistleblower / omsbuds mechanism in place
Transport	
What is the level of control at a facility of materials moving between laboratories or while in shipping/receiving areas?	4 = No controls during internal transport 3 = Agent transported by authorized individual but may be left unattended in unsecured areas 1 = Agent not left outside of custody of authorized individual during transit unless secured but level of security is lower than how it is secured in storage **0 = Agent not left outside of custody of authorized individual during transit unless secured in a manner equivalent or better to how it is secured in storage**
What type of vetting is required for personnel transporting material within the facility?	4 = Facility personnel who have access to materials during internal transport are not vetted

	2 = Facility personnel who have access to the materials during internal transport are vetted but to a lower degree than those who handle the agent in the laboratory **0 = Facility personnel who have access to materials during internal transport are vetted to the same degree or better as personnel who handle the agent in the laboratory**
What type of administrative approvals is required for internal transport?	4 = No approvals or documentation required for internal transport 2 = Pre-approval not required for internal transport but transfer is documented in laboratory records **0 = Pre-approval required for internal transport and the transfer is documented in laboratory records**
What type of administrative approvals is required for external transport?	4 = No approvals or documentation required for external transport 3 = Pre-approval not required for external transport but transfer is documented in laboratory records 1 = Pre-approval by a responsible individual at the facility required prior to shipping to external recipient **0 = And a material transfer agreement is required prior to final approval or an external regulatory body must approve the transfer prior to shipment**
What is the required security level for the receiving facility when sharing this agent?	4 = No biosecurity (or biosecurity status is unknown) at receiving facility 2 = Receiving facility has biosecurity but their level of security is lower than at shipping facility 1 = Receiving facility has equivalent or better biosecurity **0 = And notifications between shipping and receiving facility at time of dispatch and receipt, respectively** ***SA: recipient notification of APHIS/CDC upon receipt (or non-receipt at expected time) within 48 hours***
How are agents packaged for external transport?	4 = Agent can be identified by examining labels on outside of the package **0 = Conforms to infectious substance shipping labeling requirements but does not identify the specific agent on the outside of the package.**
How are external carriers selected?	4 = No thought is given to security in selection of carrier 2 = External carrier chosen that has good reputation for security of commercial shipments (e.g. FedEx, DHL, Airborne Express) **0 = And the carrier has a security plan in place that covers shipments of dangerous biological agents**

Material Control and Accountability	
How does the facility determine which materials are subject to material control and accountability (MC&A) measures?	4 = No materials are subject to MC&A measures 3 = Individual PIs/lab owners make decisions about which materials require MC&A measures **2 = Facility just relies on regulatory or international lists (e.g Select agent list, Australia Group list) to determine which materials at their facility need MC&A measures** 1 = Facility risk assessment to identify and categorize those materials and forms of materials that require MC&A measures 0 = And, where applicable, proactive measures towards the reduction of risk through elimination, substitution or minimization of volumes/quantities of agents, and the type and number of manipulations conducted.
Which materials are inventoried?	4 = No material cataloging 3 = Seed stock inventory electronically managed 2 = Seed stock inventory actively managed and working stocks, including infected animal status, tracked through laboratory notes **1 = Seed stock inventory electronically managed using a secure system and includes tracking of samples that have been transferred into and out of the lab, source, strain, controlled substance identification, form, responsible individual, etc.** 0 = Seed and working stock containers bar coded or otherwise identified, marked and cataloged for inventory tracking purposes.
What is the level of control of agents while in use (working stocks, infected animals, etc)?	4 = No controls in place when materials are in use **2 = Controls in place when materials are in use (e.g. working tissue cultures, animals subjected to challenge experiments, in equipment such as incubators and centrifuges, etc.) but at lower level than controls for material in storage** 0 = Controls in place when materials are in use (e.g. working tissue cultures, animals subjected to challenge experiments, in equipment such as incubators and centrifuges, etc.) at equivalent level to controls for material in storage
Are there clearly defined accountability roles and responsibilities?	4 = No designation of responsibilities 2 = PI aware of each agent used within their laboratory 1 = A responsible individual is designated to oversee the control of protected agents **0 = A qualified and vetted individual is designated to oversee the control of protected agents (agent-by-agent basis, on a per-laboratory basis, etc.)**

Are there clearly defined procedures for material control and accountability (MC&A)?	4 = No procedures for MC&A exist **2 = Some MC&A procedures are in place but they are not comprehensive and/or are not fully implemented** **0 = Written procedures are in place and implemented to ensure timely and accurate recording, reporting and auditing of materials subject to MC&A measures**
Information Security	
Has information which is considered sensitive been clearly identified, marked, and protected at a level equivalent to the risk of loss or release?	4 = No identification and classification of information in place **1 = Sensitive (security-related) information is clearly addressed in the security plan to define how it is identified, marked, and classified.**
Is information which is considered sensitive protected from release or loss?	4 = No protection of information 2 = Some information protection procedures are in place but they are not comprehensive and/or are not fully implemented **0 = Protecting sensitive (security-related) information at a level equivalent to the risk (e.g. information considered a valuable asset is held redundantly by the institution. Information is accessed on a need-to-know basis, by pre-approved/screened authorized individuals. Procedures for handling, storing, transmitting, and destroying sensitive information) has been clearly defined in the security plan.**
Are there clearly defined communication policies regarding sensitive information?	**4 = No communication policies** 2 = Staff is trained on communication policies 0 = Means of communicating sensitive information is controlled (e.g. encryption for electronic transmission, no cellular discussions or communication/viewing sensitive materials).
Are electronic critical infrastructure systems (including inventory databases, alarm control stations, access control systems, building monitoring systems, etc) protected from attack?	**4 = No protection (e.g. adversary can access the systems through the internet)** 2 = Basic good practices are in place (e.g. firewalls, desktop security) 0 = Comprehensive IT security infrastructure in place or not applicable because no sensitive information is stored
Are there clearly defined policies for public disclosure of information?	**4 = No public disclosure procedures/policies in place** 2 = Some procedures/policies regarding public disclosure are in place but they are not comprehensive and/or are not fully implemented 0 = Potentially sensitive (security-related) information is screened prior to public release, by an established review and approval process. Modification of information to make it appropriate for public release

Program Management	
Does the institution have defined roles and responsibilities for biosecurity?	4 = There is no identification of, or education on, biosecurity roles and responsibilities **3 = Facility personnel are educated on their biosecurity roles and responsibilities** 2 = A biosafety officer is identified at this facility 0 = Management at this facility ensures roles, responsibilities, and authorities are defined, documented, and communicated
Has the institution made a commitment to security?	4 = Management at this facility is not aware, or interested in, biosecurity concerns 3 = Management at this facility is aware of biosecurity concerns, but has not implemented a biosecurity policy or devoted resources to address the issue 2 = Management at this facility have made some efforts to improve biosafety at the facility, but they are not comprehensive and/or are not fully implemented **1 = This facility has a comprehensive biosecurity policy in place, which was developed, authorized, and signed by top management. The policy is appropriate to the nature and scale of the risk. Management establishes the commitment and objectives of the biosecurity system, and communicates this to all stakeholders.** 0 = Management at this facility identifies and prioritizes program needs and allocates funds as necessary
Does the institution have comprehensive biosecurity documentation?	4 = This facility has no biosecurity policies, manuals, or SOPs 3 = This facility has no specific biosecurity documentation 2 = This facility has some biosecurity documentation, but they are not comprehensive and / or not fully implemented 1 = This facility has biosecurity policies, manuals, and SOPs **0 = This facility's biosecurity documentation also includes risk assessment and incident response information**
Does the institution conduct biosecurity drills or exercises?	4 = This facility does not conduct any biosecurity exercises 2 = This facility conducts tabletops or other exercises on an ad hoc basis **1 = This facility conducts annual exercises** 0 = This facility includes external responders in their exercises

Does the institution periodically review the biosecurity program?	4 = There is no review of the biosecurity program 3 = The biosecurity program is reviewed and revised as necessary after any incidents or near-incidents. **2 = The biosecurity program is reviewed and revised as necessary annually and after any incidents or near-incidents** 1 = The biosecurity program is subject to internal self-assessments 0 = Management at the facility ensures continual improvement, conducts routine self-assessments, and ensures corrective and preventive actions. Reviews include assessing opportunities for improvement and any needs for changes to the system, procedures, policies, and objectives.

Based upon these results, a bioscience laboratory in compliance with the US Select Agent Regulations would have a likelihood score at or below 0.74 out of a worst case score of 4, or a relative reduction of successful theft from an outside adversary by almost 80% as compared to a laboratory with no security measures implemented. This score is a weighted roll up of the individual scores, as a result, it may be possible for a laboratory to be outside of compliance in one criterion but still be overall within the minimal acceptable level of potential of successful theft. The potential scores are calculated independent of the likelihood of successful use of the agent (successful use is defined by the likelihood of successful exposure/infection from a malicious release).

These calculated values provide users of the model a base line of expected results of a laboratory in compliance to the regulations.

Conclusions

The nature of the BioRAM model demonstrates utility in evaluation of bioscience laboratories to characterize the biosecurity risk. This model can be used in reviewing laboratories to determine compliance to the US Select Agent Regulation. Careful consideration to how each criterion is scored should be considered by the evaluator to ensure a laboratory is not vastly outside of compliance in one area. Additionally, the regulations do not include any considerations for the biological properties of the agent's (an agent is either on or off the list) the agent's properties which influence the likelihood of successful misuse or the consequences of the misuse must be evaluated separately from the laboratory. The agent portion of the model supports the teiring of the US Select Agent and demonstrates complementary results to the FESAP recommendations.

Model Details

The updated software used in this model will be made available for use and evaluation. The detailed algorithms and weights used in this model will also be made available upon request.