

# Bridging Science and Security for Biological Research

Personnel Security Programs  
Meeting Report • 21 - 22 August 2013



Prepared by the American Association for the Advancement of Science in conjunction with the Association of American Universities, Association of Public and Land-grant Universities, and the Federal Bureau of Investigation

## BRIDGING SCIENCE AND SECURITY FOR BIOLOGICAL RESEARCH: PERSONNEL SECURITY PROGRAMS

**Meeting Report**  
August 21-22, 2013  
Washington, DC

### Organized and Prepared By

Kavita M. Berger, American Association for the Advancement of Science  
Jennifer Roderick, American Association for the Advancement of Science  
Carrie Wolinetz, Association of American Universities  
Kari McCarron, Association of Public and Land-grant Universities  
Edward You, Federal Bureau of Investigation  
K. William So, Federal Bureau of Investigation  
Sonia Hunt, Federal Bureau of Investigation



## Acknowledgements

We would like to thank the panelists and meeting attendees who provided valuable discussion and helpful comments on the report. This meeting was supported by a contract from the Biological Countermeasures Unit of the Federal Bureau of Investigation's WMD Directorate. We thank the FBI WMD Directorate for its generous support of this meeting.

## Disclaimer

The concerns or suggestions outlined in this report reflect the discussions at the workshop and do not necessarily represent the views of the FBI WMD Directorate; AAAS Board of Directors, its Council, or membership; AAU Board of Directors or membership; or APLU Board of Directors or membership.

Produced in the United States (2014)  
American Association for the Advancement  
of Science  
1200 New York Avenue, NW  
Washington, DC 20005

## About FBI/WMDD/BCU

The FBI's WMD Directorate (WMDD) was created after September 11, 2001 to provide a cohesive and coordinated approach to countering WMD threats and responding to incidents if they occur. Recognizing the unique and inherent challenges to preventing bioterrorism, the FBI/WMDD/Biological Countermeasures Unit (BCU) conducts extensive outreach to the life sciences community to proactively build mutually-beneficial relationships and broaden scientists' understanding of biosecurity concerns.

## About AAAS

The American Association for the Advancement of Science (AAAS) is the world's largest general scientific society and publisher of the journal, *Science* ([www.sciencemag.org](http://www.sciencemag.org)). AAAS was founded in 1848, and serves 262 affiliated societies and academies of science, reaching 10 million individuals. *Science* has the largest paid circulation of any peer-reviewed general science journal in the world, with an estimated total readership of 1 million. The non-profit AAAS ([www.aaas.org](http://www.aaas.org)) is open to all and fulfills its mission to "advance science and serve society" through initiatives in science policy, international programs, science education, and more.

## About AAU

The Association of American Universities (AAU) is a non-profit association of 60 U.S. and two Canadian pre-eminent public and private research universities. Founded in 1900, AAU focuses on national and institutional issues that are important to research-intensive universities, including funding for research, research and education policy, and graduate and undergraduate education.

## About APLU

The Association of Public and Land-grant Universities (A•P•L•U) is a non-profit association of public research universities, land-grant institutions, and many state university systems and has member campuses in all 50 states and the U.S. territories. The nation's oldest higher education association, APLU is dedicated to advancing research, learning, and engagement. Current initiatives include efforts in math and science teacher preparation, international development, institutional accountability, online education, and more.

# Table of Contents

---

<b>About the Project .....</b>	<b>4</b>
Bridging Science and Security for Biological Research.....	4
FBI Biosecurity and Outreach Project .....	4
<b>Personnel Security.....</b>	<b>6</b>
Elicitation and Insider Threat .....	7
<b>History of Personnel Security Activities in the United States .....</b>	<b>8</b>
Recent Policy Discourse on Personnel Security .....	9
The Meeting .....	11
<b>Meeting Summary.....</b>	<b>12</b>
Personnel Security Programs: Mitigation of Security Threats .....	12
Sector-Specific Personnel Suitability Programs .....	13
Non-Defense Institutions .....	14
Defense Institutions .....	16
Psychological Assessments.....	17
Underlying Approach .....	17
Effectiveness of Personnel Security Programs.....	18
<b>Conclusions.....</b>	<b>19</b>
<b>Appendix 1: Meeting Agenda .....</b>	<b>20</b>
<b>Appendix 2: Meeting Participants .....</b>	<b>23</b>
<b>Appendix 3: Federal Select Agent Program.....</b>	<b>26</b>
<b>Appendix 4: Army Biosurety Program.....</b>	<b>28</b>
<b>Appendix 5: U.S. Code of Federal Regulations.....</b>	<b>33</b>
<b>Appendix 6: Publications on Personnel Security for Biological Select Agents and Toxins .....</b>	<b>35</b>
<b>Appendix 7: Biosecurity/Personnel Security Case Studies.....</b>	<b>36</b>
<b>One-Page Description of FBI WMD Coordinator Overview.....</b>	<b>42</b>

# About the Project

---

The Federal Bureau of Investigation (FBI) Weapons of Mass Destruction (WMD) Directorate has developed a robust biosecurity outreach and awareness program with the scientific community. To strengthen this relationship, the FBI WMD Directorate contracted with the American Association for the Advancement of Science (AAAS) to host a series of outreach and policy meetings with research, policy, and security stakeholders and summarize important lessons learned, challenges faced, and areas for improvement of local and national biosecurity initiatives.

## Bridging Science and Security for Biological Research

This project was carried out in collaboration with the Association of American Universities (AAU) and Association of Public and Land-grant Universities (APLU), AAAS, and the FBI WMD Directorate.

The first meeting, held in February 2012, provided opportunities for academic scientists and research administrators to build trust and enhance their relationship with the security community, with the mutual goal of jointly addressing the challenges of mitigating biosafety and biosecurity risks.

The second meeting, held in September 2012, provided the opportunity for scientists and research administrators to share best practices and lessons learned about the review and oversight of dual use life sciences research with each other and with the security and policy-making communities.

The third meeting, held in February 2013, focused on critical issues resulting from foreign scientists studying or working in the U.S., international collaboration, and U.S. scientists working in foreign countries.

The fourth meeting, held in April 2013, focused on the challenges faced during implementation of the revised Select Agents and Toxins Regulations and possible approaches for addressing those challenges.

The fifth meeting, held in August 2013, focused on improving understanding of the components of a sound personnel security program, providing examples of existing personnel security programs, and determining mitigation strategies for identified gaps.

## FBI Biosecurity and Outreach Programs

The FBI contributes to the U.S. government's efforts to reduce the risk of bioterrorism by enforcing the federal statutes that prohibit development, production, or stockpiling of biological weapons. A major component of these efforts is the biosecurity initiatives developed by the Biological Countermeasures Unit (BCU) of the FBI's WMD

Directorate. These initiatives focus on preventing the acquisition or exploitation of biological material, technology, and expertise to intentionally cause harm.

The BCU has established a successful biosecurity outreach program, the goal of which is to establish strong, sustainable relationships with officials and scientists from research institutions to prevent and mitigate potential threats faced by research institutions.. The primary way in which the FBI engages with the scientific community is through their Academic Biosecurity Workshops. FBI WMD Coordinators conduct the workshops using a series of dialogues and exercises to bring relevant academic, health, first responder, law enforcement, and industry experts together to: 1) promote an understanding of their respective roles and responsibilities, capabilities, and resources; and 2) develop feasible, implementable threat mitigation strategies. The WMD Coordinators offer a point of contact at the local level and provide local support and security expertise. These efforts build on a shared goal of serving the public good.

The tangible benefits generated by these engagements are evident by the increased interest of research institutions in the FBI Biosecurity Workshops, increased interaction with local FBI WMD Coordinators, and incorporation of the WMD Coordinator in the notification protocols of an institution's security plan. In addition, this model has garnered international attention; requests for assistance to implement similar academic workshops have come from both the law enforcement and academic communities of foreign nations.

A one-page description of the FBI WMD Coordinator Overview is included at the end of this report.

# Personnel Security

---

Research institutions and their staff face a number of threatening acts – including stalking, domestic violence, sexual harassment, campus and workplace violence, and other criminal acts – on a fairly routine basis. In fact, the U.S. Occupational Health and Safety Administration cites homicide as the “fourth-leading cause of fatal occupational injuries in the United States.”<sup>1</sup> In addition to these more common occurrences, scientists and research institutions have been, and continue to be targets of domestic terrorism, including violent animal rights and environmental extremism. Beyond acts of violence, government, private, and academic research institutions face theft of materials, trade secrets, and intellectual property; diversion of assets; espionage; and human error or negligence, which are more common and imminent risks.

Threats may come from employees of an institution (i.e., insider threat) or non-employees (i.e., external threats), and from domestic or foreign individuals or groups. Individuals or groups might target individual staff, faculty, and/or students; specific facilities or building; or the entire institution. Academic institutions, along with private companies and government laboratories, can be targets of internal or external threats.

Often, an institution’s research activities determine which individuals or groups present a threat(s). For example, research institutions that support research with animals and scientists who conduct research with animals might be targeted by animal rights extremists (e.g., individuals or groups such as the Animal Liberation Front). Similarly, institutions that conduct national security-relevant studies or research with restricted materials might encounter threats from foreign or domestic adversaries who seek access to research results and/or materials. Similarly, private companies are often targeted by competitors to gain access to propriety information, trade secrets, intellectual property, and new research and development initiatives (i.e., industrial espionage). Finally, individuals or groups with harmful intent may seek access to sensitive research materials, technologies, and/or expertise to enhance their ability to develop biological or chemical weapons.

Strategies used by external threats to influence or manipulate institutional personnel, or otherwise gain access to sensitive information from research institutions include:

- Hacking electronic media;
- Inquiring about research at conferences or trade fairs;
- Sending or recruiting students at U.S. universities;
- Romantic or sexual advances;
- Exploiting foreign assistance or cooperation; and
- Targeting certain ethnicities or nationalities.

---

<sup>1</sup> Occupational Health and Safety Administration. Safety and Health Topics: Workplace Violence. Available at <https://www.osha.gov/SLTC/workplaceviolence>. Accessed on February 13, 2014.

## Elicitation and the Insider Threat

Individuals or groups might target employees through elicitation, which “is a technique used to discreetly gather information. It is a conversation with a specific purpose: [to] collect information that is not readily available and do so without raising suspicion that specific facts are being sought. It is usually non-threatening, easy to disguise, deniable, and effective. The conversation can be in

person, over the phone, or in writing.”<sup>2</sup> When “conducted by a skilled collector, elicitation will appear to be normal social or professional conversation.”<sup>3</sup> Employees may never realize that they were targeted or provided meaningful information. Examples of elicitation or manipulation are included in the box.

Elicitation/Manipulation	
	
<b>Techniques</b>	<b>Why it Works</b>
<ul style="list-style-type: none"><li>▪ Flattery</li><li>▪ Target the outsider</li><li>▪ Confidential bait</li><li>▪ Leading questions</li><li>▪ Feigned ignorance</li><li>▪ False interviews</li><li>▪ Good listener/validation</li><li>▪ Opposition/feigned incredulity</li><li>▪ Deliberate false statements</li></ul>	<ul style="list-style-type: none"><li>▪ A desire to feel important</li><li>▪ May not realize importance of information</li><li>▪ A tendency to gossip</li><li>▪ A tendency to believe others are honest</li><li>▪ A desire to appear well informed</li><li>▪ A desire to be polite and helpful</li><li>▪ A desire to feel appreciated</li><li>▪ A desire to convert someone to our opinion</li><li>▪ A tendency to correct others</li></ul>

Personnel security programs were developed to safeguard institutions and scientific research by minimizing or avoiding harmful acts caused or carried out by employees. Employees that might cause harm to the research institution, specific facilities, or individual staff members could be acting on their own accord or under the influence of others (external threats).

Criminal background checks capture only a portion of individuals who could harm others intentionally or accidentally. Federal requirements for personnel security and safety rely on criminal background checks to minimize the threat of individuals displaying threatening behaviors or intent gaining access to sensitive materials or information.

<sup>2</sup> Federal Bureau of Investigation. Elicitation Techniques. Available at: <http://www.fbi.gov/about-us/investigate/counterintelligence/elicitation-techniques>. Accessed on January 7, 2014.

<sup>3</sup> Ibid.

# History of Personnel Security Activities in the United States

---

The inception of U.S. personnel security programs dates back to the Civil Service Act of 1883, which required applicants for federal employment to possess the requisite character, reputation, trustworthiness, and fitness for employment. The Hatch Act of 1939 added the prohibition that a federal employee cannot be a member of any organization that advocates the overthrow of the U.S. government. Similarly in 1942, War Service Regulation II denied federal employment to anyone whose loyalty was in “reasonable doubt,” the definition of which was left to the judgment of the U.S. Civil Service Commission.

The first research-based personnel security program was authorized by the Atomic Energy Act of 1946 to protect atomic/nuclear weapons research and development. The act created the Atomic Energy Commission; mandated the development of a personnel security program for nuclear weapons facilities; and directed the Federal Bureau of Investigation (FBI) to investigate the character, associations, and loyalty of applicants. Amendment of the Atomic Energy Act in 1954 authorized the establishment of the Nuclear Regulatory Commission (NRC) Safeguards and Security programs. The NRC programs created a structure for the protection of “Restricted Data” as a separate category from national security clearances. Most scientists that have had to undergo vetting and monitoring worked in the national security and defense sectors. During the second half of the 20<sup>th</sup> century, Presidential Executive Orders were issued, acts passed, and amendments made regarding personnel reliability and security.

During this time period, personnel security vetting at universities and non-defense laboratories centered on export control regulations and deemed exports, and protection of intellectual property. The export control regulations require institutions to obtain an export license to transfer controlled technologies or information<sup>4</sup> to individuals and entities from certain countries. A subset of the export controls regulations involves transfer of controlled technologies and information to foreign individuals in the U.S. who are from certain countries. The deemed export rules apply to scientists from certain countries who are visiting, studying, or working in the U.S. and who do not have permanent residence status, U.S. citizenship, or another protective status. In addition, research institutions often have technology transfer offices to prevent transfer of technologies without the appropriate intellectual property rights protections in place.

Since 2001, the U.S. has passed a series of laws and developed several regulations focused on preventing unauthorized access to chemical, biological and radiological

---

<sup>4</sup> Within the context of export control regulations, fundamental research in science and engineering are exempt from export control regulations.

materials. (Brief descriptions of the relevant laws and regulations for vetting persons with access to biological agents and toxins are included in the appendices of this report.) The anthrax mailings in 2001 brought new focus on structured personnel security programs in government and non-government research involving biological Select Agents and Toxins. Fingerprinting, suitability and reliability verification, and security assessments were among the security provisions implemented for scientists and support staff seeking access to hazardous chemicals, cesium irradiators, and biological select agents and toxins.

In addition to the increase in legal requirements, research institutions encounter internal and external threats from violent animal rights extremists, violent activists against other types of life sciences research, disgruntled students and staff, and other individuals' intent on doing harm. These realities have prompted some universities and research institutions to establish threat assessment teams, which are comprised of representatives from several institutional offices and campus/local law enforcement. These teams are convened to communicate threats to the research campus and to identify and implement measures to prevent or mitigate such threats. Furthermore, the FBI WMD Directorate has developed case studies that highlight the types of threats and tactics perpetrated by individuals in research laboratories and hospital environments to increase the understanding and awareness of personnel security issues at research institutions.

## Recent Policy Discourse on Personnel Security

In 2009, the National Academies established the Committee on Laboratory Security and Personnel Reliability Assurance Systems for Laboratories Conducting Research on Biological Select Agents and Toxins. The committee was charged with assessing the efficacy of regulations, procedures and oversight that were instituted to safeguard against the deliberate use of Biological Select Agents and Toxins (BSAT).<sup>5</sup> The committee identified six principles that should guide consideration of BSAT research, and these principles provided the lens through which the committee offered its conclusions and recommendations:

- Research on Biological Select Agents and Toxins is essential to the national interest;
- Research with Biological Select Agents and Toxins introduces potential security and safety concerns;
- The Federal Select Agent Program should focus on those biological agents and toxins that might be used as biothreat agents;
- Policies and practices for work with BSAT should promote both science and security;
- Not all laboratories and not all agents are the same; and

---

<sup>5</sup> "Responsible Research with Biological Select Agents and Toxins", National Research Council (US) Committee on Laboratory Security and Personnel Reliability Assurance Systems for Laboratories Conducting Research on Biological Select Agents and Toxins, Washington (DC): National Academies Press (US); 2009.

- Misuse of biological materials is taboo in every scientific community.<sup>6</sup>

Consideration of these principles led the committee to nine recommendations that it believed were essential for keeping BSAT research secure from both internal and external threats.

Also in 2009, the National Science Advisory Board for Biosecurity (NSABB) published its recommendations on personnel reliability, after more than two years of consultation with security experts from several sectors. The NSABB concluded that strong institutional and laboratory management is essential for the development of a “culture of responsibility, integrity, trust, and effective biosecurity.”<sup>7</sup> It suggested several practices that institutions could adopt. However, the Board recommended that these practices not be applied uniformly to the academic sector by the federal government because implementation of personnel reliability practices will be affected by local and state laws and institutional policies. The NSABB provided several recommendations to enhance “hiring and employment practices to meet personnel reliability needs,” encourage “biosecurity awareness and promote responsible conduct,” and assess “the effectiveness of practices aimed at enhancing personnel reliability and a culture of responsibility.”<sup>8</sup>

The 2012 revision of the U.S. Select Agents and Toxins Regulations requires the implementation of a personnel security program for vetting and continuously monitoring personnel holding or seeking access to thirteen pathogens and toxins classified as significant public safety and security risks to the United States (referred to as “Tier 1 agents”). In response, several institutions that support research with these pathogens have independently established behavioral threat assessment teams; these teams help institutional officials evaluate the suitability and reliability of incoming and existing laboratory personnel that work with Tier 1 agents. These teams draw on the institutional offices of human resources, general counsel, security and law enforcement, environmental health and safety, and occupational health.

During a 2013 meeting on the implementation of the revised Select Agents and Toxins Regulations, participants representing universities throughout the U.S. requested information on how to best design and implement personnel security programs at their institutions. In response, the American Association for the Advancement of Science (AAAS), FBI WMD Directorate, Association of American Universities (AAU), and Association of Public and Land-grant Universities (APLU) organized a meeting for university officials and security experts to share information and programs on personnel security. Since universities must address compliance requirements and other security

---

<sup>6</sup> Ibid.

<sup>7</sup> National Science Advisory Board for Biosecurity. Guidance for Enhancing Personnel Reliability and Strengthening the Culture of Responsibility: A Report of the National Science Advisory Board for Biosecurity. (2011). Available at: [http://oba.od.nih.gov/biosecurity/pdf/CRWG\\_Report\\_final.pdf](http://oba.od.nih.gov/biosecurity/pdf/CRWG_Report_final.pdf). Accessed on October 10, 2013.

<sup>8</sup> Ibid.

threats, participants were asked to consider the breadth of possible personnel security threats that a research institution might encounter.

## The Meeting

In August 2013, AAAS, AAU, APLU, and the FBI convened a meeting of scientists, research administrators, and personnel security experts to discuss key considerations in initial and on-going personnel security programs in the biological sciences research and development sector.

The *goals* of the meeting were:

- To discuss and compare personnel security programs, sharing best practices and models among sub-sectors of biological sciences research and development;
- To better understand elicitation and vulnerability, which could contribute to compromised security, and security of information and intellectual property; and
- To suggest approaches for personnel suitability assessments.

The meeting was held as not-for-attribution to encourage interaction and discussion. This report describes the major themes and policy-relevant issues that were presented at the meeting in the sections: *Meeting Summary*, and *Conclusions*. These sections are followed by seven appendices that include the meeting agenda, list of participants, a summary of the Select Agents and Toxins Regulations, a summary of the current Army regulations on biosurety,<sup>9</sup> a summary of the relevant sections of the U.S. Code of Federal Regulations, publications on personnel security of Biological Select Agents and Toxins, and biosecurity/personnel security case studies.

---

<sup>9</sup> The Army Biosurety Program provides “protection to personnel, the local population, and the environment by ensuring that the biological select agents and toxins (BSAT) operations are conducted safely; that BSAT are secure; and that personnel involved in those operations meet the highest standards of reliability.” Available at <http://mrmc.amedd.army.mil/assets/docs/media/biosuretyCommPlan.pdf>. Accessed on February 25, 2014.

# Meeting Summary

---

## Personnel Security Programs: Mitigation of Security Threats

Personnel threats come in two forms: insider threats and external threats. The overall effectiveness and acceptance of personnel security programs hinges on sensitizing employees to the possibility that people in their workplace might harm others for personal reasons or recruited or manipulated by outside groups.

Participants agreed that addressing personnel security in practice relies on employers:

- Identifying individuals who pose a threat prior to hiring;
- Identifying existing employees whose risk potential changes over time;
- Identifying a threat when it arises; and
- Managing threats safely and effectively after they are detected.

Participants identified certain strategies that they have used, or would consider using, to mitigate personnel security threats, particularly insider threats (Box 1).

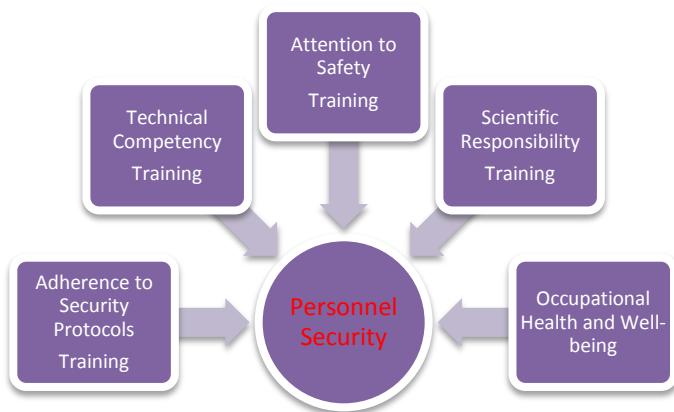
### Box 1. Insider Threat Mitigation Strategies

Protection of Data/Information	<ul style="list-style-type: none"><li>• Protect sensitive and/or critical information using passwords or other electronic mechanisms</li><li>• Mark or track sensitive information</li><li>• Implement data security programs to prevent theft of data or other sensitive information, including intellectual property</li><li>• Enforce deemed export control requirements</li></ul>
Hiring	<ul style="list-style-type: none"><li>• Be aware of possible influencing affiliations, including the institutions where current or prospective employees studied, worked (some institutions might have demonstrated links to problematic groups or activities)</li><li>• Communicate with other organizations about possible problems of individuals seeking transfers or employment</li></ul>
Personnel Access	<ul style="list-style-type: none"><li>• Clearly define the statement of work for employees working with sensitive research or restricted materials</li><li>• Implement a tiered system in which personnel must be approved for access to the research facility, restricted or controlled areas, and/or restricted or controlled materials</li></ul>
Employee Behavior	<ul style="list-style-type: none"><li>• Encourage self, anonymous, and peer reporting of possible problems</li><li>• Require employees working with sensitive research or restricted information to report new and/or unusual contacts</li><li>• Stress performance goals, which promote ownership and responsibility of one's actions</li><li>• Encourage face-to-face interaction between peers and colleagues and stress mentorship to facilitate communication, build trust, reinforce expectations, and identify possible problems</li><li>• Implement an employee "opt-out" option to allow employees to remove themselves from high-stress, high-risk research for a short time period without punitive action</li></ul>
Training	<ul style="list-style-type: none"><li>• Require employees to undergo security training</li><li>• Require periodic awareness training for employees</li></ul>
Personnel Action	<ul style="list-style-type: none"><li>• Develop clear institutional policies for how to handle cases in which an employee is suspected of inappropriate behavior</li><li>• Separate management actions from reliability actions and linking punishments to expected behavior of personnel</li></ul>
Community Engagements	<ul style="list-style-type: none"><li>• Establish open lines of communication and partnership with the local FBI WMD Coordinator</li><li>• Conduct table top exercises with local and state officials</li></ul>
Visitors	<ul style="list-style-type: none"><li>• Share information about visitors to the institution</li></ul>

While these strategies can provide a baseline for risk mitigation as institutions begin to develop their personnel security programs, each institution should carefully consider all possible strategies and incorporate those approaches that best fit their facilities, threats, and community. The key is to develop programs that focus on minimizing and effectively mitigating the threat without limiting creativity and unconventional thinking, or creating a risk-averse environment that might be detrimental to scientific advancement.

## Sector-specific Personnel Suitability Programs

Mitigation strategies of most personnel suitability programs fall within five key areas: adherence to security protocols, technical competency, attention to safety (including working in high stress environments competently and reliably), scientific responsibility, and occupational health and wellness. Training is essential for security, safety and responsibility.



Personnel suitability programs naturally differ according to specific needs of the sector (e.g., national defense, private sector, or academia) and the type of research or scientific activities conducted. In general, programs include suitability based on educational and work verification, competency, criminal background check, and medical evaluation. The medical evaluation may include a psychological assessment to determine whether the person might have criminal or otherwise harmful behavioral tendencies.<sup>10</sup> Lastly, the incorporation of scientific responsibility - scientists who are ethically sound and conduct themselves in socially conscious manner – is arguably an important component of personnel suitability or reliability programs.

Meeting participants provided details of their personnel security programs. A summary of the components of four of these programs is shown in Table 1 and described below. Three of the contributors were academic institutions while the fourth was a defense

<sup>10</sup> In 2009, the National Science Advisory Board for Biosecurity recommended to the U.S. government not to use mental assessments, drug and alcohol tests, or polygraph tests in personnel reliability assessments. In addition, the NSABB stated “The strength of such psychological assessments is in their ability to identify major psychological disorders; however, their ability to identify more subtle deviations or concerns is more problematic. Moreover, identifying an individual with malevolent intent appears, if not impossible, at least extremely difficult.” National Science Advisory Board for Biosecurity. *Enhancing Personnel Reliability among Individuals with Access to Select Agents*. (2009)

institution - a facility in which national security initiatives comprise the sole or primary purpose of research activities (e.g., a national laboratory).

**Table 1. Sector-specific Examples of Personnel Security Programs**

Example	University #1	University #2	University #3	Defense Laboratory
Primary Office	Biological Safety Office	Biological Safety Office	Biological Safety Office	Security Office
Independent Committee Review	Personnel Suitability Committee	Behavioral Security Committee	Development team of security experts and research personnel	Insider threat working group
Other Offices Involved	<ul style="list-style-type: none"> <li>• Human Resources</li> <li>• General Counsel</li> <li>• Occupational Health</li> <li>• Director of Recruiting and Selection</li> </ul>	<ul style="list-style-type: none"> <li>• Human resources</li> <li>• Campus police</li> </ul>	<ul style="list-style-type: none"> <li>• Campus police</li> </ul>	
Checks	<ul style="list-style-type: none"> <li>• Pre-employment Background Check</li> <li>• Fingerprinting</li> <li>• Medical check</li> <li>• Behavioral Interviews</li> </ul>	<ul style="list-style-type: none"> <li>• Background checks</li> </ul>	<ul style="list-style-type: none"> <li>• Background checks</li> </ul>	<ul style="list-style-type: none"> <li>• Mental health</li> <li>• Credit check</li> <li>• Criminal check</li> <li>• Education history</li> <li>• Substance/alcohol abuse</li> <li>• Citizenship</li> <li>• Foreign travel</li> <li>• Foreign relatives</li> <li>• Foreign investments</li> <li>• Foreign co-habitants</li> <li>• Organization affiliation</li> <li>• Intelligence service affiliation</li> </ul>
Ongoing Assessments	<ul style="list-style-type: none"> <li>• Personnel reporting</li> <li>• Peer observation</li> <li>• Supervisor assessment</li> <li>• Medical surveillance</li> </ul>	<ul style="list-style-type: none"> <li>• Hands-on mentorship</li> <li>• Monitor health and well-being</li> </ul>	<ul style="list-style-type: none"> <li>• Mentor assessment</li> <li>• Technical assessment</li> </ul>	<ul style="list-style-type: none"> <li>• Behavioral evaluations</li> </ul>

## Non-defense Institutions

Compliance with security-centric federal regulations has driven the establishment of personnel security programs at non-defense institutions (research institutions whose mission is *not* national defense.). These programs have been socialized within institutions through the promotion of a culture of reliability, shared responsibility, and laboratory safety, in addition to compliance. This approach often shifts the focus towards the health and well-being of individual researchers and organizations, and away from security-driven rules.

Recent efforts have focused on linking biosafety to personnel security because biological safety measures are a critical component of academic research programs. The focus of this approach is ensuring scientists can work with hazardous materials and sensitive information competently and reliably. One biosafety practice used in several scientific institutions is the voluntary, “non-punitive” opting out of laboratory work by scientists and research staff who are ill or are otherwise indisposed.

Although safety is only one element of a multi-faceted personnel security program, many non-defense institutions identified their Biological Safety Offices as the having primary responsibility over program development and implementation. However, institutional human resource and general counsel offices are also critically important stakeholders in personnel security and often underutilized. They initiate review of the eligibility and hiring potential of prospective employees and are involved in any employment and labor law issues that might arise during employment. A significant challenge can be in accessing information about prospective employees, particularly since equal opportunity and employment laws vary from state to state and could limit the types of questions asked and/or where or how information is accessed. Additionally, real and perceived liabilities limit the type and quality of information available from previous employers and references, especially for non-U.S. citizen applicants.

The use of Facebook and other social media in hiring decisions is strongly discouraged, if not outright forbidden, in part because affiliations stated on social media sites might not accurately reflect or predict intent or action.

Despite these limitations, hiring officials have been able to learn a lot about prospective employees by inquiring about gaps in their education and work history; assessing their attitudes and behavior in response to certain types of questions, such as "how would you conduct studies with animals?" or "have you performed the job tasks before?"; or paying attention to the types of questions the interviewee asks.

Efforts are being made to provide and increase awareness of employee health and wellness programs, which might include psychological support and evaluations. Employee health and wellness programs could help identify and address potential problems, such as negligence or intentionally harmful behavior. Furthermore, efforts have been undertaken to improve awareness and education of institutional policies, and stress that everyone is responsible for ensuring safety, security, and competency.

The role that scientific responsibility - which includes integrity, ethics, quality, and professionalism - plays in personnel security is a topic of debate among scientific and security experts. The debate centers on the validity of correlating violations of scientific responsibility with personnel security risks. However, the NSABB noted examples of sabotage when deliberating about personnel reliability with restricted pathogens and

toxins. In addition, they explicitly stated that “there is value in assessing prior work history and performance as a predictor of future conduct.”<sup>11</sup>

One recent example of a potential lapse in integrity might involve scientists who accept money to republish scientific articles with joint affiliations or overstate their results to attract funding.<sup>12</sup> These scientists might be susceptible to individuals or groups who pay for information or laboratory materials. Though not a violation of integrity, not informing relevant institutional officials about foreign collaborators might increase the risk that information, materials, or technologies could be inappropriately taken. Directed studies that examine whether scientific responsibility could contribute to personnel security would help resolve current disagreements.

Finally, non-defense industrial companies use mock interviews to train employees on how to recognize and defend against attempts by competing companies to gather information, implicitly and explicitly, about research and development initiatives.

## Defense Institutions

Since the mid-20<sup>th</sup> Century, the weapons and defense-oriented industries have used personnel security programs and procedures to vet new hires and monitor existing employees. In these facilities, the focus on personnel security is on mitigating potential vulnerabilities of staff from influence by external groups or individuals, and internal security breaches. A focus on scientific responsibility has long been a part of personnel security programs in the defense sector. Programs are designed to increase awareness among their scientific and support staff about individuals and groups that might seek access to restricted materials and information, and common approaches used to gain this access.

In defense institutions, the Security Office often holds sole responsibility for personnel security (unless the institution includes laboratory components) (Table 1). An independent review board that works in conjunction with the Security Office may be assembled to evaluate personnel reliability. Pre-employment screening is usually very extensive at defense institutions because protection of sensitive national security information is paramount. In addition, the likelihood that behavioral and psychological evaluations are conducted as part of an on-going assessment program is high; however, their use is not standardized throughout the defense sector.

---

<sup>11</sup> National Science Advisory Board for Biosecurity. Guidance for Enhancing Personnel Reliability and Strengthening the Culture of Responsibility: A Report of the National Science Advisory Board for Biosecurity. (2011). Available at: [http://oba.od.nih.gov/biosecurity/pdf/CRWG\\_Report\\_final.pdf](http://oba.od.nih.gov/biosecurity/pdf/CRWG_Report_final.pdf). Accessed on October 10, 2013.

<sup>12</sup> AAAS, AAU, APLU, FBI. Bridging Science and Security for Biology Research: Institutional Science and Security Workshop Report. 2012. Available at <http://www.aaas.org/report/bridging-science-and-security-biological-research>. Accessed at February 24, 2014.

## Psychological Assessments

The inclusion of behavioral and psychological assessments can be helpful if used correctly. Programs that incorporate these assessments could offer employees the opportunity to discuss their problems or concerns openly and in a non-punitive manner. Defense and non-defense institutions that have successfully implemented these programs have often cited the need to communicate their importance, engender trust between the employee and the designated institutional official (e.g., psychiatrist or psychologist), and encourage employees to seek medical help if needed. However, heavy reliance on psychological assessments to evaluate personnel suitability is problematic in several ways:

1. Specific psychological disorders, with the exception of certain personality disorders, have not been definitively correlated with increased risk of a specific type of threat. With no scientific evidence, the characteristics with which to screen individuals are not known. The baseline occurrence of psychological disorders in employees in different workforce groups is not known. Therefore, the presence of certain conditions in the scientific population is not informative.
2. Screening for risk factors based on known threats will result in a large number of individuals inappropriately identified as risks (i.e., false positives) because the incidence of personnel security threats is low.
3. Testing for psychological disorders “will be minimally effective and maximally intrusive”<sup>13</sup> because it could identify and exclude individuals who are otherwise suitable and reliable for the job. In addition, these tests could deter qualified, trustworthy individuals from joining a research program or organization because they do not want to share their medical histories with their employers.
4. Even if individual risk factors could be identified, risk assessments to predict violent behavior involve real-time (rather than periodic) evaluation, inclusion of “environmental and situational variables, and historic and dynamic risk factors.”<sup>14</sup>

## Underlying Approach

While some institutions have implemented personnel security programs that address specific compliance requirements, others have implemented broader institution-wide programs that comply with federal regulations and address other imminent threats. Some programs that were implemented well before the passage of federal personnel security regulations for cesium irradiators, chemical hazards, and Biological Select Agents and Toxins had to be revised to meet the new requirements. These revisions proved somewhat challenging for institutions, especially those that spent years (even decades) refining their personnel security programs to comply with Department of Defense requirements (see Appendix 4 for Army Regulation 50-1), secure primate research centers, or safeguard information at Veterans Affairs medical centers.

---

<sup>13</sup> Schouten, R. Meeting Presentation.

<sup>14</sup> Schouten, R. Meeting Presentation.

Personnel security programs need to reinforce mutual responsibility and a "culture of caring" that promote a positive research environment.

---

*"Keep your eyes open.  
We're all in this together."*

---

Stakeholders common to all institutions are the researchers, human resource managers, general counsel, occupational health and safety staff, environmental health and safety staff, and security forces, which might include security guards, campus police, local law enforcement, the FBI, or the Joint Terrorism Task Force.

The composition of other relevant stakeholders depends on the mission of the institution - i.e., whether its primary missions are for-profit or non-profit, education and/or research, diagnostic and health care, or defense/national security. For example, at universities and colleges where students and staff have access to sensitive or restricted/controlled materials (e.g., students, faculty, and staff with access to Biological Select Agents and Toxins laboratories), student conduct offices, counseling centers, and health centers might be part of the stakeholder community. In addition, institutions might consider employee assistance programs as relevant stakeholders.

## **Effectiveness of Personnel Security Programs**

Measuring the effectiveness and success of most security programs is extremely challenging. However, possible metrics could include prevention/mitigation of threatening actions; the number of students/staff involved in sensitive or restricted/controlled research; continued stakeholder interest in addressing personnel security; increased reporting of issues or infractions; and the iterative improvement of personnel security programs based on lessons learned.

# Conclusions

---

Institutions must maintain a balance between preserving scientific openness and implementing policies to prevent insider and external threats. Preventive measures include procedures for vetting and assessing employees and practices to prevent inadvertent sharing of information or materials with individuals having malicious intent. Although implementing procedures to vet and continually assess staff for their reliability and trustworthiness is difficult, these procedures are necessary to minimize security risks associated with personnel vulnerabilities. However, the characteristics and behaviors that might raise security concerns might be the same as those that enhance creativity and risk-taking in research; personnel security programs that take this into account could be implemented and accepted in the broader, non-defense scientific community.

The cost of designing and implementing personnel security programs is high - both financially and in employee trust and confidence. Much of the problems with trust and confidence at institutions stem from a lack of authoritative resources on vetting and evaluating personnel, and a fundamental lack of awareness and appreciation of the threats and potential consequences which ensue from a breach in security. Without these resources, administrators and responsible officials struggle to identify the most relevant information on which to base their evaluations. If not developed carefully, these programs could inadvertently cause a decrease in qualified and capable staff who can conduct research involving sensitive materials or research animals, or drive scientists to become security risks themselves.

Development, implementation, and acceptance of personnel security programs relies on cooperative partnerships among all relevant offices and stakeholders at an institution; high-level support of institutional and laboratory leadership; and the promotion of mutual ownership and development among stakeholders. Programs that improve iteratively as lessons are learned, encourage open communication and trust between all institutional stakeholders, and incorporate an appeals process will be successful in non-defense and defense institutions. Finally, sharing of effective practices on personnel security between research institutions could help standardize practices and defray the current costs in establishing and maintaining personnel security programs.

# Appendix 1:

## Meeting Agenda

---

### **BRIDGING SCIENCE AND SECURITY FOR BIOLOGICAL RESEARCH: Personnel Security Programs**

August 21-22, 2013  
Washington, DC

#### **Agenda**

##### **Day 1**

Location: Woodward Bernstein Room  
2<sup>nd</sup> Floor, Donovan House, 1155 14<sup>th</sup> Street, N.W., Washington, DC 20005

6:30pm – 9:00pm      **Reception and Dinner**

7:30pm – 8:30pm      **Dinner Speaker**

*The dinner session is designed to encourage active discussion among speakers about the meeting topic. The speaker will discuss personnel reliability and suitability in the context of an active research environment.*

Welcome: *Norman Neureiter*, American Association for the Advancement of Science

Speakers: *Ronald Schouten*, Massachusetts General Hospital

##### **Day 2**

Location: AAU Conference Room  
5<sup>th</sup> Floor, 1200 New York Ave., NW, Washington, DC 20005

8:00am – 8:30am      **Registration and Breakfast**

8:30am - 8:45am      **Welcome**

8:45am – 10:30am      **Personnel Security: What Personnel Suitability Programs Intend to Address**

*This session will focus on the basic concepts of personnel suitability and compare federal requirements for personnel security. In addition, speakers will discuss the influencing and*

*facilitating risk factors that contribute to personnel suitability, including elicitation, co-option, personal vulnerabilities, and/or other factors.*

Moderator: *Supervisory Special Agent Edward You*, Federal Bureau of Investigation

Panelists: *David Relman, M.D.*, Stanford University  
*David L. Wynes, Ph.D.*, Emory University  
*Chief Linda Stump*, University of Florida  
*Dan Klug*, Arizona State University  
*Alina Bloom*, Sandia National Laboratory  
*TBD*, Pfizer Corporation

10:30am – 11:00am **Break**

11:00am – 12:00pm **Example Suitability Programs**

*This session will focus on existing personnel suitability programs, including the factors taken into account, policies implemented, and procedures developed to address personnel security concerns. This session will include a discussion about security of information and intellectual property.*

Moderator: *Carrie Wolintez*, Association of American Universities

Panelists: *Leon C. Igras*, Arizona State University  
*Dee Zimmerman*, University of Texas, Medical Branch  
*Casey Skvork*, National Institute of Health  
*J. Patrick Fitch*, National Biodefense Analysis and Countermeasure Center  
*Bill VanSchalkwyk*, Massachusetts Institute of Technology and Lincoln Laboratory  
*Susan Wyatt Sedwick*, University of Texas, Austin

12:00pm – 12:30pm **Lunch Break**

12:30pm – 2:00pm **Example Suitability Programs (continued...)**

*This session will focus on existing personnel suitability programs, including the factors taken into account, policies implemented, and procedures developed to address personnel security concerns.*

Moderator: *Carrie Wolintez*, Association of American Universities

Panelists: *Leon C. Igras*, Arizona State University  
*Dee Zimmerman*, University of Texas, Medical Branch  
*Casey Skvork*, National Institute of Health

*J. Patrick Fitch*, National Biodefense Analysis and Countermeasure Center  
*Bill VanSchalkwyk*, Massachusetts Institute of Technology and Lincoln Laboratory  
*Susan Wyatt Sedwick*, University of Texas, Austin

2:00pm – 2:30pm      **Break**

2:30pm– 5:00pm      **Working Session: Facilitated Discussion on Personnel Security**  
*During this session, the facilitators will engage all participants in discussion about the risks and threats faced regarding personnel issues, possible and feasible risk mitigation strategies, and other relevant questions to identify the key concepts on which institutions could consider developing a personnel security program.*

Facilitators: *Bob Hayes*, The Security Executives Council  
*Kavita M. Berger*, American Association for the Advancement of Science  
*Carrie Wolinetz*, Association of American Universities  
*Supervisory Special Agent Edward You*, Federal Bureau of Investigation

5:00pm      **Adjourn**

## Appendix 2: Meeting Participants

---

Sawkat Anwer, Ph.D., DMVH  
Distinguished Professor and Associate Dean  
for Research  
Tufts University, Cummings School of  
Veterinary Medicine  
[Sawkat.Anwer@tufts.edu](mailto:Sawkat.Anwer@tufts.edu)

Charles Bailey, Ph.D.  
Executive Director, National Center for  
Biodefense and Infectious Diseases  
George Mason University  
[cbailey2@gmu.edu](mailto:cbailey2@gmu.edu)

Alina R. Bloom, MIPP  
Counterintelligence Officer  
Sandia National Laboratories  
[arbloom@sandia.gov](mailto:arbloom@sandia.gov)

Marissa M. Cardwell, Ph.D.  
Assistant to the Director Biosafety Program  
Massachusetts Institute of Technology  
[cardwell@mit.edu](mailto:cardwell@mit.edu)

Leo M. Chalupa, Ph.D.  
Vice President for Research  
George Washington University  
[lmchalupa@gwu.edu](mailto:lmchalupa@gwu.edu)

Robert Davey, Ph.D.  
Professor  
Texas Biomedical Research Institute  
[rdavey@txbiomed.org](mailto:rdavey@txbiomed.org)

Patricia L. Donini  
Employee Relations Director/Deputy  
Director HR/Payroll  
George Mason University  
[pdonini@gmu.edu](mailto:pdonini@gmu.edu)

Denise Donnelly  
Assistant Biosafety Officer, ARO; CHMM  
University of Colorado Denver  
[DENISE.DONNELLY@ucdenver.edu](mailto:DENISE.DONNELLY@ucdenver.edu)

Susan Ehrlich, J.D., LL.M. (Biotechnology  
and Genomics)  
Judge (ret.)  
Arizona Court of Appeals  
[ehrlich\\_sa@cox.net](mailto:ehrlich_sa@cox.net)

Pat Fitch, Ph.D.  
Director  
National Biodefense Analysis and  
Countermeasures Center  
[joseph.fitch@nbacc.dhs.gov](mailto:joseph.fitch@nbacc.dhs.gov)

Russell Furr, MPH, CIH  
Director, Environmental Safety  
University of Maryland  
[furr@umd.edu](mailto:furr@umd.edu)

David Gillum, M.S., RBP  
Associate Director, Environmental Health  
and Safety  
Arizona State University  
[David.Gillum@asu.edu](mailto:David.Gillum@asu.edu)

Kimberly Glasgow  
Applied Physics Laboratory  
Johns Hopkins University

Bob Hayes  
Managing Director  
The Security Executives Council  
[bhayes@secleader.com](mailto:bhayes@secleader.com)

Jacki Higgins, MFS  
Certifying Official  
National Biodefense Analysis and  
Countermeasures Center  
HigginsJ@nbacc.net

Cheri Hildreth  
Director, Environmental, Health and Safety  
University of Louisville  
cheri.hildreth@louisville.edu

Deborah Howard, M.P.H., CBSP  
Biological Safety Manager  
University of North Carolina, Chapel Hill  
dmhoward@ehs.unc.edu

Leon C. Igras, MS  
Director, Environmental Health and Safety /  
CDC Responsible Official  
Arizona State University  
leon.igras@asu.edu

Joe Kanabrocki, Ph.D.  
Assistant Dean for Biosafety  
University of Chicago  
jkanabro@bsd.uchicago.edu

Dan Klug  
Director, Recruitment & Selection  
Arizona State University  
daniel.klug.1@asu.edu

Mary Beth Koza, MBA  
Director, Environmental Health and Safety,  
Responsible Official CDC Select Agent  
Program  
University of North Carolina, Chapel Hill  
mbkoza@ehs.unc.edu

Janel Labor  
Special Agent  
Federal Bureau of Investigation  
Janel.Lobur@ic.fbi.gov

Gary Landucci  
Director of BSL3 Training and  
Development  
University of California, Irvine  
g.landucci@uci.edu

Boris Lazic, M.S.  
Director of Human Resources  
Boston University  
blazic@bu.edu

James LeDuc, Ph.D.  
Director, Galveston National Laboratory  
Professor, Microbiology and Immunology  
University of Texas Medical Branch  
jwleduc@utmb.edu

Rachel Levinson, Ph.D.  
Director, National Research Initiatives  
Arizona State University  
Rachel.Levinson@asu.edu

Kathryn Mellouk, MPA  
Interim Associate Vice President for  
Research Compliance  
Boston University  
kateski@bu.edu

Norman Neureiter  
Director, Center for Science, Technology  
and Security Policy  
American Association for the Advancement  
of Science  
nneureit@aaas.org

Victor P. Pantusa, M.S.  
Director EHS, Responsible Officer  
Texas Biomedical Research Institute  
vpantusa@txbiomed.org

Susan Piguet  
Elizabeth R. Griffin Foundation  
piguetsc@gmail.com

Nichole Proctor  
Program Manager  
Office of Safety and Security  
The George Washington University  
[nproctor@gwu.edu](mailto:nproctor@gwu.edu)

David Relman  
Professor and Co-Director of CISAC  
Stanford University  
[relman@stanford.edu](mailto:relman@stanford.edu)

Ronald Schouten, M.D., J.D.  
Director, Law & Psychiatry Service  
Massachusetts General Hospital  
[rschouten@partners.org](mailto:rschouten@partners.org)

David H. Silberman  
Director, Health and Safety Programs  
Stanford University  
[silberman@stanford.edu](mailto:silberman@stanford.edu)

Diann Stedmann  
Biosafety Manager and Responsible Official  
George Mason University  
[dstedman@gmu.edu](mailto:dstedman@gmu.edu)

Linda Stump  
Chief of Police  
University of Florida  
[lstamp@ufl.edu](mailto:lstamp@ufl.edu)

Benn Tannenbaum, Ph.D.  
Sandia National Laboratories  
[bhtanne@sandia.gov](mailto:bhtanne@sandia.gov)

Joanne M. Trujillo  
Personnel Security Manager

Sandia National Laboratories  
[jmtruji@sandia.gov](mailto:jmtruji@sandia.gov)

Jay Walsh, Ph.D.  
Vice President for Research, Professor  
Biomedical Engineering  
Northwestern University  
[jwalsh@northwestern.edu](mailto:jwalsh@northwestern.edu)

Susan Weekly  
President  
Biosafety Professionals, LLC  
[sweekly@biosafetyprofessionals.com](mailto:sweekly@biosafetyprofessionals.com)

Zachary Wilson, MS  
Biosafety Specialist  
University of Colorado Denver  
[Zachary.Wilson@ucdenver.edu](mailto:Zachary.Wilson@ucdenver.edu)

Susan Wyatt Sedwick, Ph.D., CRA  
Associate Vice President for Research and  
Director, Office Sponsored Projects  
The University of Texas at Austin  
[sedwick@austin.utexas.edu](mailto:sedwick@austin.utexas.edu)

David Wynes, Ph.D.  
Vice President for Research Administration  
Emory University  
[dwynes@emory.edu](mailto:dwynes@emory.edu)

Domenica Zimmerman  
Lead Biosafety Officer  
University of Texas Medical Branch  
[dzimmerm@UTMB.EDU](mailto:dzimmerm@UTMB.EDU)

# Appendix 3:

## Federal Select Agent Program

---

The Federal Select Agent Program (FSAP) is jointly comprised of the Centers for Disease Control and Prevention/Division of Select Agents and Toxins (CDC/DSAT) and the Agriculture Select Agent Services (AgSAS; formally known as the Animal and Plant Health Inspection Services (APHIS)) within the U.S. Department of Agriculture.<sup>15</sup> The Federal Select Agent Program works closely with Department of Justice's Federal Bureau of Investigation, Criminal Justice Information Service (CJIS) to identify those individuals who are prohibited from access to Select Agents and Toxins based on the restrictions identified in the USA PATRIOT Act. CJIS conducts a Security Risk Assessments (SRA) of all individuals, Responsible Officials, Alternate Responsible Officials, and non-governmental entities that request access to select agents and toxins. The Federal Select Agent Program authorizes access to Select Agents and Toxins based on the results of the SRA.

An SRA is required for all individuals who have access to select agents or toxins and is valid for three years unless terminated sooner by the CDC, AgSAS, or the employer. The SRA is tied to the entity for which the individual works; it cannot be transferred if she or he moves to another BSAT facility.

The FSAP requires registration of facilities including government agencies, universities, research institutions, and commercial entities that possess, use or transfer biological agents and toxins that pose a significant threat to public, animal or plant health, or to animal or plant products.

An individual is considered a “*restricted person*” under the USA PATRIOT Act if he or she:

- Is under indictment for a crime punishable by imprisonment for a term exceeding one year or has been convicted in any court of a crime punishable by imprisonment for a term exceeding one year;
- Has received a dishonorable discharge from the U.S. military. This provision ensures that those who commit comparable crimes while in the military will also be denied access to BSAT materials;
- Is a fugitive from justice;
- Is an unlawful user of any controlled substance (as defined in section 102 of the Controlled Substances Act<sup>16</sup>);

---

<sup>15</sup> Select Agents Regulations. Available at <http://www.selectagents.gov/Regulations.html>. Accessed on February 24, 2014.

<sup>16</sup> <http://www.fda.gov/RegulatoryInformation/Legislation/ucm148726.htm>

- Has been adjudicated as a mental defective or has been committed to any mental institution. The prohibition is based on specific legal distinctions that make this a small category of individuals;
- Is an alien illegally or unlawfully in the United States; or
- Is an alien (other than an alien lawfully admitted for permanent residence) who is a national of a country that has repeatedly provided support for acts of international terrorism. This is operationalized as nationals of countries formally designated as state sponsors of terrorism. Currently there are four such countries: Cuba, Iran, Sudan, and Syria.

Additionally, under the Bioterrorism Preparedness Act<sup>17</sup>, an individual could not have access to select agents if he or she is “*reasonably suspected*” by any federal law enforcement or intelligence agency of:

- Committing a federal crime of terrorism;
- Having a knowing involvement with an organization that engages in domestic or international terrorism or with any other organization that engages in intentional crimes of violence; or
- Being an agent of a foreign power.

The assessment of whether an individual has any of these disqualifying factors is based on responses to questions on the SRA application (FBI Form FD-961<sup>18</sup>) along with a fingerprint check and a search of a wide range of federal databases to identify disqualifying background/activities.

---

<sup>17</sup> <http://www.fda.gov/RegulatoryInformation/Legislation/ucm148797.htm>

<sup>18</sup> <http://www.fbi.gov/about-us/cjis/bioterrorism-security-risk-assessment-form/bioterrorfd961>

# Appendix 4:

## Army Biosurety Program

---

Following the events of 2001, the U.S. Army began establishing policies and regulations, specifically Army Regulation 50-1, in order to govern research involving BSAT. Under this surety program, it became Army policy that BSAT in the possession or custody of the Army shall be properly safeguarded against theft, loss, diversion, or unauthorized access or use, and that operations with such agents are conducted in a safe, secure, and reliable manner. The key element to the program is the Biological Personnel Reliability Program (BPRP).

PRP is one of the cornerstones of several of the Army's Surety Programs and ensures only those personnel who have demonstrated the highest degree of individual reliability for allegiance, trustworthiness, conduct, behavior, and responsibility will be allowed to perform duties that meet the criteria established for surety duties. The purpose of the PRP is to ensure that each person who performs duties involving Special Nuclear Material, Chemical, and Biological agents meets the highest possible standards of reliability due to the serious nature or lethal characteristics of the material.

In April 2009, the latest Army Biosurety Program, established in Army Regulation 50-1, came into effect.<sup>19</sup> It is based on the recommendations from the 2001 Inspector General review of Army biological laboratories and the existing chemical surety program, as per Army Regulation 50-6 in addition to implementing DOD Instruction 5210.89, Minimum Security Standards for Safeguarding Biological Select Agents and Toxins. The BPRP is implemented in conjunction with federal requirements for select agent registration and FBI Security Risk Assessment and acts as a tool for commanders/directors to make risk-based assessment decisions in order to ensure persons with access to BSAT meet high reliability standards.

“The BPRP includes—

- (1) Identifying positions with duties that afford access to BSAT.
- (2) Designating certifying officials who will certify the reliability and suitability of individuals for the BPRP(described below).
- (3) Screening, evaluating, and certifying individuals for the BPRP.
- (4) Continuing evaluation in the form of periodic reinvestigations (PR), drug tests, and evaluation by supervisors, fellow workers, certifying officials, and support agency personnel, as well as self-reporting by individuals enrolled in the BPRP.
- (5) Removing an individual from BPRP duties due to medical restriction, suspension, disqualification, or administrative termination.
  - b. Explosive ordnance disposal (EOD) and mishap/incident response personnel are not required to meet the reliability standards of this chapter and will be

---

<sup>19</sup> Army Biosurety Program. Available at [http://www.apd.army.mil/pdffiles/r50\\_1.pdf](http://www.apd.army.mil/pdffiles/r50_1.pdf). Accessed on February 24, 2014.

- given access to BSAT only to the extent necessary to mitigate or eliminate a hazard during an emergency.
- c. Requests for access by foreign nationals to BSAT under authorized visits, assignments or exchanges will be processed in accordance with DOD Directive 5230.20, AR 380–10, and DOD 5200.2-R.
  - d. To ensure compliance with the Privacy Act of 1974 and AR 340–21, all personnel who wish to be considered for assignment to BPRP duties must grant authority for release of information and records to allow the certifying official and other authorized officials to receive and review medically potentially disqualifying information, and to review personnel and security files. If an individual does not grant permission for the records check and review, that person is not eligible for BPRP duties. (Exception: Eligibility for BPRP duties will not be affected if DOD contractor and government civilian employees decline to provide written consent to release drug/substance or alcohol abuse information. See paragraph 2–13b).
  - e. At facilities or installations where individuals may be in multiple personnel reliability programs (for example, the biological and chemical PRP), separate screening is not required for each program. Written local procedures will address PRP processing for such individuals, to include addressing any program differences and training requirements specific to each program. Procedures for transferring between PRP programs are covered in paragraph 2–1.
  - f. An individual who is certified in another DOD PRP can be accepted into the BPRP at the discretion of the facility commander/director.
  - g. Commanders/directors may authorize escorted and/or supervised access to BSAT for individuals who are not in the BPRP but who have a favorably-adjudicated personnel security investigation (PSI) per paragraphs 2–12b and 2–12c and who meet the requirements of paragraph 2–1h. Only BPRP-certified persons can conduct the escort/supervision.
  - h. Any individual who requires access to BSAT as defined in paragraph 2–2a, must first have valid approval based on a security risk assessment per Title 42, Code of Federal Regulations, Part 73 (42 CFR 73), 7 CFR 331, or 9 CFR 121.

### **Mandatory disqualifying factors**

The certifying official will disqualify individuals from the BPRP when any of the traits, diagnoses, conditions, or conduct listed below exists. The certifying official will submit disqualification actions to the reviewing official for review. If, during this review, the reviewing official discovers extraordinary circumstances that warrant an exception to disqualification, he or she may submit a request through Army Command channels to HQDA, ODCS G–3/5/7, ATTN: DAMO–SSD. The individual remains disqualified until and unless the exception is approved.

- a. Current diagnosis of drug/substance or alcohol dependence based on a determination by an appropriate medical authority in accordance with the current Diagnostic and Statistical Manual of Mental Disorders (DSM) of the American Psychiatric Association.

- b. Drug/substance abuse within the five years previous to the initial BPRP interview. Certifying officials having any doubt on the status of a certain drug as illegal or controlled should consult the CMA, local law enforcement officials, or the supporting legal office. Exceptions: isolated incidents of use of another person's prescribed drug, self-medication exceeding the recommended safe dosage on the medication's packaging of over the counter substances, or improper use of an individual's own prescribed medications will be evaluated per paragraph 2–8 of this regulation.
- c. Trafficking in illegal or controlled drugs as well as cultivating, processing, or manufacturing illegal or controlled drugs within the last 15 years.
- d. Drug/substance abuse while enrolled in the BPRP, whether admitted or as the result of a verified positive drug test. Exceptions: isolated incidents of use of another person's prescribed drug, self-medication exceeding the recommended safe dosage on the medication's packaging of over the counter substances, or improper use of an individual's own prescribed medications will be evaluated per paragraph 2–8 of this regulation.
- e. Inability to meet safety requirements, such as unable to correctly wear personal protective equipment required for the assigned position, other than temporary medical conditions. Questions regarding the duration of medical conditions will be referred to the CMA.
- f. Meeting the criteria of a Restricted Person.

*Note.* For individuals requiring Centers for Disease Control and Prevention (CDC) or Animal and Plant Health Inspection Service (APHIS) registration for access to BSAT, such registration is sufficient determination that the individual is not a restricted person.

#### **Other disqualifying factors**

Any of the following traits, diagnoses, conditions, or conduct listed below may be grounds for the disqualification of an individual from the BPRP, based on the certifying official's informed judgment.

- a. *Alcohol-related incidents/abusing alcohol.*
  - (1) Certifying officials will evaluate the circumstances of alcohol-related incidents that occurred in the five years prior to the initial interview and request a medical evaluation. An individual diagnosed through such medical evaluation as currently alcohol-dependent will be disqualified per paragraph 2–7a. Individuals diagnosed as abusing alcohol will be handled per paragraph (2) below. For an individual not diagnosed as a current alcohol-dependent/abusing alcohol, including those individuals identified as recovering alcoholics, the certifying official will determine reliability based on results of the investigation, the medical evaluation, and any extenuating or mitigating circumstances (such as successful completion of a rehabilitation program). The certifying official will, as appropriate, then qualify or disqualify the individual from the BPRP.
  - (2) Individuals diagnosed as abusing alcohol but who are not alcohol-dependent shall, at a minimum, be suspended from BPRP processing pending completion of the rehabilitation program or treatment regimen prescribed by the CMA. Before the

individual is certified into the program, the certifying official will assess whether the individual has displayed positive changes in job reliability and lifestyle, and whether the individual has a favorable medical prognosis from the CMA and a psychological evaluation is completed. The individual will complete a 1 year period of strict compliance with an aftercare program. Failure to satisfactorily meet these requirements shall result in disqualification.

*b. Drug/substance abuse.*

- (1) In situations not otherwise addressed in paragraph 2-7b, a certifying official may qualify or disqualify an individual who has abused drugs/substances more than five years before the initial PRP interview. In deciding whether or not to disqualify individuals in these cases, the certifying official will request CMA evaluation and may consider extenuating or mitigating circumstances. To qualify the individual for the BPRP, the certifying official's documentation of the PDI (para 2-15a) must include an approval signed by the reviewing official. If the reviewing official does not approve, the individual will be disqualified from the BPRP (para 2-26). Examples of potential extenuating or mitigating circumstances include, but are not limited to—
  - (a) Successful completion of a drug rehabilitation program.
  - (b) Participation in a twelve-step program.
  - (c) Isolated experimental drug abuse.
  - (d) Age at the time of the drug abuse ("youthful indiscretion").
- (2) Certifying officials may qualify or disqualify individuals who have isolated episodes of use of another's prescription drugs, or who, in an effort to self-medicate, inadvertently or deliberately exceed the recommended safe dosage on the medication's packaging of over the counter substances, or who improperly use their own prescribed medications.
  - (a) If the use occurred while the individual was enrolled in the BPRP, the certifying official will request CMA evaluation. If the certifying official believes the use does not represent a reliability concern and desires to retain the individual in the BPRP, the documentation recording the PDI (para 2-15a) must include an approval signed by the reviewing official. If the reviewing official does not approve, the individual will be disqualified from the BPRP (para 2-26).
  - (b) If the abuse occurred within 15 years before the initial BPRP interview, the certifying official will request CMA evaluation. Certifying officials will consider such abuse in conjunction with other PDI in determining reliability of the individual.

*c. Medical condition.*

- (1) Any significant mental or physical medical condition, medication usage, or medical treatment, which may result in—
  - (a) An altered state of consciousness.
  - (b) Impaired judgment or concentration.
  - (c) Increased risk of impairment if exposed to biological agents.
  - (d) Impaired ability to safely wear personal protective equipment required for the biological surety position, or

- (e) Inability to perform the physical requirements of the biological surety position, as substantiated by a CMA to the certifying official.
- (2) Medical information that falls within these parameters is disqualifying if and when the certifying official considers it prejudicial to reliable performance of BPRP duties.
- (3) The CMA will evaluate individuals and make recommendations to the certifying official on suitability for duty in the BPRP for individuals currently under treatment with hypnotherapy.
- (4) The CMA will obtain a mental health assessment, evaluate individuals, and make recommendations to the certifying official on suitability for duty in the BPRP for individuals who have attempted or threatened suicide before entry into the BPRP or while enrolled in the BPRP. To qualify individuals who have attempted or threatened suicide while enrolled in the BPRP, the certifying official's documentation of the PDI (para 2–15a) must include an approval signed by the reviewing official.
- d. *Inappropriate attitude, conduct, or behavior.* In determining reliability, the certifying official will conduct a careful and balanced evaluation of all aspects of an individual. Specific factors to consider include, but are not limited to—
- (1) Negligence or delinquency in performance of duty.
- (2) Conviction of, or involvement in, a serious incident indicating a contemptuous attitude toward the law, regulations, or other duly constituted authority. Serious incidents include, but are not limited to assault, sexual misconduct, financial irresponsibility, contempt of court, making false official statements, habitual violation of traffic laws, and domestic violence.
- (3) Poor attitude or lack of motivation. Poor attitude can include arrogance, inflexibility, suspiciousness, hostility, flippancy toward BPRP responsibilities, and extreme moods or mood swings.
- (4) Aggressive/threatening behavior toward other individuals.
- (5) Attempting to conceal PDI from certifying officials through false or misleading statements, or by willfully neglecting to report current PDI.

Under the BRPR, disqualifying criteria include:

- Current diagnosis of drug/substance or alcohol dependence
- Drug/substance abuse within 5 years of initial interview (certifying official judgment required if over 5 years);
- Drug trafficking within 15 years of initial interview;
- Drug/substance abuse while enrolled in the PRP;
- Inability to meet safety requirements of the position;
- Medical conditions or treatment that: affect consciousness, judgment, concentration; increase risk from BSAT exposure; impair ability to wear protective equipment; or impair physical ability required for duties; or
- Documented suicide attempts or threats of suicide.

# Appendix 5:

## U.S. Code of Federal Regulations

---

The Federal Select Agent Program, Biological Personnel Reliability Program (BPRP), and other personnel security programs can be traced back to the Office of Personnel Management's (OPM) Code of Federal Regulations Title 5, Chapter I, Subchapter B, Part 731. This document establishes specific criteria and procedures for making determinations of suitability and for taking suitability actions regarding employment in covered positions.<sup>20</sup>

In determining whether a person is suitable for Federal employment, only the following factors will be considered a basis for finding a person unsuitable and taking a suitability action:

- 1) Misconduct or negligence in employment;
- 2) Criminal or dishonest conduct;
- 3) Material, intentional false statement, or deception or fraud in examination or appointment;
- 4) Refusal to furnish testimony as required;
- 5) Alcohol abuse, without evidence of substantial rehabilitation, of a nature and duration that suggests that the applicant or appointee would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of the applicant or appointee or others;
- 6) Illegal use of narcotics, drugs, or other controlled substances without evidence of substantial rehabilitation;
- 7) Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force; and
- 8) Any statutory or regulatory bar which prevents the lawful employment of the person involved in the position in question.

However, OPM and relevant agencies must consider any of the following additional considerations to the extent OPM or the relevant agency, in its sole discretion, deems any of them pertinent to the individual case:

- 1) The nature of the position for which the person is applying or in which the person is employed;
- 2) The nature and seriousness of the conduct;
- 3) The circumstances surrounding the conduct;
- 4) The recency of the conduct;

---

<sup>20</sup> Covered Position refers to a position in the competitive service, a position in the excepted service where the incumbent can be noncompetitively converted to the competitive service, and a career appointment to a position in the Senior Executive Service

- 5) The age of the person involved at the time of the conduct;
- 6) Contributing societal conditions; and
- 7) The absence or presence of rehabilitation or efforts toward rehabilitation.

In accordance with the above, the following criteria are used to determine the risk levels for each position occupied by a federal employee:

- 1) High Risk: High Risk positions have the potential for exceptionally serious impact on the integrity and efficiency of Federal service. These positions involve duties that are especially critical to the agency or the program mission with a broad scope of responsibility and authority.
- 2) Moderate Risk: Moderate Risk positions have the potential for moderate to serious impact on the integrity and efficiency of Federal service. These positions involve duties that are considerably important to the agency or program mission with significant program responsibility or delivery of service.
- 3) Low Risk: Low Risk positions have the potential for limited impact on the integrity and efficiency of Federal service. These positions involve duties and responsibilities of limited relation to the agency or program mission.

Regardless of subject matter (biological, nuclear, chemical, or other) the Code of Federal Regulations provides the foundation to all selection criteria currently implemented in the U.S. regarding personnel reliability, whether implicitly or explicitly. Indeed this is true regardless of whether the role was federal or not and required a security clearance or not since the criteria and framework provide a “*common sense*” approach to any person considered for hire.

# Appendix 6:

## Publications on Personnel Security for Biological Select Agents and Toxins

---

Carr K, Henchal EA, Wilhelmsen C, Carr B. Implementation of biosurety systems in a Department of Defense medical research laboratory, *Biosecur Bioterror*. 2004; 2(1):7-16.

Centers for Disease Control and Prevention and the U.S. Dept. of Agriculture. Guidance for suitability assessments. 2012 Oct.

[http://www.selectagents.gov/resources/Tier\\_1\\_Suitability\\_Guidance\\_version\\_2\\_1.pdf](http://www.selectagents.gov/resources/Tier_1_Suitability_Guidance_version_2_1.pdf).

Centers for Disease Control and Prevention and the U.S. Dept. of Agriculture. Information systems and security control guidance documents. 2012 Oct.

[http://www.selectagents.gov/resources/Information\\_Systems\\_Security\\_Control\\_Guidance\\_version\\_3\\_English.pdf](http://www.selectagents.gov/resources/Information_Systems_Security_Control_Guidance_version_3_English.pdf).

Centers for Disease Control and Prevention and the U.S. Dept. of Agriculture. Security guidance for select agent or toxin facilities. 2012 Oct.

[http://www.selectagents.gov/resources/Security\\_Guidance\\_version\\_2\\_English.pdf](http://www.selectagents.gov/resources/Security_Guidance_version_2_English.pdf).

Higgins JJ, Weaver P, Fitch JP, Johnson B, Pearl RM. Implementation of a personnel reliability program as a facilitator of biosafety and biosecurity culture in BSL-3 and BSL-4 laboratories. *Biosecur Bioterror*. 2013 Jun;11(2):130-7.

NSABB. Guidance for Enhancing Personnel Reliability and the Strengthening of Cultural Responsibility. 2011 Sept. [http://oba.od.nih.gov/biosecurity/pdf/CRWG\\_Report\\_final.pdf](http://oba.od.nih.gov/biosecurity/pdf/CRWG_Report_final.pdf).

Skvorc C and Wilson DE. Developing a behavioral health screening program for BSL-4 laboratory workers at the National Institutes of Health. *Biosecur Bioterror*. 2011 Mar;9(1):23-9.

# Appendix 7:

## Biosecurity/Personnel Security Case Studies

---

The case studies presented here provide insight into personnel reliability and suitability, both from an insider and external threat perspective. Moreover, the cases provide examples of how biological materials were used in the commission of a violent act, misused, or posed as a vulnerability due to access to materials or facilities. Information included in these case studies was taken from public record.

### **Non-violent Insider – Theft, Loss, Diversion or Illegal Possession, Transfer of Dangerous Pathogen**

**Larry Wayne Harris (Fairfield County, OH, 1995):** Harris was a trained molecular biologist, member of several white supremacist organizations including the Idaho-based Aryan Nations, and self-proclaimed biodefense expert. Harris made several grandiose claims and grossly misrepresented his importance to officials and other contacts in order to gain attention and illegally procure dangerous pathogens. He used forged documents to order *Yersinia pestis* (plague). In 1997, Harris pleaded guilty to wire fraud and was sentenced to probation and community service. This event was one of the motivations for the establishment of the Select Agent Program to control access, possession, and transfer of Select Agents and Toxins.

**Denys Hughes (Wichita, KS, 1995):** During a traffic stop by a Sheriff's Deputy, books on bomb making and poisonous plants, multiple firearms, and petri dishes were found in Hughes's vehicle. Hughes was later released with all his items. Consensual searches of Hughes's apartment in Phoenix, AZ led to the discovery of castor plants and seeds, ricin recipes, gunsmithing equipment, and home-made silencers. Another consensual search at a Wisconsin residence uncovered a clandestine manufacturing laboratory that was producing an unknown product. Multiple charges were brought against Hughes and he was sentenced to seven years in prison for attempted production of a biological agent for use as weapon, possession of unregistered destructive device, and possession of unregistered silencer.

**Konan Michel Yao (Pembina, ND, 2009):** Yao was a postdoctoral fellow studying ebola virus and HIV vaccines at the Canadian Public Health Agency's National Microbiology Laboratory in Winnipeg, Manitoba. Yao was to begin a new fellowship position at the U.S. National Institutes of Health in Bethesda, MD, but was stopped by U.S. Customs and Border Protection inspectors at the Pembina, ND port of entry. Inspectors found vials wrapped in aluminum foil inside a glove and packaged in a plastic bag. Yao stole 22 vials containing DNA encoding specific Ebola genes on his last day of work at the National Microbiology Laboratory so he would not have to start his research from scratch once at NIH. Yao was prosecuted for violating U.S. customs statutes.

## **Violent Insider - Use of Biological Agent as a Weapon**

**Sheela Birnstein and Diane Yvonne Onang (Wasco County, OR, 1984):** Birnstein (a.k.a. Ma Anand Sheela, Sheela Silverman, Sheela Ambal Patel) and Onang (a.k.a. Ma Anand Puja) conspired with Bhagwan Shree Rajneesh and other members of the Rajneeshi Cult in 1984 to poison the population of The Dalles, Oregon. The plot was carried out in an effort to influence a local election and reverse a critical land-use determination that prevented the creation of the City of Rajneehpuram in Wasco County. Onang, a nurse practitioner in the Rajneesh Medical Corporation, used her position and title to set up a laboratory, ostensibly for clinical diagnostic work, on the Rajneeshi land. She acquired *Salmonella typhimurium* from American Type Culture Collection. Cultures of *S. typhimurium* were disseminated on foodstuff in salad bars of various restaurants prior to election day. On July 22, 1986, both women entered Alford pleas (the defendant asserts their innocence, but acknowledges that prosecution's presentation of evidence will most likely bring a beyond a reasonable doubt verdict) for the salmonella poisoning and other charges. Birnstein received twenty years for attempted murder, twenty years for first-degree assault, ten years for second-degree assault, four-and-a-half years for her role in the salmonella poisoning, four and a half years for a wiretapping conspiracy, and five years' probation for immigration fraud. Onang received fifteen, fifteen, seven and a half, and four-and-a-half years, respectively, for her role in the first four crimes, as well as three years' probation for a wiretapping conspiracy.

**Brian T. Stewart (St. Charles County, MO, 1992):** Stewart was a phlebotomist at St. Joseph's Hospital West in Lake St. Louis, MO. In February 1992, Stewart infected his 11-month old son with HIV from a used syringe while the child was being treated for asthma and pneumonia. Stewart's motive was to murder the child in order to avoid paying child support in accordance with a court-ordered paternity settlement. The crime did not come to light until the child was diagnosed with HIV in 1996. Stewart was convicted of 1<sup>st</sup> degree assault in 1998 and sentenced to life in prison. According to hospital coworkers and a fellow Illinois National Guardsmen, Stewart, when angry, would threaten to harm people by injecting them with contaminated blood to which he had routine access.

**Dr. Richard J. Schmidt (Lafayette, LA, 1994):** Schmidt was a Louisiana gastroenterologist convicted of 2<sup>nd</sup> degree attempted murder. He used a hypodermic syringe contaminated with HIV and hepatitis, later linked to two specific patients, to deliberately infect a former lover. Schmidt used routine vitamin B-12 injections that he had been giving the victim to treat complaints of fatigue as cover for the final HIV/hepatitis-contaminated injection. During his eight year relationship with the victim, Schmidt confronted and threatened the lives of two men who were known to be lovers of the victim. Schmidt also lied to other health care professionals treating the victim, telling them that he (Schmidt) had tested the victim for HIV with negative results. This was the first time in the United States that prosecutors used forensic evidence linking an infection in a person to a stolen source of an infectious agent to achieve a conviction.

**Dr. Debora Green (Johnson County, KS, 1995):** Green was trained in emergency medicine and later switched to a hematology/oncology specialty. In 1995, Green was charged with the

murder of two of her three children and the attempted murder of the 3<sup>rd</sup> by burning down the house owned by her and her estranged husband, Dr. Michael Farrar. Farrar had threatened to seek custody of their three children during divorce proceedings, citing Green's chronic substance abuse. The subsequent police investigation discovered Green attempted to murder Farrar using ricin, which she purified from castor beans purchased at local garden centers. Pre-trial psychological evaluations revealed Green had a lack of interest in social relationships, tendency towards a solitary lifestyle, secretiveness, emotional coldness, and apathy. Witnesses described her explosive outbursts at minor slights and chronic substance abuse. Green entered an Alford plea at a critical point in the trial and was sentenced to two successive 40-year prison sentences for the murder charges.

**Diane Thompson (Dallas, TX, 1996):** Thompson, a diagnostic laboratory technician at St. Paul Medical Center, sent an anonymous email to coworkers inviting them to eat pastries. The baked goods were contaminated with *Shigella dysenteriae Type II* which Thompson had acquired through her access to the laboratory. The incident resulted in 12 coworkers becoming ill with four having to be hospitalized. In 1995, she gave tainted food to her boyfriend after he attempted to end their relationship. Thompson also used her position to falsify laboratory reports, which prevented the correct diagnosis of the boyfriend's illness. Other violent acts against the boyfriend included the use of a contaminated syringe to take a blood sample and stalking. Thompson pled guilty to four counts of tampering with consumer products and was sentenced to 20 years in prison.

**Bruce Ivins (Frederick, MD, 2001):** Ivins was the primary suspect in 2001 anthrax mailings (Amerithrax case) that involved multiple anthrax-laced letters, 22 infections, and 5 deaths. Ivins was a prominent anthrax researcher, responsible for vaccine development, at the United States Army Medical Research Institute for Infectious Diseases (USAMRIID). Ivins had a significant history of behavioral and psychological disturbances, including criminal offenses. He illegally carried a pistol as an undergraduate and was armed at his thesis defense in graduate school. Ivins started stalking a fellow undergraduate, a member of Kappa Kappa Gamma sorority, after she turned him down. Ivins' stalking behaviors continued at USAMRIID where he targeted two female laboratory technicians, even long after one left USAMRIID. In late April 2002, investigators confronted Ivins about reports that he had furtively tested for anthrax spores in his office and other areas outside the 'hot suites' (the sealed rooms where researchers worked with deadly pathogens). Ivins confirmed the testing and volunteered that he also conducted cleanups in the lab not once but twice—in December 2001, when he bleached over areas he'd found to be contaminated, and again in mid-April, when he conducted a search for errant anthrax spores. These acts violated the lab's standard procedure, which called for the safety office to investigate and clean up any contamination. Ivins committed suicide by an overdose of acetaminophen prior to his arrest.

### **Violent Outsider - Use of Biological Agent as a Weapon**

**Edward Bachner (Illinois, 2008):** Bachner, a personal financial advisor, purchased tetrodotoxin (TTX) online from two pharmaceutical companies to murder his wife. By his own admission and according to associates and family, Bachner had a very elaborate fantasy life and maintained separate lives unknown to his wife. The murder was part of an elaborate scheme to collect on

\$20 million in life insurance benefits. Bachner obtained the insurance policies fraudulently by misrepresenting his and his wife's association with three U.S. corporate entities. To acquire the TTX, Bachner posed as a medical doctor and president of a fabricated research company, EB Strategic Research, in order to make the online purchases. Bachner placed four separate TTX orders. The final order—2 mg below the exempted quantity for possession by an un-registered entity under the U.S. Select Agent Regulations—raised the suspicions of an employee, who notified authorities. Bachner had been the subject of an FBI assessment earlier for internet communications soliciting help in other plans to murder his wife. During searches of his home, investigators recovered several illegal firearms, false CIA credentials, and a “murder manual.” Bachner was sentenced to 7 years and 8 months in federal prison for wire fraud and possession of TTX with intent to use as a weapon [U.S. Code Title 18, Section 175(a)].

### **Violent Insider - Targeting Biomedical Science or Health Care**

**David Kwiatkowski (New Hampshire, 2012):** Kwiatkowski was a radiological technician accused of infecting over 40 hospital surgical patients with hepatitis C, including one patient who died of the infection. Kwiatkowski sustained a habit of drug abuse by stealing syringes with fentanyl and then replacing the used ones refilled with saline and tainted with his own blood. Kwiatkowski worked at ten hospitals over four years in eight states as a subcontracted technician. Misconduct and disciplinary incidents resulted in dismissals from several hospitals, but derogatory information often was not reported to employment agencies, management at new jobs sites, or state licensing bodies. One placement agency falsified an email to make it look as though they had notified state licensing authorities. The failure to act on his trend of drug-related incidents and dismissals represents one of the worst examples of “passing the bad apple.” Kwiatkowski was sentenced to 39 years imprisonment for fraud and tampering with commercial products.

**Dr. Amy Bishop (Huntsville, AL, 2010):** Bishop killed three and wounded six coworkers with a handgun after being denied tenure in the Biology Department at the University of Alabama, Huntsville. Bishop had a history of previous violence. She shot and killed her brother but it was ruled an accident after an incomplete investigation. She attacked a mother with a small child who took the last booster seat, resulting in charges of assault and battery and disturbing the peace. She was questioned in connection with an explosive device sent to her postdoctoral advisor after a dispute. Colleagues described her behavior as abrasive, narcissistic, bizarre, and out of touch with reality. In 2006, several undergraduate students signed a petition asking the Department Chair for her removal, but it did not result in changes. Bishop was sentenced to life imprisonment without the possibility of parole.

**Raymond Clark III (New Haven, CT, 2010):** Clark was a veterinary technician at a Yale University vivarium. He pleaded guilty to the 2009 murder of graduate student Anne Le and entered an Alford plea to the charge of sexual assault. Le was found inside a wall cavity in the basement of the Yale laboratory upside down with indications of sexually assault. It was determined she had been asphyxiated and, among other injuries, her jaw and collarbone were broken before death. Coworkers reported that Clark clashed with researchers about their apparent disregard for animal husbandry protocols. A team leader in the Yale University facility stated several of his researchers complained last year that Clark was rude to them, prompting the team leader to alert Clark’s supervisor. Neighbors and coworkers described Clark as a “control

freak” and having frequent altercations with his fiancée. Clark was sentenced to a prison term of 44 years.

### **Violent Biomedical Science/Health Care Insider – Targeting Outsiders**

**Major Nidal Malik Hasan (Fort Hood, TX, 2009):** Hasan was a U.S. Army psychiatrist who shot and killed 13 and wounded 29 others. Prior to his transfer to Fort Hood, Hasan received poor performance evaluations while stationed at Walter Reed Medical Center. At Walter Reed, colleagues and superiors were deeply concerned about his inappropriate behavior and comments, describing him as disconnected, aloof, paranoid, and belligerent. The behavioral concerns went unreported until after the shooting. The ensuing Court Martial found Hasan guilty on 13 counts of premeditated murder and 32 counts of attempted premeditated murder. Hasan was sentenced to death.

**James Holmes (Arapahoe County, CO, 2012):** Holmes killed 12 and injured 58 in an attack at a movie theater in Aurora, Colorado. Holmes was a graduate student studying neuroscience at the University of Colorado-Anschutz but withdrew shortly after failing to pass his qualifying exams. Over the six months prior to the attack, Holmes prepared extensively by conducting surveillance/planning, building explosive devices, and procuring several firearms. The psychiatrist treating Holmes reported concerns to police and campus threat assessment committee, but no action taken because Holmes withdrew from the graduate program. Holmes texted another student weeks prior to the attack and asked about mental disorders and warned student to stay away from him. Holmes pled not guilty by reason of insanity to more than 16 counts of murder and attempted murder.

**Aafia Siddiqui (Afghanistan, 2008):** Siddiqui, a Pakistani national, studied in the U.S. and received a B.S. in biology from MIT and a Ph.D. in neuroscience from Brandeis University. She was a member of the Muslim Students’ Association at MIT and was introduced to Imam Suheil Laher, a public advocate of jihad, and Abdulla Azzam, a Muslim Brother and Osama bin Laden’s mentor. She and her husband—a Pakistani anesthesiologist who worked at Brigham and Women’s Hospital—left the U.S. after September 11, 2001. Siddiqui’s first marriage ended amid allegations that Siddiqui was physically abused. Siddiqui later married Ammar al-Baluchi, the nephew of Kalid Sheikh Mohammed, the chief planner of the 9/11 attacks. In 2008, Afghan Police detained her and found sodium cyanide and documents describing the creation of explosives, chemical weapons, other weapons involving biological material and radiological agents, and landmarks including the Plum Island Animal Disease Center in her possession. On the second day of her detention, Siddiqui attacked two FBI agents and two U.S. Army officers during an interview. Siddiqui was convicted in New York of attempted murder of U.S. nationals abroad and assault on U.S. officers. She was sentenced to an 86-year prison sentence.

### **Violent Outsider - Targeting Biomedical Science or Health Care**

**Eric Robert Rudolph (Cherokee County, NC, 1998):** Rudolph was responsible for a series of bombings carried out in the name of anti-abortion and anti-gay rights organizations. He was also responsible for the bombing at the Centennial Olympic Park in Atlanta, GA, which resulted in the death of a Birmingham, AL police officer and injured over 100 people. Rudolph pled guilty

to charges, including murder, as part of an agreement to avoid the death penalty. In prior bombings, Rudolph used flattery to befriend young, female temporary employees, new administrative staff, and security guards at clinics. Through these techniques, he obtained information regarding security protocols, functions, and scheduling in order to maximize the injurious effects of the attacks on the clinics.

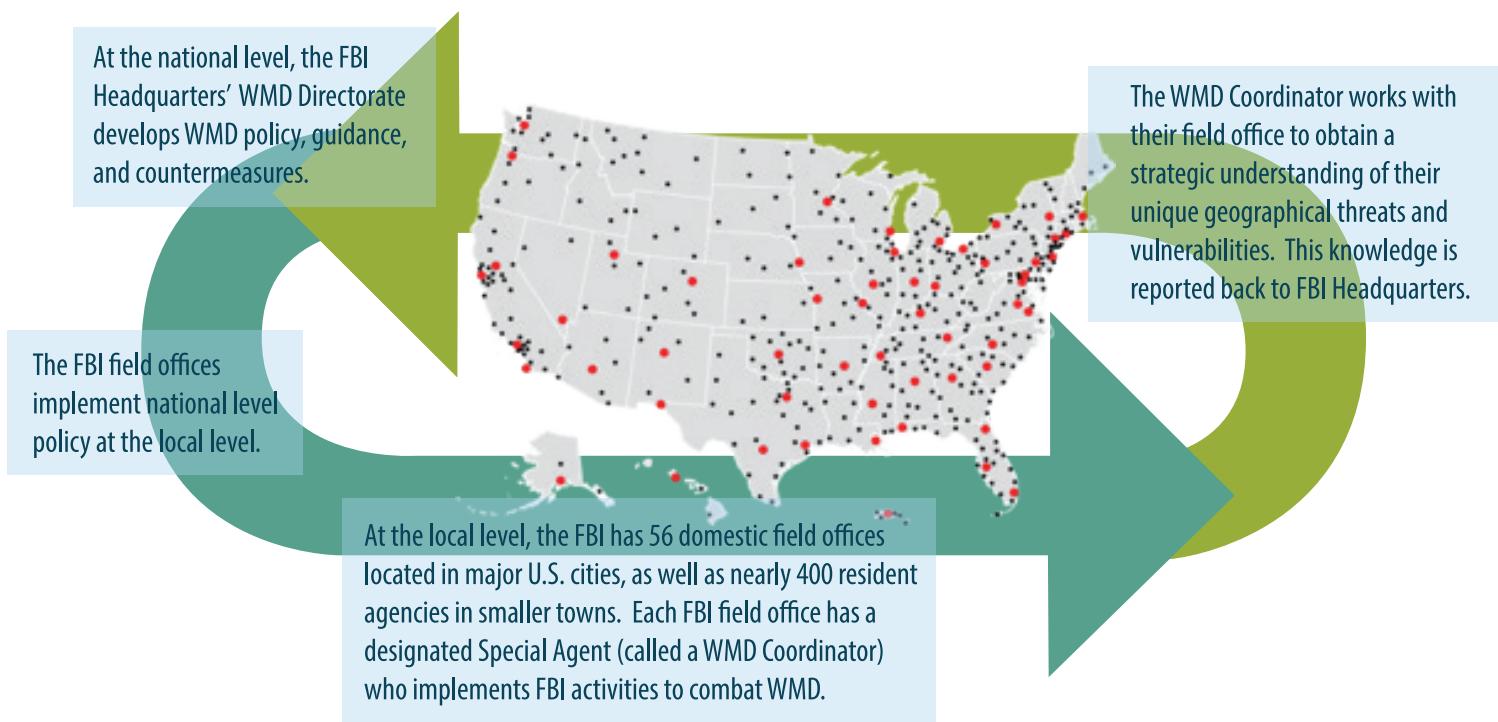
### **Non-violent Insider - Targeting Research Infrastructure**

**Mohsen Hosseinkhani (New York, 2009):** Hosseinkhani, a cardiology fellow at Mt. Sinai Hospital, was terminated because of poor work performance. He broke into a laboratory twice after being fired, stealing approximately \$10,000 worth of equipment and sabotaging several experiments by mixing up live animal specimens in an ongoing study. It was subsequently determined his original employment information was not verified, his education background was not found in university registries, and his address of residence was inaccurate. Hosseinkhani was charged with burglary and grand larceny, including transportation of stolen materials to Russia. While awaiting trial, Hosseinkhani again broke in to the laboratory and sabotaged more experiments. Hosseinkhani fled to Iran to avoid prosecution.

**Vipul Bhrigu (Ann Arbor, MI, 2009):** Bhrigu, a University of Michigan postdoctoral fellow, meticulously and systematically sabotaged the work of Heather Ames, a graduate student in his laboratory, over a 3-month period. Bhrigu poisoned his victim's cell-culture media with alcohol to discredit Ames and work on a prestigious research project. Ames was not taken seriously when she reported her suspicions to the laboratory manager and was even considered a subject of the ensuing investigation. Ames was subjected to two interrogations and a polygraph before investigators concluded that another individual was responsible. Cameras were installed in the laboratory and the resulting footage revealed Bhrigu's sabotage. Bhrigu pleaded guilty to destruction of property but found employment at Toledo University, his alma mater. He did not disclose the reason for termination at Michigan or mention his plea. He has fled the US with his wife, in violation of his parole, to avoid sentencing.



# FBI's WMD Coordinator Overview



In addition to domestic FBI field offices, the FBI has WMD Coordinators located overseas that provide regional expertise, assist with WMD investigations and prosecutions, and develop joint training programs.  
*Tbilisi, Georgia \* Lyon, France \* Singapore, Singapore*

## FBI's 56 Field Office Locations

Albany, NY	Indianapolis, IN	Oklahoma City, OK
Albuquerque, NM	Jacksonville, FL	Omaha, NE
Anchorage, AK	Kansas City, Missouri	Philadelphia, PA
Atlanta, GA	Knoxville, TN	Phoenix, AZ
Baltimore, MD	Las Vegas, NV	Pittsburgh, PA
Birmingham, AL	Little Rock, AR	Portland, OR
Boston, MA	Los Angeles, CA	Richmond, VA
Buffalo, NY	Louisville, KY	Sacramento, CA
Charlotte, NC	Memphis, TN	Salt Lake City, UT
Chicago, IL	Miami, FL	San Antonio, TX
Cincinnati, OH	Milwaukee, WI	San Diego, CA
Cleveland, OH	Minneapolis, MN	San Francisco, CA
Columbia, SC	Mobile, AL	San Juan, PR
Dallas, TX	Newark, NJ	Seattle, WA
Denver, CO	New Haven, CT	Springfield, IL
Detroit, MI	New Orleans, LA	St. Louis, MO
El Paso, TX	New York, NY	Tampa, FL
Honolulu, HI	Norfolk, VA	Washington, DC
Houston, TX		

## WMD Coordinator Responsibilities

- ▶ **Conduct outreach** with federal, state, and local stakeholders (including industry, academia, and scientific communities)
  - ▶ Develop partnerships with industry leaders
  - ▶ Conduct biosecurity outreach to universities to promote safe and secure research
- ▶ **Implement countermeasures**, developed by FBI Headquarters (WMD Directorate), to detect and deter specific WMD threats and vulnerabilities
  - ▶ Conduct assessments within area of responsibility to identify risks and vulnerabilities
  - ▶ Promote biosecurity guidelines (ex. Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA)
- ▶ **Investigate WMD crimes and acts of terrorism**
  - ▶ Identify individuals or groups expressing interest in acquiring WMD
  - ▶ Coordinate with public health Laboratory Response Network
- ▶ **Provide WMD training** to both FBI and public community
  - ▶ Conduct Joint Criminal-Epidemiological Investigation Training
  - ▶ Conduct exercises with federal, state, local law enforcement and first responders

# Key Statutes, Regulations, and Criminal Code to Prevent Misuse of Biological Agents

## U.S. FEDERAL CRIMINAL CODE

*U.S. federal criminal code is a compilation of U.S. federal laws which the FBI enforces.*

### U.S. Criminal Code, Title 18

**Sec. 175 part a:** Crime to knowingly possess any biological agent, toxin, or delivery system for use as a weapon (establishes BWC violations as crime)

**Sec. 175 part b:** Crime to knowingly possess any biological agent, toxin, or delivery system if not reasonably justified for a prophylactic, protective, bona fide or other peaceful research purpose

**Sec. 175b(c):** Crime to knowingly possess a select agent, regardless of intent, if not registered with the Select Agent Program

**Sec. 175c:** Crime to produce, engineer, or synthesize smallpox ("variola virus" considered 85% or more of variola major or minor gene sequence)

**Sec. 842(p):** Crime to teach or demonstrate use of or making of WMD material

**Sec. 2332a:** Crime to use (or conspire, threaten, or attempt to use) a WMD

## U.S. FEDERAL STATUTES

*Federal statutes are legislation that have been passed by Congress and signed into law by the U.S. President.*

### Public Health Security & Bioterrorism Preparedness Response Act (2002)

Requires those that possess biological agents or toxins deemed a threat must notify HHS (threat to public health) or USDA (threat to animal or plants).

### USA PATRIOT Act (2001)

Places restrictions on persons who possess select agents and provides criminal penalties for possession of such agents that cannot be justified for specified peaceful purposes.

### Antiterrorism & Effective Death Penalty Act (1996)

Directed HHS to establish a list of select agents and toxins, transfer procedures, and training requirements; created civil and criminal penalties for violations.

## U.S. FEDERAL CRIMINAL CODE

*The CFR is a compilation of regulations developed by regulatory agencies to implement laws. Although the FBI is not a regulatory agency, the FBI investigates violations of federal law, including criminal offenses against the CFR.*

**7 CFR Part 331** Govern select agents that pose a threat to plants

**9 CFR Part 121** Govern select agents that pose a threat to animals

**42 CFR Part 73** Govern select agents that pose a threat to public health

*The FBI looks forward to contributing its law enforcement expertise and experiences with the global community in hopes of strengthening collective national capacities to combat the threat of bioterrorism.*

## U.S. Federal Select Agent Program

The Federal Select Agent Program (SAP) regulates the possession, use, and transfer of biological agents and toxins that could pose a severe threat to public health (overseen by the U.S. Department of Health & Human Services, Centers for Disease Control and Prevention) as well as animals and plants (overseen by the U.S. Department of Agriculture, Animal & Plant Health Inspection Service).

A key objective of this U.S. program is to promote laboratory security by developing select agent regulations, providing guidance to the regulated community, and inspecting U.S. facilities working with select agents and toxins. The FBI conducts Security Risk Assessments, a requirement of the Select Agent Program, on all entities and personnel in the U.S. requesting access to select agents and toxins.

**U.S. Federal Select Agent Program website:**

[www.selectagents.gov](http://www.selectagents.gov)



### Federal Bureau of Investigation

935 Pennsylvania Ave. NW, Washington D.C., 20535

The FBI has legal attaché offices in more than sixty U.S. embassies. To find the nearest office and contact information, please refer to: <http://www.fbi.gov/contact-us/legal>