



# Biosecurity: The Law Enforcement Perspective

---

Weapons of Mass Destruction Directorate  
Federal Bureau of Investigation

Edward H. You

Biological Countermeasures Unit



# Enforcement of U.S. Laws

## Title 18, United States Code (U.S.C.)

---

### Biological Weapons

#### **18 USC 175(a)**

Crime to knowingly possess a biological agent, toxin, or delivery system for use as weapon, establishes BWC violations as crime

#### **18 USC 175(b)**

Crime to knowingly possess a biological agent, toxin, or delivery system if not for peaceful, bona fide or prophylactic research purposes

#### **18 USC 175b**

Crime to knowingly possess select agent, regardless of intent, if not registered with U.S. Select Agent Program

#### **18 USC 175c**

Crime to produce, engineer, or synthesize smallpox

### Weapons of Mass Destruction and WMD Terrorism

**18 USC 806** Enhances ability to seize assets of those with WMD intent

**18 USC 842** Crime to teach or demonstrate the making or use of a WMD

**18 USC 2332a** Crime to use (or conspire, threaten, or attempt to use) a WMD





# FBI WMD Responsibilities

- FBI is the lead U.S. Federal agency for investigating and responding to terrorism including Bioterrorism.
- FBI consolidated all WMD operations into a new Directorate in July 2006
- WMDD Missions
  - Countermeasures and Preparedness
  - Investigations and Operations
  - Intelligence Analysis
- Biological Countermeasures Unit, Objectives
  - Build national and international bioterrorism threat detection, identification, and reporting capabilities
  - Improve bioterrorism assessment and investigative capabilities
  - Enhance bioterrorism scientific, industry, and academic outreach



# WMD Coordinator Responsibilities

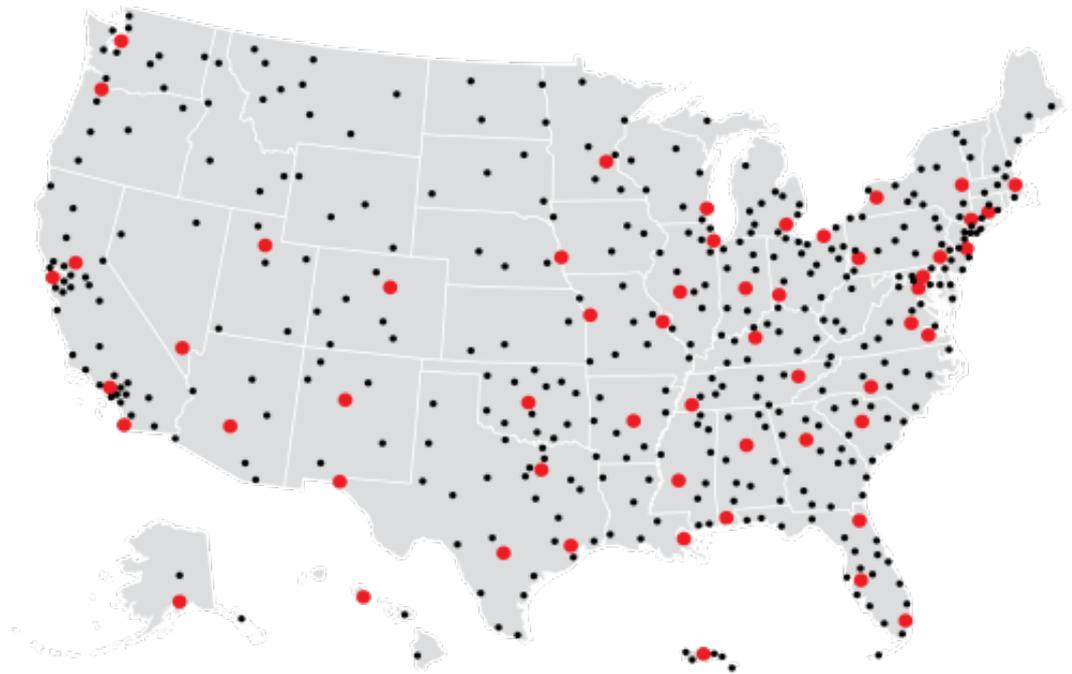
- **Conduct outreach** with federal, state, and local stakeholders (including industry, academia, and scientific communities)
  - Conduct biosecurity outreach to universities to promote a culture of security
  - Develop partnerships with industry leaders
- **Implement countermeasures** to detect and deter biological threats
  - Conduct assessments within area of responsibility; identify risks and vulnerabilities
  - Promote biosecurity guidelines (ex. HHS Screening Guidance for Synthetic DNA Providers)
- **Investigate bio crimes and acts of bioterrorism**
  - Coordinate with public health Laboratory Response Network
  - Receive notice of significant test results
  - Receive notice of theft, loss, or release
- **Provide training** to both FBI and public community
  - Conduct Joint Criminal-Epidemiological Investigation Training
  - Conduct exercises with local law enforcement & first responders
- **Biosecurity resource/expertise**



# FBI Biosecurity Equities

## Domestic FBI Operations

- 56 domestic Field Offices
  - Each with a WMD Coordinator
- 400+ Resident Agencies
- FBI Headquarters Division
- Criminal Justice Information Service, Biosecurity Risk Assessment Group
- Agent-in-the-Lab Program



# FBI Academic Biosecurity Workshops



## Workshop Goal:

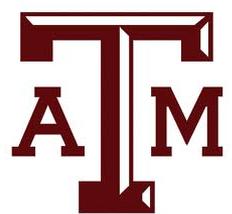
Improve the cooperation among law enforcement agencies and research institutions to mitigate potential biosecurity issues that may affect public health and safety

## Target Audience:

- Biosafety Professionals/Responsible Officials
- First Responders (Law Enforcement, Fire, EMS)
- Public Health
- Environmental Health & Safety Professionals
- Emergency Management
- Institutional Leadership
- Human Resources
- Faculty, Post Docs and Students



THE UNIVERSITY OF TEXAS  
MD ANDERSON  
CANCER CENTER  
*Making Cancer History®*





UNCLASSIFIED

# Comprehensive Biosecurity

## Physical Security

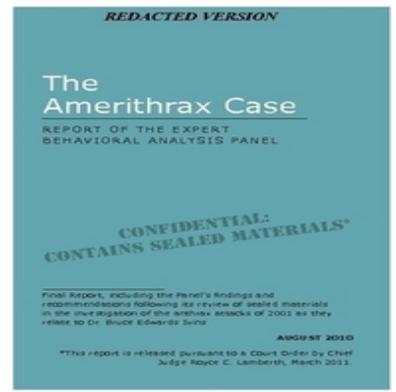
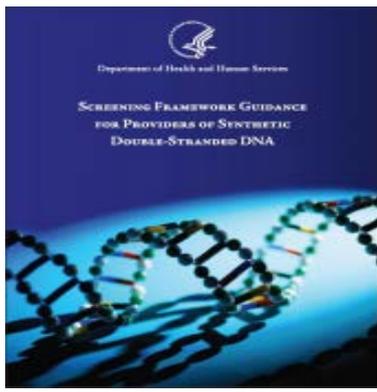
- Access control
- Intrusion detection
- Physical barriers
- Inventory controls
- Incident response

## Information Security

- Cyber security
- Operational security
- Surveillance/Elicitation Detection

## Personnel Security

- Suitability
- Reliability
- Occupational Health and Wellness
- Training





# U.S. Criminal Acts with Biological Agents

---

- 1916**     **Arthur Warren Waite**  
Dentist / Bacteriologist  
Poisoning with infectious agent and murder of In-laws
- 1984**     **Diane Onang** (Rajneeshi Cult)  
Nurse Practitioner  
Acquired *Salmonella typhi* for an attack on local residents of the Dales, Oregon
- 1992**     **Brian T. Stewart**  
Phlebotomist  
Injected son with HIV contaminated blood
- 1994**     **Dr. Richard J. Schmidt**  
Gastroenterologist  
Injected lover with HIV infected blood from one of Schmidt's patients
- 1995**     **Dr. Deborah Green**  
Oncologist  
Attempted murder of estranged husband with ricin
- 1996**     **Diane Thompson**  
Attacked colleagues with *S. dysenteriae* type 2 contaminated blueberry muffins and doughnuts
- 2001**     **Dr. Bruce Ivins**  
U.S. Army Microbiologist  
Primary suspect in the Amerithrax Case at the time of his death by suicide (not convicted)





# FBI's Security Risk Assessments

---

SRAs are requirement of Select Agent Program

Security risk assessment  $\neq$  background check

SRA uses biographical and biometric data to determine if candidate meets criteria of “restricted person” based on list of prohibitors

SRA's scope limited by Congress to relevant Federal databases in order to screen for criminal and terrorist activity while protecting privacy of individuals.

- Purpose of a SRA is to exclude individuals with specific, serious criminal or terrorism-related activity in their backgrounds from having access to BSAT





UNCLASSIFIED

# FBI Security Risk Assessment, Statutory Prohibitors



## USA PATRIOT Act (18 USC 175b)

- Under indictment for crime punishable by imprisonment for term exceeding one year
- Convicted of crime punishable by imprisonment for a term exceeding one year
- Fugitive from justice
- Unlawful user of any controlled substance
- Alien illegally or unlawfully in United States
- Adjudicated as a mental defective or has been committed to any mental institution
- 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
- Discharged from Armed Services of United States under dishonorable conditions
- Member of, or acts on behalf of, a terrorist organization as defined in the Immigration and Nationality Act (8 USC 1182)

## Bioterrorism Response Act

- Committing crime specified in 18 USC 2332b(g)(5) [Acts of Terrorism Transcending National Boundaries]
- Having a knowing involvement with organization that engages in domestic or international terrorism (as defined in 18 USC 2331) or with any other organization that engages in international crimes of violence
- Being an agent of a foreign power (as defined in 50 USC 1801)





# Select Agent Program Applicant #1

---

12/06/1986

Charge 1 – **Fraud**

Conviction: Fraud (Misdemeanor)

01/20/1990

Charge 1 – **Theft By Check**

Conviction: Theft By Check (Misdemeanor)

06/24/1995

Charge 1 - **Aggravated Assault With Deadly Weapon**

Conviction: Aggravated Assault ( 2<sup>nd</sup> Degree Felony)

Sentence: 5 Year Suspended, Probation Discharge, Conviction Set-Aside

07/06/1997

Charge 1 – **Assault Causes Bodily Injury**

Disposition: Dismissed



# Select Agent Program Applicant #1

(continued)

07/06/1997

Charge 1 – **Theft Property  $\geq$ \$20  $<$ \$500 By Check**

Conviction: Theft  $\geq$ \$20  $<$ \$500 (Misdemeanor)

07/12/1997

Charge 1 – **Assault Causes Bodily Injury**

Conviction: Assault Family Violence (Misdemeanor)

01/14/2011

Charge 1 – **Driving While Intoxicated**

Charge 2 – **Possession Controlled Substance PG 3 $<$  28G**

Disposition: Pending/Referred to County Attorney





UNCLASSIFIED

# Select Agent Program Applicant #1

(continued)

## Conclusion:

- The maximum imprisonment for misdemeanors in Texas does not exceed 1 year; therefore, the applicant **did not meet the restrictor** of “convicted in any court of a crime punishable by imprisonment for a term exceeding 1 year.”
- The applicant **did not meet the restrictor** of “unlawful user of any controlled substance.”
- The FBI will regularly check with the court for a final disposition on the most recent arrest. If the applicant is convicted of possession of a controlled substance, he/she will meet the “unlawful user of any controlled substance” restrictor.



FBI SRA





# Restricted by category

---

Since inception of SRA program:

Adjudicated mental: 6  
Agent of a Foreign Power: 2  
Alien of a Terror State: 4  
Controlled Substance: 27  
Dishonorable Discharge: 2  
Federal crime of terrorism: 0  
Criminal conviction: 192  
Fugitive from justice: 13  
Illegal/unlawful alien: 19  
Intentional crimes of terrorism: 0  
Under indictment: 27

Total: **292**





UNCLASSIFIED

# Personnel Pre-Access Suitability Assessment

Developed in response to Presidential Executive Order creating the Federal Experts Security Advisory Panel (FESAP) to enhance U.S. Biosecurity.

Certain information should be requested from an applicant:

- Criminal history
- Home address history
- Work history
- Contact information for 3 professional and 3 peer references
- Visa/residency status (for foreign applicants)

Certain information should be obtained via records request, if possible:

- Criminal records
- Civil orders (restraining orders/protective orders)
- Driving records
- Education records
- Professional licenses/certification

Interviews should be conducted with the applicant and their professional and peer references. Use of tactical interview procedures using structured, open-ended questions is the best approach





# Ongoing Personnel Reliability



**Reliability:** the continuation of possessing suitable characteristics (as defined by U.S. policy)

Once individuals are granted access to the lab, aspects of suitability should continue to be checked on an ongoing basis.

Reviews of reliability should look for:

- Changes in employee performance
- Behaviors that might indicate changes in the behavioral baseline (established during the pre-access suitability investigation)
- Concerning behaviors
- Sources of stress in the employee's work and private life
- *Whole person paradigm must guide security decisions*

Security decisions may include removal of access or a re-assessment of individual employee behavioral baselines

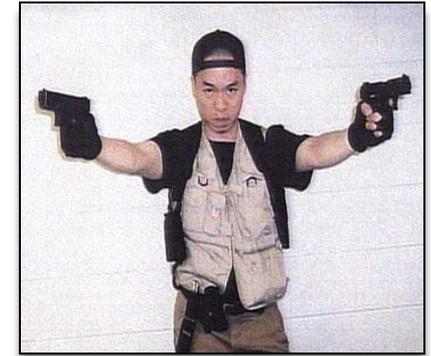
Dramatic change in work schedule or work-life balance may be due to changes in the nature and scope of the work and may not be derogatory





# Peer and Self Reporting

*“A key finding common to every retrospective analysis of major incident of workplace or campus violence is the extent to which co-workers and supervisors were concerned about the perpetrator prior to the event.”*  
(Virginia Tech Panel, 2007)



- **Peer Reporting**

- ✓ Peers must know what constitutes a concerning behavior and be empowered to make reports
- ✓ Training should explicitly describe concerning behaviors and behavioral changes that a peer may observe.
- ✓ Institutional safeguards against reprisal and false reports

- **Self Reporting**

- ✓ Studies of campus and workplace violence as well as targeted violence have shown that people are likely to rationalize their behaviors.
- ✓ Employees are much more sensitive to stresses in their lives and the grievances that they have against co-workers, friends and family.
- ✓ Training in support of self-reporting should address the root causes of behaviors of concern: stress and grievance.





# Examples of Concerning Behaviors

---

- Sending inappropriate emails
- Unjustified anger, aggression
- Inappropriate conduct toward colleagues
- Sabotaging colleagues research
- Physical violence (to objects or persons)
- Acts of vandalism or property damage
- Unexplained absences
- Deception
- Laboratory work that does not correspond to official project
- Working during “off hours” without justification or documentation
- Signs of alcohol/drug abuse
- Security breaches, accessing computer/email passwords, stealing laboratory notebooks or reagents
- Talking about wanting to harm themselves or others
- Mention of plans to commit acts of violence to persons or property
- Providing false information on applications or other formal institutional documents
- Unlawfully carrying weapons
- Cruelty to animals

***Goal is to identify a pattern of concerning behavior;  
not a one time anomaly (unless excessive)***

---

# Examples of Concerning Behavioral Changes

- Performance of duties declines markedly
  - Increase in risk-taking behaviors
- Significant increase in terms of distraction or mistakes
  - Increasingly withdrawn
- Significant and prolonged deterioration in appearance



# Examples of Stress and Grievance

- Major health issues
- Change in marital/relationship status
- Death of relative/friend
- Change in professional status
- Change in financial status
- Love/obsessive relationship
- Change in co-workers
- Change in occupational routine
- Change in workplace organization
- Change in work function
- Victim of (unrelated) violence
- Challenges to personal beliefs





# Reporting Indicators

---

Factors explaining why peers didn't report observed suspicious behavior:

- 1) Poor training – didn't know which behaviors were serious enough to report.
- 2) Poor reporting structure – didn't know who to report their suspicions to.
- 3) Diffusion of responsibility – thought others would report it.
- 4) Familiarity breeds contempt – downplayed aberrant behaviors ("having a bad day").





# Group Adversary Threats

## Environmental/Animal Rights Extremists

- Animal Liberation Front (ALF)
- Stop Huntingdon Animal Cruelty (SHAC)
- Environmental Liberation Front (ELF)

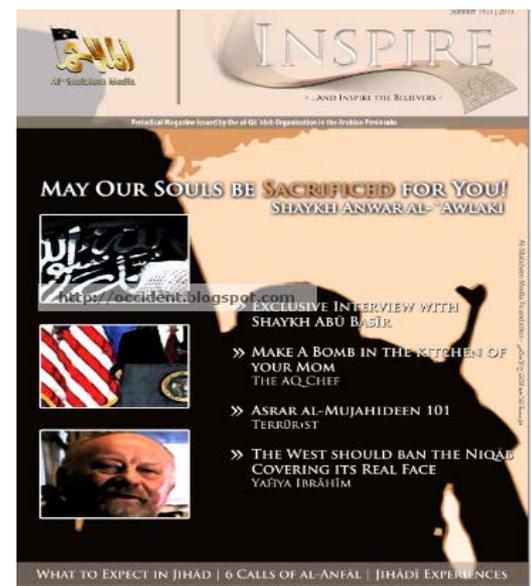
## Violent Anti-Abortion/Gay/Other Ultra-Conservative Activists

- Army of God
- World Church of the Creator

## Terrorist Organizations

- Al Qaeda
- Hamas

## Foreign Powers (state-sponsored programs)



**STUDENTS  
EARN EA\$Y MONEY!!!**

Negotiation Is Over would like to pay you  
**\$100 cash**  
for information about each biomed student who is learning to experiment on animals in your university.

Provide us with the following,  
you can quit your part time job:

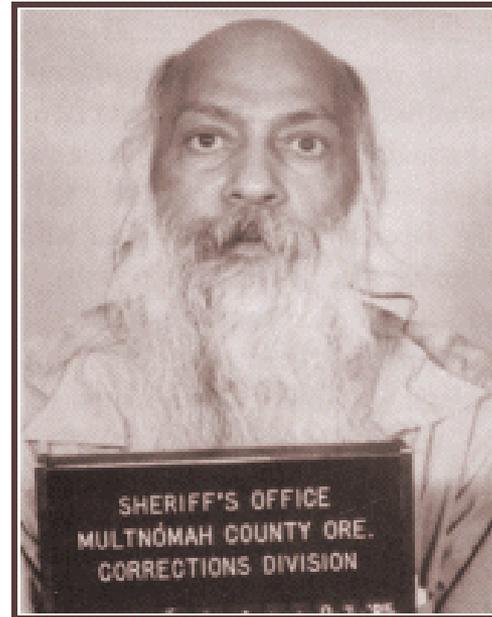
- ❖ name of vivisection student
- ❖ picture of student
- ❖ address, phone and any other contact info
- ❖ pictures and/or summary of animal experiments in which student is involved

To claim your reward money anonymously, simply contact  
NIO at (352) 396-4132  
or write to us at [camille@negotiationisover.com](mailto:camille@negotiationisover.com)





# Group Adversaries

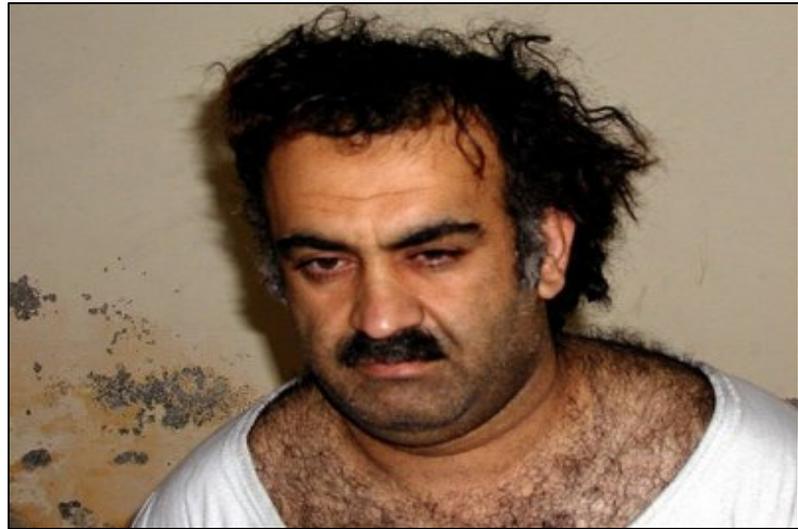


## **Diane Yvonne Onang** (*Group: Rajneeshi Cult*)

A nurse practitioner in the Rajneesh Medical Corporation conspired with Bhagwan Shree Rajneesh, and other members of the Rajneeshi Cult, in 1984 to poison the population of The Dales, OR in an effort to influence a local election. The cult had their own legally operating diagnostic clinic and used Onang's position and title, to acquire *S. typhimurium* from ATCC.



# Group Adversaries



## **Aafia Siddiqui** (*Group: Al Qaeda*)

Pakistani that came to the U.S. in 1990 to receive education (B.S. in biology from MIT, Ph.D in neuroscience from Brandeis in 2001). Might have been radicalized through contacts in MIT's Muslim Students' Association. After 9/11, she left the U.S. to serve as a mujahideen medic; married nephew of KSM, chief planner of 9/11. When she was detained in Afghanistan in 2008, she was in possession of sodium cyanide, planning documents for production of filovirus-based weapons, and schematics of the Plum Island Animal Disease Center. Currently serving an 86 year prison sentence.





# Security Awareness Training

Promotes awareness of and compliance with institutional security policies

Security Awareness Training might include:

- Insider Threats
- Security policies and procedures
- Incident reporting and incident response
- Continuity of Operations
- Self & Peer reporting requirements
- Information security policies
- Operations security concepts
- Surveillance detection
- Elicitation/manipulation detection and response
- Periodic updates regarding local external threats





---

# QUESTIONS

**Edward H. You**

FBI Headquarters  
Weapons of Mass Destruction Directorate  
Biological Countermeasures Unit  
Edward.You@ic.fbi.gov





# Select Agent Program Workshop

## November 2012

Agricultural Select Agent Program (USDA/APHIS)  
CDC Select Agent Program (HHS/CDC)  
Bioterrorism Risk Assessment Group (FBI/CJIS)



# Regulatory Requirement

Pre-access suitability assessment and an ongoing suitability assessment are designed to reduce the risk of biological select agent and toxins (BSAT) misuse through the actions of an “insider.”



# What is an Insider Threat?

Refers to an individual who has access to BSAT as part of his or her job and has the potential to misuse them. The scenarios that illustrate the insider threat involve the theft, misuse, or diversion of BSAT by an individual who had been approved to have access to them. Some examples of the “insider” include:

- an individual with malevolent intent who infiltrates a research facility under the guise of a legitimate researcher, only to steal, release or divert BSAT;
- an individual with access to BSAT who is coerced or manipulated into providing access or expertise to unauthorized individuals with malevolent intent; or
- an individual whose job duties include legitimate access to BSAT but who may misuse, release or divert BSAT as a result of a significant life-changing event.



# Why the Concern Regarding Insider Threat?

- October 2001 anthrax attacks:
  - Caused 5 fatalities and 17 illnesses
  - Costs included
    - More than \$23 million to decontaminate one Senate office building
    - Approximately \$2 billion in revenues lost to the postal service
- Federal Bureau of Investigation and Amerithrax Expert Behavioral Analysis Panel
- Federal Experts Security Advisory Panel's Recommendation



# Federal Experts Security Advisory Panel's Recommendations

Federal Experts Security Advisory Panel

**Recommendations to the Select Agent  
Program on Components of Guidance to  
Registered Entities  
for  
Enhancing Personnel Security for Access  
to Tier 1 Biological Select Agents and  
Toxins**

3/26/12

## **Personnel Security at entities housing Tier 1 BSAT should include:**

- Suitability and reliability assessments of individuals requesting and continuing to have access to Tier 1 BSAT;
- Reporting and assessment of potential and known threats to the well-being of staff, safety of the public, and safety and security of Tier 1 BSAT; and
- Procedures to inform personnel at registered entities possessing Tier 1 BSAT of the risks and challenges associated with work with Tier 1 BSAT to facilitate their participation and assistance in support of personnel assessment.

## **In order to achieve successful personnel security initiatives:**

- Leadership at registered entities possessing Tier 1 BSAT should support the implementation of personnel assessment initiatives at their institution



# Suitability Assessment Guidance

- Pre-Access Suitability Assessment Program
- Ongoing Suitability Assessment Program
- Transitioning of Individuals with Access to Tier 1 BSAT at Effective Date
- Denial, Termination or Suspension of Individual's Access to Tier 1 BSAT



# Suitability Assessment Terms

- **Ongoing Suitability Assessment:** After the initial pre-access suitability assessment, a standardized procedure to continue to determine if an individual is reliable, loyal, trustworthy, honest, free from emotional or mental instability, possess sound judgment, free of conflicting allegiances and potential for coercion, and possess a willingness to abide by regulations governing the possession, use, or transfer of select agents.
- **Personnel Suitability:** Personnel with access to BSAT should be reliable, loyal, trustworthy, honest, free from emotional or mental instability, possess sound judgment, free of conflicting allegiances and potential for coercion, and possess a willingness to abide by regulations governing the possession, use, or transfer of select agents.



# Suitability Assessment Terms

- **Pre-Access Suitability Assessment:** The evaluation of an individual using standardized procedures to determine if an individual is reliable, loyal, trustworthy, honest, free from emotional or mental instability, possess sound judgment, free of conflicting allegiances and potential for coercion, and possess a willingness to abide by regulations governing the possession, use, or transfer of select agents.
- **Suitability Assessment Program:** A combination of pre-access and ongoing suitability practices along with a comprehensive mechanism of allowing individuals to report risks and threats to safety and security of Tier 1 BSAT to entity leadership.
- **“Whole Person” Assessment:** A balanced assessment of an individual that accounts for a behavioral baseline and the milieu or environment in which that person works, lives and socializes, along with mitigating circumstances, and overall qualities of credibility and suitability.



# Roles & Responsibilities

- Entity Leadership - supports the Responsible Official for the development and implementation of a suitability assessment program
- Responsible Official - authority to immediately restrict or deny access based on behavioral, medical or administrative grounds for personnel and responsible for notifying the Federal Select Agent Program
- Individuals with Access to Tier 1 BSAT - monitor their own suitability, as well as the suitability of others



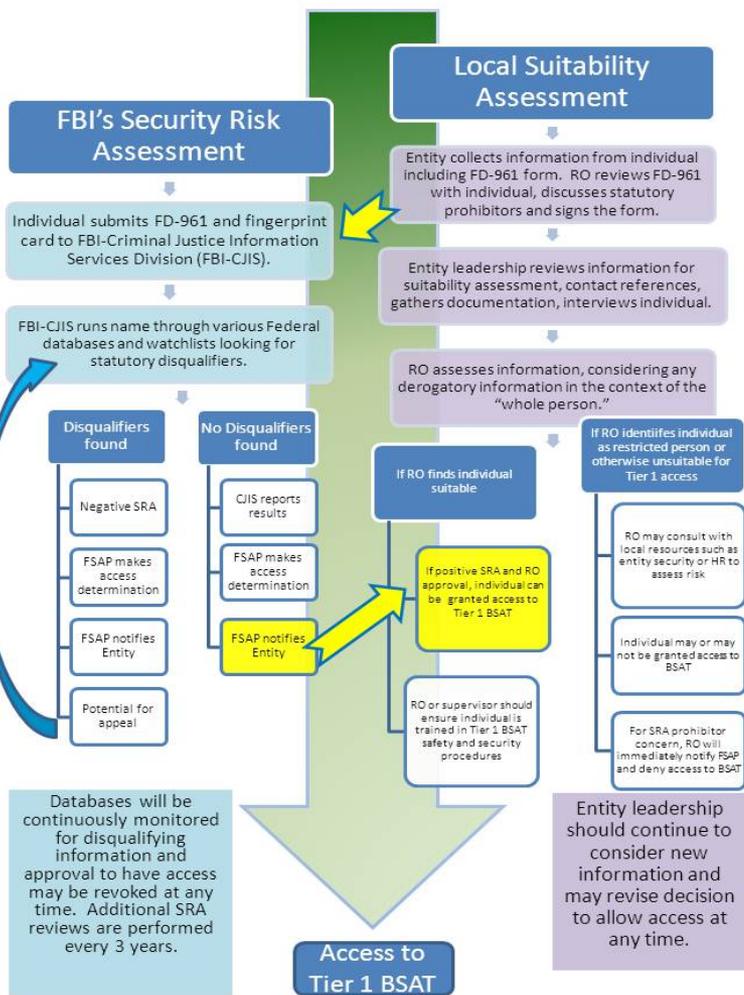
# Reviewer and Certifying Official

A concept that an entity may want to consider is the designation of two individuals:

- **Reviewer:** An entity official whose position duties include monitoring the suitability assessment program and reviewing designated suitability actions.
  - Security or administrative professional
  - Legal counsel
- **Certifying Official:** An entity official whose duties include the certification of personnel meet the established requirements of an entity-specific suitability assessment and monitoring program.
  - Outside the individual's supervisory chain
  - Human Resources Professional, Employment Assistance Program counselor, Principal Investigator not associated with the individual's work



# Pre-Access Suitability



- Collection and Verification of Information
  - Home Address History
  - Work History
  - Education History
  - Criminal History
  - Resume or Curriculum Vitae (including scientific publications and affiliations)
  - Professional License/Certification History
  - Visa Status (if applicable)
  - References, including Contact Information
- Additional Information Requested for Individuals in a Supervisory Role
- Interview with the Applicant and Assessment of Personal Behavior and Work Practices

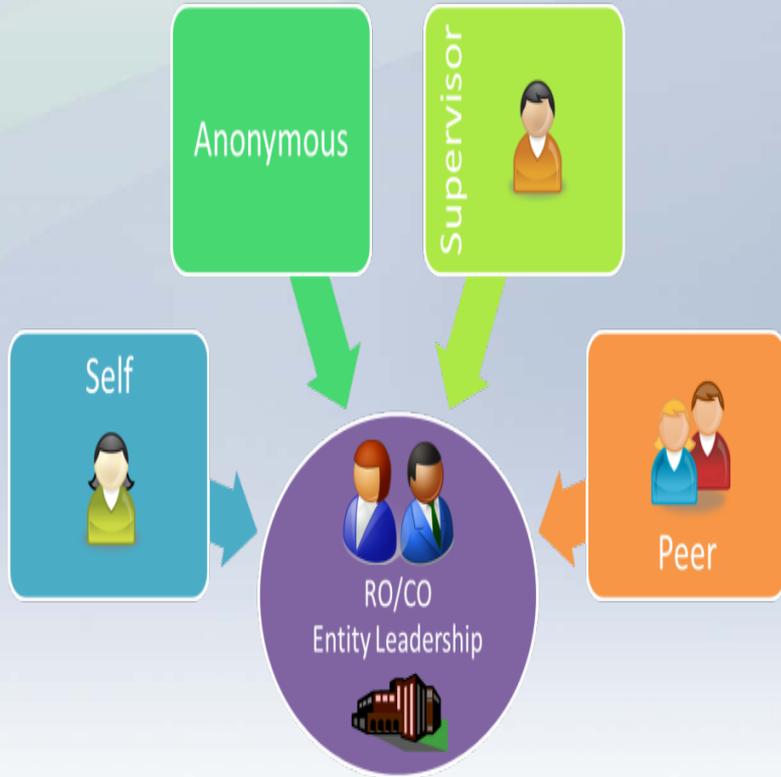


# Ongoing Suitability Assessment

- Mechanisms for self- and peer-reporting of behaviors of concern. Specifically, incidents or conditions that could affect an individual's ability to safely have access to or work with Tier 1 BSAT or to safeguard Tier 1 BSAT from theft, loss, or release.
- Ongoing monitoring of suitability for individuals with access to Tier 1 BSAT.
- Training of employees with access to Tier 1 BSAT on entity policies and procedures for reporting, evaluations, and corrective actions concerning the assessment of personnel suitability.



# Self- and Peer-Reporting



- The types of information to report
- To whom the information should be reported
- How the reported information will be used to assess risks and determine actions
- Documentation requirements and availability of entity resources
- Confidentiality of the reporting process



# Ongoing monitoring

- Ongoing suitability monitoring can be accomplished through many different avenues:
  - Tier 1 BSAT users technical, biosafety, and security annual performance evaluations
  - Periodic review of Tier 1 BSAT user's access requirements by duties and responsibilities
  - Review of Criminal Records and Visa Status



# Training

- Coordinated with other required training
- Could include, but is not limited to:
  - Insider threat awareness
  - Behaviors of Concern
  - Entity pre-access suitability policies concerning access to Tier 1 BSAT
  - Self- and peer-reporting procedures
  - Statutory prohibitors
  - Tier 1 BSAT user evaluation process
  - Entity policy on ongoing suitability assessment procedures
  - Entity policy on ongoing suitability monitoring procedures
  - Corrective actions procedures and policies
  - Procedures for voluntary and involuntary removal of Tier 1 BSAT access
  - Information security (e.g., need to know)

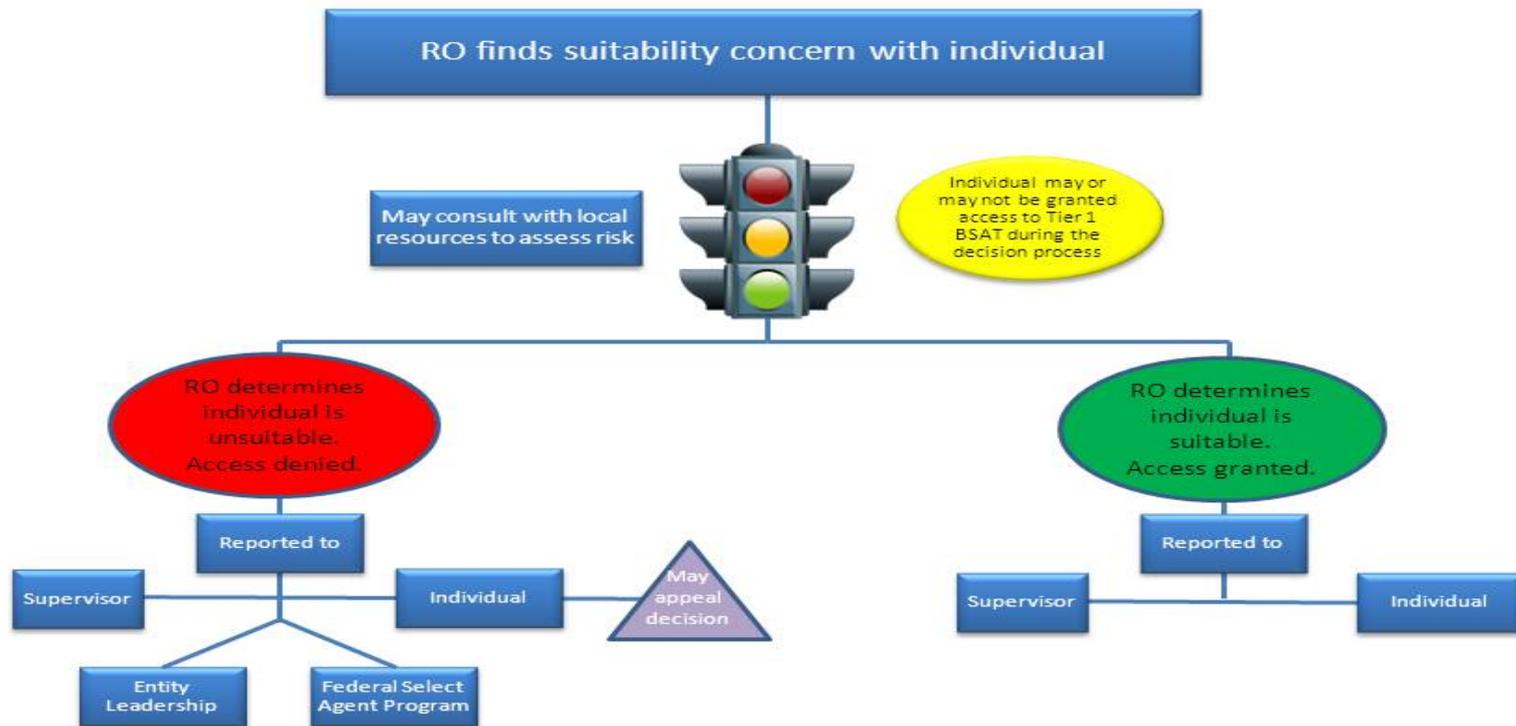


# Transition of Individuals with Access to Tier 1 BSAT at Effective Date

- Individuals who already have approved access to Tier 1 BSAT are not required to have a pre-access suitability assessment, but will be subject to the entity's ongoing assessment and monitoring program.
- If the entity has concerns about an individual that has access to Tier 1 BSAT, the entity should perform a modified pre-access suitability assessment for the individual that may include:
  - Records Verification
  - Training on Entity's Suitability Assessment Program and Tier 1 BSAT regulatory requirements



# Denial, Termination or Suspension of Individual's Access to Tier 1 BSAT



# Visitors for short-term training with Tier 1 BSAT

## Pre-access Suitability Options:

- Host entities can always enroll trainees into its pre-access suitability program.
- Verify with the home entity or organization that the trainee has gone through a pre-access suitability program and is subject to ongoing assessment.
- Verify with the home entity or organization that the trainee has gone through similar pre-access checks (references, employment, criminal) and accept those checks as sufficient.
- Verify with home entity which pre-access checks have been accomplished and work with the home entity to complete any checks which were not done.
- *The host entity can deny access to Tier 1 agents to any trainee if the host entity cannot verify the trainee's status.*



# Visitors for short-term training with Tier 1 BSAT

## Ongoing Assessment Options:

- Ensure training is monitored.
- Limit access to the registered area.
- Limit access within the registered areas.
- *If a trainee demonstrates a behavior which may compromise safety or security, the entity should consider removing his/her access.*



# Questions for Discussion

- How would inspectors verify the entity's suitability assessment program?
  - Security plan
  - Interviews
- Are there forms that the entity is required to provide to document the entity's suitability assessment program?
  - No, the information should be covered in the Security plan. Though not required, the entity may provide information to support the entity's suitability assessment program such as information about entity's Self- and Peer-Reporting Program and annual evaluations?



# Questions for Discussion

- Is a background investigation done for a security clearance considered equivalent to a suitability assessment?
  - The entity may use a background investigation to complement suitability assessment program. However, this is not a requirement of the regulations.
- What are the minimum requirements to develop a suitability assessment program?
  - Section 11 (Security) requires that the security plan must describe procedures for conducting a pre-access suitability assessment of persons who will have access to a Tier 1 select agent or toxin and describe procedures for the ongoing assessment. The ongoing assessment procedures must include : self- and peer-reporting of incidents or conditions that could affect an individual's ability to safely have access to or work with select agents and toxins, or to safeguard select agents and toxins from theft, loss, or release; training of employees with access to Tier 1 select agents and toxins; and ongoing suitability monitoring of individuals.



# Questions for Discussion

- Where can I go to seek assistance with developing the entity's suitability assessment program?
  - Guidance Document
  - Federal Select Agent Program
  - Local Federal Bureau of Investigation Weapons of Mass Destruction Coordinator
- Is our entity required to perform drug screening?
  - No, it is not a requirement of the regulations.
- Is our entity required to investigate a person's finances or run a credit report?
  - No, it is not a requirement of the regulations.





# Select Agent Program Workshop

## November 2012

**For more information, please contact the Federal Select Agent Program**

Telephone: 301-734-5960 (APHIS) or 404-718-2000 (CDC)

E-mail: [ASAP@APHIS.USDA.GOV](mailto:ASAP@APHIS.USDA.GOV) (APHIS) or [lrsat@cdc.gov](mailto:lrsat@cdc.gov) (CDC)

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

*The findings and conclusions in this report are those of the authors and do not necessarily represent the official position of the Federal Select Agent Program.*

