# Personnel Security: Insider Threat Mitigation

**Ben Perman, PhD, RBP**
**American Biological Safety Association**
**2013 Annual Meeting**
**Kansas City, MO  October 23, 2013**

# Is the Insider Threat real?

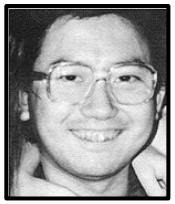
- “There has never been a case of someone weaponizing bio material from inside the lab.”
- “I don’t work with BSAT so the probability of someone stealing or intentionally misusing bio material/technology is extremely low.”
- “Everyone who works here is FBI cleared—the gold standard– and thus is suitable to work here.”
- “Our lab has a robust suitability process when hiring staff, so everyone here will always be a good guy.”
- “If someone was going to do something bad, we would know about it and someone would report it.”

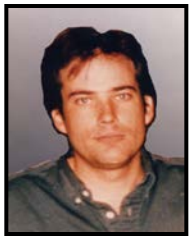













# Threat Assessment

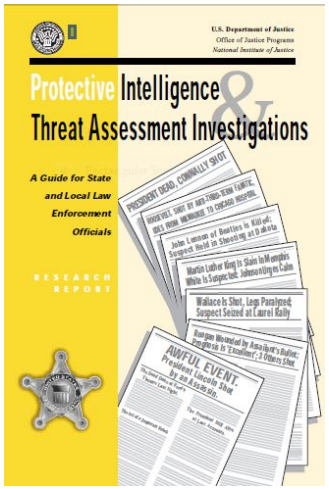
Threats are posed by adversaries. Adversaries are people.

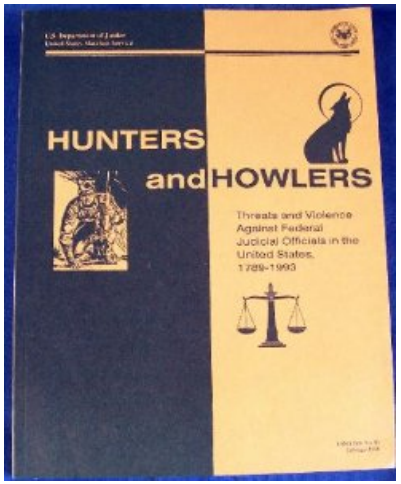
People provide a series of clues to their current and future status as a threat through their behavior – they do not “just snap”

Threatening behaviors tend to escalate over time so early detection and mitigation is effective – this is known as the targeted violence process

Personnel Security practices are informed by knowledge about:

- how threats develop; and,
- how to detect threats during their development

# Personnel Security

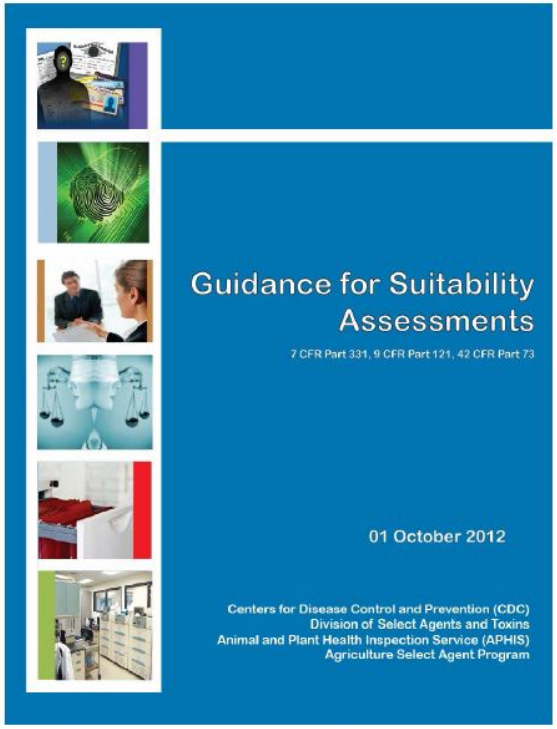
Personal Security Programs empower employees to take responsibility for their own protection and become aware of the nature of potential threats that they may encounter.

- **Pre-access Suitability –** establishes a behavioral baseline
- **Personnel Reliability** - ongoing assessment to identify if/when individual deviates from their behavioral baseline
- **Training** – awareness is the pre-requisite for compliance
- **Personal Security -** protects individuals from unknowingly contributing to an insider threat by educating them in areas such as operation security, information security, and threat awareness

Collectively works to identify, monitor, and counter insider threats

# Pre-Access Suitability in Regulation

- **42 CFR 73.11(f)(1)**
  - [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;
- **CDC Guidance for Suitability Assessments**
  - A combination of pre-access and on-going suitability practices, in conjunction with comprehensive and consistent review mechanisms, determining the reliability of personnel for access to Tier 1 BSAT, and allowing individuals to report risks and threats to safety and security concerning Tier 1 BSAT to entity leadership.



# Pre-Access Suitability

**FBI Security Risk Assessment**

- Not a “background investigation”
- Does not determine if an employee is suitable to access BSAT

**Applicant/employee Information**

- Criminal history
- Home address history
- Work history
- Contact information (professional / peer)
- Visa/residency status

**Information obtained from records**

- Criminal records
- Civil orders
- Driving records
- Education records
- Professional licenses/certification


“What do you mean, it’s not a good résumé? It’s the most expensive one they had on eBay!”

**Interviews**

- Applicant / employee
- Professional and peer references (seek secondary contacts)
- Employ tactical interview procedures (e.g. structured, open-ended questions)

# Personnel Reliability in Regulation

- **42 CFR 73.11(f)(3)**
  - [The security plan must] Describe procedures for the ongoing assessment of the suitability of personnel with access to a Tier 1 select agent of toxin. The procedures must include:
  - (i) 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.
  - (ii) The training of employees with access to Tier 1 select agents and toxins on entity policies and procedures for reporting, evaluation, and corrective actions concerning the assessment of personnel suitability; and
  - (iii) The ongoing suitability monitoring of individuals with access to Tier 1 select agents and toxins.

# Examples of Concerning Behaviors

- Sending inappropriate emails, texts, mail or other written/verbal communication
- 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 in “off-hours” without justification or documentation
- Security breaches, accessing computer/email passwords, stealing laboratory notebooks or reagents
- Violent or suicidal ideation
- Violent or suicidal planning
- Violent or suicidal preparation
- False report - applications or other formal institutional documents
- Unlawfully carrying weapons
- Cruelty to animals
- Stalking, obsessional relationship
- Significant change in appearance
- Significant work/life change
- Alcohol / drug abuse
- Undue focus on grievance

# Personnel Reliability

**Reliability**: The maintenance of suitable characteristics for continued access to valuable biological materials. …trust.

**Reliability Scope**

- Changes in employee performance
- Behaviors that might indicate changes in the behavioral baseline established in the initial suitability phase
- Behaviors of concern
- Incidents
- Work-life issues and incidents
- *"Whole person" paradigm*

**Reliability Process**

- Periodic reassessment of suitability
- Peer and self-reporting

# Failure to Report

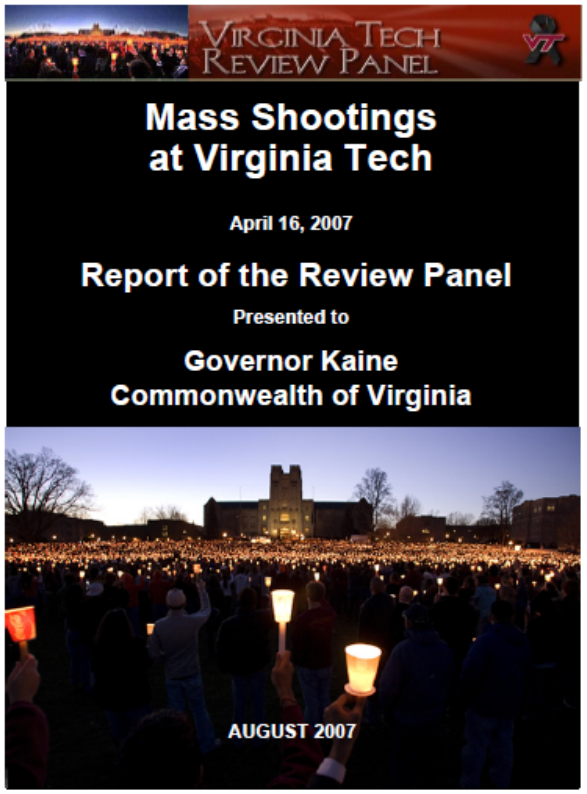
**Poor training** – didn't know which behaviors were serious enough to report; didn't understand the value of reporting incidents

**Poor leadership** – fear of reprisal or lack of confidence in organization and policies

**Diffusion of responsibility** – thought others would report it

**Familiarity breeds contempt** – had become desensitized to behaviors

# Threat Assessment Task Force




## Interdisciplinary Membership

- Laboratory Management (PI, RO, BSO)
- Personnel Administration (HR, EAP, Ombudsman)
- Security and Law Enforcement
- Occupational Health and Wellness
- Threat Assessment Professional

## Threat Assessment Process

- Staff won't comply with reporting if they don't feel protected.
- Deters intentional false reporting if staff know review process will occur every time
- Consistent follow-through will establish a culture trust in the system for all employees (both reporter and reported)

# Personnel Security Training

**Personnel Reliability Peer and Sell Reporting Process**

- Ways to report self/peer concerns and who to report to
- Reporting process/rules
- Behaviors of concern
- Mandatory incident reporting
- False report warning
- Reprisal protection – “whistleblower”

**Personal Security**

- Operational security
- Information security – includes cyber secu
- Elicitation and manipulation awareness
- Counter-surveillance awareness

**Local threat updates**

- Threat history
- Threat presence and direct threats
- Indirect threats – police activity

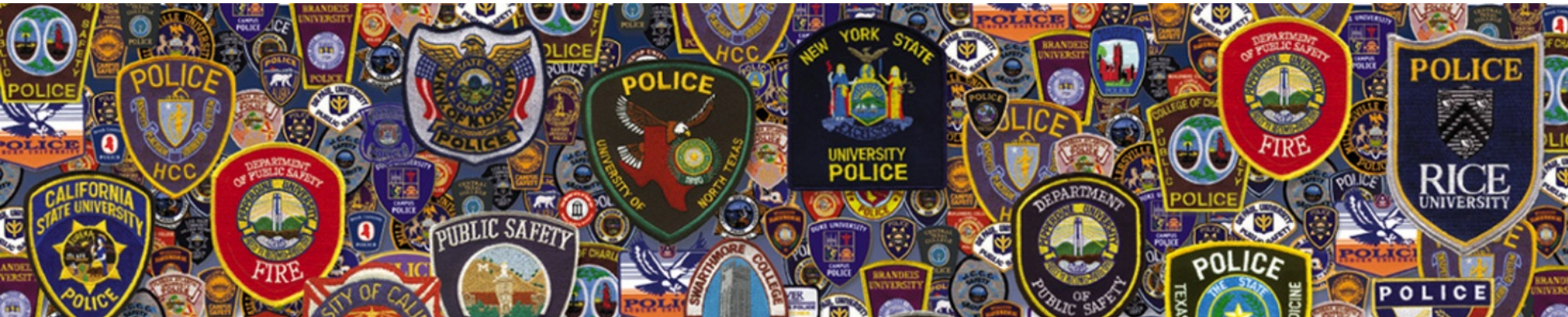
# Leadership Training

## Additional Training for Managers

- Receiving and processing reports
- Trust, preventing false report and retribution
- Referral of reports to Threat Assessment Team
- Tactical interview techniques
- Termination and  suspension of access

## Additional Training for Threat Assessment Task Force

- The institutional threat assessment process
- Local threat updates
- Best practice:  Conduct tabletop exercise using a couple recent or hypothetical case studies that exercise institutional Personnel Security policies



# Conclusions

**Threats are people**

- The focus of security should be on people – Personnel Security

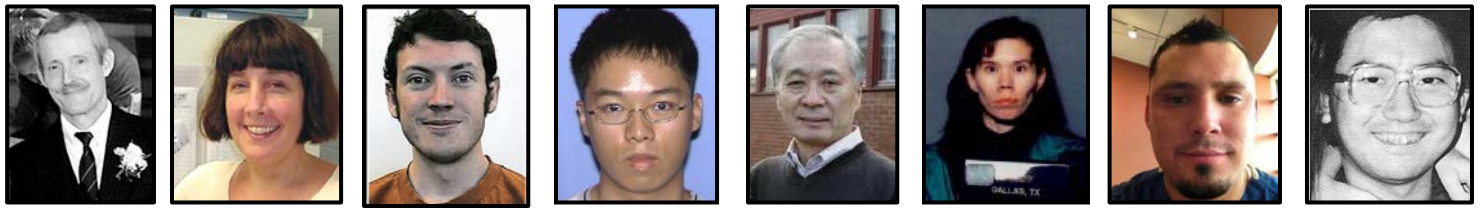
**Violence is a process**

- Threats exhibit behavioral indicators that can be used as the primary data in a threat assessment

**The "brilliant internal guardian"** – the most valuable tool, peer & self reporting. must be protected from:

- Failure to report
- False report
- Reprisal

**Personnel Security -** is the comprehensive framework to monitor behaviors, detect indicators and refer threat cases to an interdisciplinary threat assessment team.



# Resources

**Report of the Virginia Tech Review Panel.** (2007). http://www.governor.virginia.gov/tempcontent/techpanelreport.cfm

**Report of the Expert Behavioral Analysis Panel [redacted]** (2011). http://www.dcd.uscourts.gov/dcd/sites/dcd/files/unsealedDoc031011.pdf

**Hunters And Howlers: Threats And Violence Against Judicial Officials In The U.S., 1789-1993.** Frederick Calhoun (1998)

**Evaluating Risk for Targeted Violence in Schools: Comparing Risk Assessment, Threat Assessment, and Other Approaches.** Reddy *et al.* (2001). http://www.threatresources.com/downloads/evaluating_risk_schools.pdf

**U.S. Secret Service, National Threat Assessment Center** http://www.secretservice.gov/ntac.shtml

**University of Nebraska, Targeted Violence Research Team** http://psych.unl.edu/forensic/Threat_Assessment_Research2.htmlPlaceholder centers of excellence

# Acknowledgments

**Booz Allen Hamilton, Inc.**

Molly Rickard

Michael Majewski, Ph.D.

Jason Griffeth

Tricia Delarosa, Ph.D., CBSP, RBP

Lindsay Odell, Ph.D.

**AtRisk International, LLC**

Chuck Tobin

James Dornak

Daniel Apple

# Mandatory Reportable Information

- Circumstances that may affect SRA status of an individual
- Circumstances that may affect the ability of an individual to perform their job in a safe and secure manner
- Significant changes in behavior, attitudes, demeanor, or actions of an individual
- Stated or implied threats to colleagues, institutions, the security of Tier 1 BSAT, the well-being of laboratory animals, or the general public
- Any information that causes an individual to have concerns about their own ability to perform their job safely and securely
- Any circumstances that appear suspicious such as requests for security or laboratory information without justification, attempts at unauthorized access for friends or colleagues, and unauthorized work alone in a facility at off-hours