State liaisons in matters regarding WMD threats or use.

Contact:
FBI WMD Coordinators are assigned to each of the FBIs 56 field offices to serve as local and state liaisons in matters regarding WMD threats or use.

To report suspicious activity call:
1-855-TELL-FBI or 1-855-835-5324

If there is an Immediate Threat:
CALL 911

Stay Alert
Be Aware
Report Suspicious or Unusual Activities
Protect U.S. Agriculture

ANIMAL – PLANT HEALTH
SECTOR DEFENSE:
AWARENESS AND OUTREACH

The introduction of foreign, emerging, or zoonotic animal diseases, exotic plant diseases or pests, and contaminants can occur by (1) natural incursion, (2) accidental introduction, or (3) as an intentional (criminal or terrorist) act. Due to current world threats, it’s critical to rule out the possibility of an intentional act when confronted with unusual or unexpected disease events and suspicious activities or behaviors in an agricultural, research, or academic environment.

Perpetrators: (1) Domestic – International Terrorists, (2) State sponsored Insurgent / Extremist elements, (3) State sponsored WMD programs, (4) Economic Espionage by corporate or state-sponsored competitors, (5) Insider Threats, (6) an Individual "Lone Wolf".

Motivations and Goals: (1) Terrorism, (2) Technology and Data Theft, Reverse Engineering, and Copyright-Patent Infringement, (3) Economic Espionage, (4) Strategic access and control of agricultural commodity production and capacity, (5) Introduction of high threat disease pathogens for political or economic gain, (6) Intelligence and Sensitive Information Collection, (7) Recruitment or coercion of employees or technical experts, (8) Disruption operations and cyber-attacks, and (9) Hoaxes, false or actual threats, and disinformation operations.

Your work is critical to the national security and economic stability of the United States; therefore, the initial recognition of suspicious events and activities and the rapid notification of APH and LE investigators are critical to identify and interrupt terrorism regardless of the threat material, the target, the individual or group, methods, motivations, or goals.

Agricultural Targets
Evaluate and Enhance Security Measures

Employee / Staff Training Programs:
- Joint agroterrorism detection and response capability.
- Public, animal, plant health, law enforcement agencies, and State Department of Agriculture and USDA Animal-Plant Health personnel.

Joint Criminal-Epidemiological Investigations
- The FBI, USDA, and HHS/CDC have developed the Joint Criminal and Epidemiological Investigations concept to investigate possible intentional (criminal or terrorist) acts against animal, plant, and human health; including the food and agricultural sector.
- The Animal-Plant Health Joint Criminal-Epidemiological Investigations Course, sponsored by the WMD Coordinators at the FBI Field Offices, facilitates Federal, State, and Local personnel from public, animal, plant health, law enforcement agencies, and producer organizations to build field level relationships and joint agroterrorism detection and response capability.

What to Look For: Triggers and Tripwires
- Evidence of agroterrorism is inherently fragile and difficult to recognize and detect. This creates a limited window of opportunity to identify and report threats, suspicious activities, or unusual disease events, and to prevent, investigate, or disrupt planned or ongoing terrorist / criminal operations.
- Triggers and Tripwires are key tools to recognize and report suspicious or unusual events possibly associated with intentional threats or acts of terrorism.
- Definitions: “Triggers” are the first signs or traces of unusual behavior, activities, or disease events that we recognize as abnormal or suspicious. “Tripwires” are specific, agreed-upon threshold levels of these triggers used to activate notification protocols.

Animal-Plant Health Triggers
- Suspicious or unusual disease incidents and investigations
- Theft, loss of accountability, or unauthorized use of pathogens by laboratory personnel
- Detection of key syndromic surveillance clinical signs
- Simultaneous or progressive atypical outbreaks of unusual or atypical diseases in multiple locations with no epidemiological link; or outbreaks of the same disease in animals and people
- Unusual increase in animals with unexplained or unexpected diseases, incidents of high morbidity-mortality and sudden death, or increased incidence of endemic diseases
- Multiple unusual or unexplained diseases in the same animal or herd
- Disease with an unusual geographic or seasonal distribution or atypical signs and clinical presentations
- Similar genetic type among biological agents from geographically different areas; (7) Prevent outside contact with animals, crops, and wildlife; (8) Isolate new animals, segregate age groups and species, follow All-in / All-Out SOPs
- Develop emergency / threat response plans

Animal-Plant Health Triggers
- Suspicious or unusual disease incidents and investigations
- Theft, loss of accountability, or unauthorized use of pathogens by laboratory personnel
- Detection of key syndromic surveillance clinical signs
- Simultaneous or progressive atypical outbreaks of unusual or atypical diseases in multiple locations with no epidemiological link; or outbreaks of the same disease in animals and people
- Unusual increase in animals with unexplained or unexpected diseases, incidents of high morbidity-mortality and sudden death, or increased incidence of endemic diseases
- Multiple unusual or unexplained diseases in the same animal or herd
- Disease with an unusual geographic or seasonal distribution or atypical signs and clinical presentations
- Similar genetic type among biological agents from geographically distinct sources
- Identification of an unusual, atypical, genetically engineered, or antiquated strain of biological agent

Physical Security: Harden the Target
- Restrict access to vehicles, personnel with checkpoints, sign-in / sign-out SOPs
- Badging and identification for employees, delivery, maintenance personnel; (3) Limit points of access / monitor perimeter and internal fencing, gates, and locks; (4) Install adequate lighting, video surveillance, (5) Utilize trained security personnel services

What You Can Do: Security Countermeasures Programs
- (a) Biosecurity; (b) Physical Security; (c) Sensitive and Proprietary Information Security; (d) Cybersecurity.

Employee / Staff Training Programs:
- (a) Threat and trigger awareness; (b) Suspicious activity recognition and reporting protocols; (c) Emergency response protocols; (d) Know your FBI WMD Coordinator, Local Law Enforcement responders, and State Department of Agriculture and USDA Animal-Plant Health personnel.

Biological Security: Prevent Deliberate Acts
- (1) Develop biosecurity plans and management practices for farms / labs / research facilities; (2) Work with USDA-State Dept. of Ag / Cooperative Extension Service / Lab certification SMEs / FBI WMD Coordinators; develop awareness and training programs; (3) Prevent the introduction, spread, or release of diseases and contamination by animals, plants, personnel, equipment, and vehicles by all means of transmission: fomites, direct contact, aerosol / oral transmission, insect vectors, zoonotic / human transmission; (4) Implement SOPs for cleaning & disinfection of equipment, vehicles, feed, water, and supplies; (5) Require employee PPE and shower-in / shower-out SOPs; (6) Restrict staff to functional areas; (7) Prevent outside contact with animals, crops, and wildlife; (8) Isolate new animals, segregate age groups and species, follow All-in / All-Out SOPs
- Implement Biological Select Agent / Pathogen use SOPs for cleaning & disinfection of equipment, vehicles, feed, water, and supplies; (5) Require employee PPE and shower-in / shower-out SOPs; (6) Restrict staff to functional areas; (7) Prevent outside contact with animals, crops, and wildlife; (8) Isolate new animals, segregate age groups and species, follow All-in / All-Out SOPs
- Implement Biological Select Agent / Pathogen use SOPs

On-Going Personnel Suitability Assessments
- (1) Perform background checks, verifying degrees and official transcripts, and conducting interviews with peers or professional references.
- (2) Include a current criminal records check.
- (3) Assess employee performance and suitability; (2) Behavioral changes can develop at any time so continuous assessment is necessary; (3) Have a specific program in place (e.g. peer / self-reporting policies to assess behavioral indicators and ensure reliability; (4) Empower individuals to recognize and detect any threats to themselves or others.

Insiders pose a significant threat because they have the ability to bypass security.

Behavioral Indicators can be found in a broad range of scenarios, such as:
- Falsified credentials
- Unauthorized use of and removing media storage devices and research materials
- Unusual or unauthorized work schedules (e.g. working alone and unobserved at atypical times)
- Plagiarism, faked, and misrepresented data
- Research Sabotage or Espionage
- Colleague Manipulation (Threats, Coercion, Intimidation, and Recruitment efforts)
- Unapproved Experiments
- Vandalism or Theft
- Workplace Harassment or Violence
- Change in personality or espousing extreme personal / political / religious views

Pre-Access Personnel Suitability Assessments
- (1) Evaluate the ability of individuals to comply with biosafety and security protocols; or if they show behaviors that increase the risk of theft, loss, or release of biological agents or sabotage; (2) Includes: Conducting public records, police background checks, verifying degrees and official transcripts, and conducting interviews with peers or professional references.

FBI Weapons of Mass Destruction Directorate
- The FBI has the mission to prevent, detect, and disrupt threats against the agricultural sector from the use of chemical, biological, radiological/nuclear, explosive weapons, and other hazardous contaminants (e.g. CBRN-E).
- The Weapons of Mass Destruction Directorate and the WMD Coordinators (WMDG) assigned to the FBI 56 field offices and over 400 Resident Agencies assist investigations regarding the acquisition and/or use of WMD materials through outreach programs to agricultural partners.

What To Do: Security Countermeasures Programs
- (a) Biosecurity; (b) Physical Security; (c) Sensitive and Proprietary Information Security; (d) Cybersecurity.

Employee / Staff Training Programs:
- (a) Threat and trigger awareness; (b) Suspicious activity recognition and reporting protocols; (c) Emergency response protocols; (d) Know your FBI WMD Coordinator, Local Law Enforcement responders, and State Department of Agriculture and USDA Animal-Plant Health personnel.

Biological Security: Prevent Deliberate Acts
- (1) Develop biosecurity plans and management practices for farms / labs / research facilities; (2) Work with USDA-State Dept. of Ag / Cooperative Extension Service / Lab certification SMEs / FBI WMD Coordinators; develop awareness and training programs; (3) Prevent the introduction, spread, or release of diseases and contamination by animals, plants, personnel, equipment, and vehicles by all means of transmission: fomites, direct contact, aerosol / oral transmission, insect vectors, zoonotic / human transmission; (4) Implement SOPs for cleaning & disinfection of equipment, vehicles, feed, water, and supplies; (5) Require employee PPE and shower-in / shower-out SOPs; (6) Restrict staff to functional areas; (7) Prevent outside contact with animals, crops, and wildlife; (8) Isolate new animals, segregate age groups and species, follow All-in / All-Out SOPs
- Implement Biological Select Agent / Pathogen use SOPs

On-Going Personnel Suitability Assessments
- (1) Conduct annual staff reviews and periodic public records checks (e.g. criminal records, civil orders, driving records) to assess employee performance and suitability; (2) Behavioral changes can develop at any time so continuous assessment is necessary; (3) Have a specific program in place (e.g. peer / self-reporting policies to assess behavioral indicators and ensure reliability; (4) Empower individuals to recognize and detect any threats to themselves or others.

Behavioral Indicators can be found in a broad range of scenarios, such as:
- Falsified credentials
- Unauthorized use of and removing media storage devices and research materials
- Unusual or unauthorized work schedules (e.g. working alone and unobserved at atypical times)
- Plagiarism, faked, and misrepresented data
- Research Sabotage or Espionage
- Colleague Manipulation (Threats, Coercion, Intimidation, and Recruitment efforts)
- Unapproved Experiments
- Vandalism or Theft
- Workplace Harassment or Violence
- Change in personality or espousing extreme personal / political / religious views

Insiders pose a significant threat because they have the ability to bypass security.