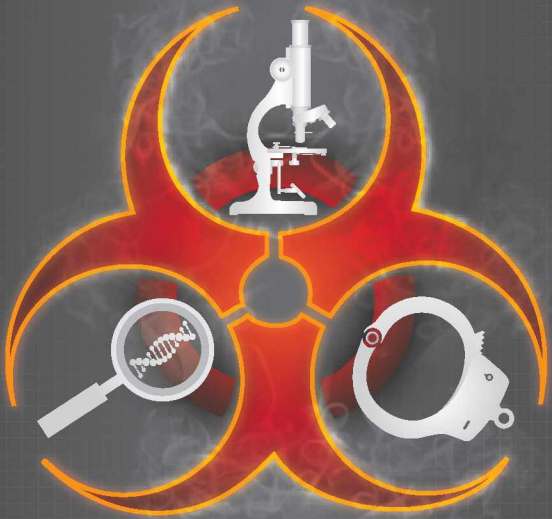
U.S. Department of Justice
Federal Bureau of Investigation

CDC
Centers for Disease Control and Prevention

Criminal and Epidemiological Investigation Handbook

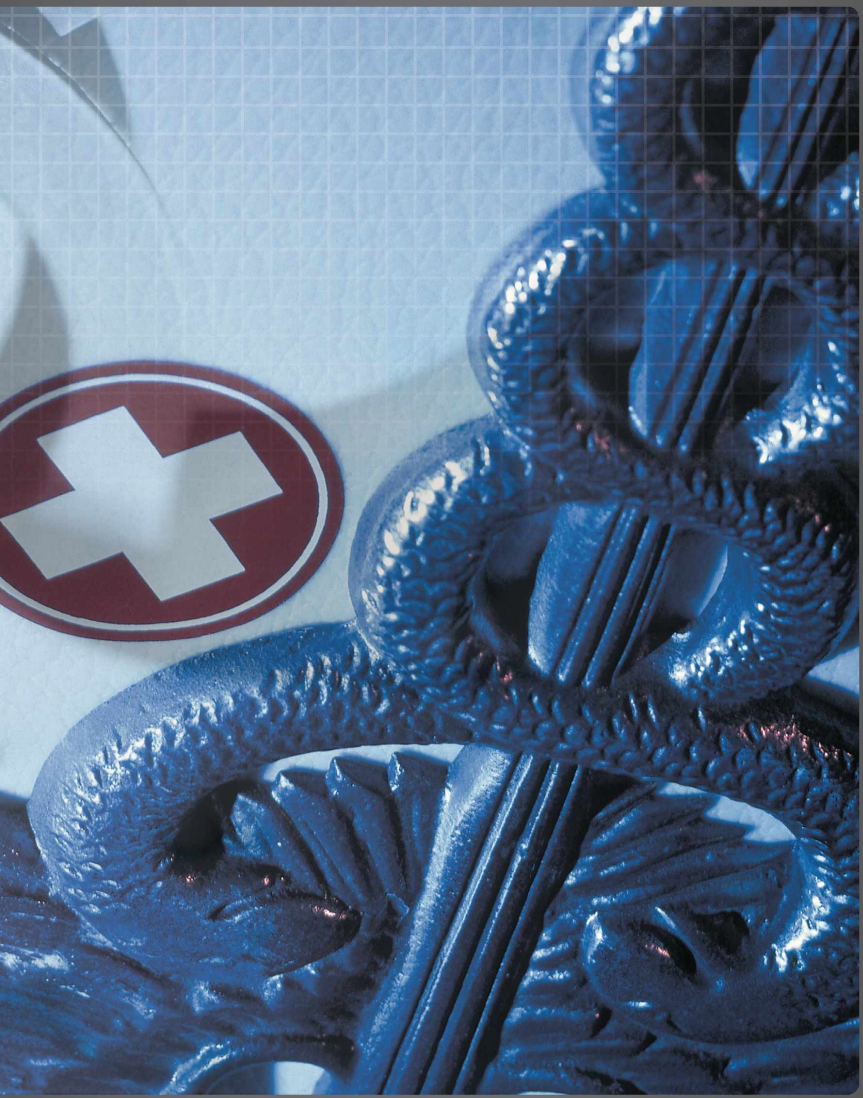


2011 EDITION

TABLE OF CONTENTS

SUMMARY 58-60

INTRODUCTION



INTRODUCTION

Events such as the September 11th attack in 2001 and the mailing of anthrax letters in September and October of that same year have proven that America is vulnerable to acts of terrorism. Current information indicates that, regardless of location, American assets and citizens will continue to be targets of terrorists. Terrorists have demonstrated their willingness to employ non-traditional weapons to achieve their ends. One such class of non-traditional weapons uses biological agents, posing new challenges to both law enforcement and public health. Since biological agents are often endemic or naturally occurring in the environment, a bioterrorism incident may be difficult to detect, and the response to mitigate the effects of a biological attack and apprehend those responsible may be delayed.

In the past, it was common for law enforcement and public health officials to conduct separate and independent investigations. Due to the unique challenges posed by a bioterrorism incident, an effective response calls for a high level of cooperation between these two disciplines. The lack of mutual awareness and understanding, as well as the absence of established communication procedures, could limit the effectiveness of law enforcement's and public health's separate, but often overlapping, investigations. Due to the continued likelihood of a biological attack, the effective use of all resources during a bioterrorism incident is critical to ensure an efficient and appropriate response. By working together, public health and law enforcement can achieve their respective objectives of identifying the biological agent, preventing the spread of the disease, preventing public panic, and apprehending those responsible.

PURPOSE

This handbook has been developed to facilitate the use of resources and to maximize communication and interaction among law enforcement and public health officials in an effort to minimize potential barriers to communication and information sharing during a bioterrorism incident. The purpose of this handbook is to:

- Provide an overview of criminal and epidemiological investigational procedures and methodologies for a response to a bioterrorism incident,
- Enhance the appreciation and understanding of each discipline's expertise by all parties, and
- Identify challenges to sharing information and provide potential solutions that may be adapted to meet the needs of the various agencies and jurisdictions throughout the United States.

Law enforcement and public health officials are encouraged to read the entire handbook and not limit their review to just their respective sections. It is important to take the time to understand the different goals and needs of the other organization before an event occurs. Doing so will enable law enforcement and public health personnel to effectively respond in a coordinated manner during a bioterrorism incident. While both disciplines have varying objectives and protocols, both public health and law enforcement ultimately share two common concerns:

- Early identification of the criminal event or public health emergency, and
- Protecting public health and public safety.

Even with these common concerns, each discipline may be hesitant to share information because of actual or perceived limitations or barriers. Identifying and resolving these issues in advance will facilitate increased dialogue and information exchange of critical information when the next incident occurs.

The 2011 edition of the *Criminal and Epidemiological Investigation Handbook* has been updated based on current policy and includes modifications based upon the experiences gained since the previous version was published.

WHAT IS BIOTERRORISM?

WHAT IS BIOTERRORISM?

DEFINITION OF BIOTERRORISM

According to the Weapons of Mass Destruction (WMD) Statute, Title 18 U.S.C. Section 2332a, bioterrorism is defined as the threat (or conspiracy) to use a weapon of mass destruction, including any biological agent, toxin, or vector as defined in Title 18 U.S.C. Section 178 against a national of the United States or within the United States. The term WMD includes "any weapons involving a disease organism." However, it does not require the actual use of a biological agent. Also, it does not require that the biological agent be a "select agent,[1]" only that that agent is capable of causing biological malfunction, disease, or death in a living organism (Title 18 U.S.C. Section 178).

A *select agent* is a biological agent or toxin that has the potential to pose a severe threat to public health and safety. The United States Department of Agriculture maintains a similar and sometimes overlapping list for agents or toxins that pose a severe threat to animal health and safety, plant health and safety, or to the safety of animal or plant products.

ROLE OF THE U.S. ATTORNEY GENERAL AND THE FEDERAL BUREAU OF INVESTIGATION

In accordance with Homeland Security Presidential Directive-5 (HSPD-5), the Attorney General has the lead responsibility for conducting criminal investigations of terrorist acts or threats by individuals or groups inside the United States, or directed at U.S. citizens or institutions abroad. Generally acting through the FBI, the Attorney

[1]Select agents / toxins are defined by a list of bacteria, viruses, fungi and toxins in the Select Agents Rules (42 CFR 73,3 and §73.4) For a complete list see Appendix 1. [Source: National Select Agent Registry]

General, in cooperation with other federal agencies and departments engaged in activities to protect national security, coordinates the activities of other members of the law enforcement community to detect, prevent, preempt, and disrupt terrorist attacks against the United States.

The National Response Framework assigns responsibility to the FBI for intelligence collection activities within the United States, related to the conduct of criminal terrorism investigations. As such, all federal, state, local, and tribal departments and agencies must notify their local Joint Terrorism Task Force (JTTF) regarding information associated with the threat of terrorism or an actual terrorist incident. The local JTTF consists of representatives from federal, state, and local law enforcement agencies (e.g. United States Secret Service, Immigration and Customs Enforcement, U.S. Coast Guard and state/local law enforcement). At least one JTTF is operational in every one of the FBI field offices located across the United States.

The FBI also has a WMD Coordinator assigned to each of its field offices. WMD Coordinators are responsible for managing the office's WMD program and serve as a point of contact for emergency responders and public health at the state and local level in the event of a threat or incident potentially involving a WMD. In the event of such an incident, the WMD Coordinator serves as a conduit for obtaining federal assistance by contacting FBIHQ WMD Operations Unit (WMDOU) for operational response direction and threat evaluation support.

WMDOU is responsible for overseeing the management of local FBI responses to WMD incidents within the United States (or against United States interests overseas) and coordinates the on-scene WMD threat credibility evaluations (formerly called WMD threat assessments)

with subject matter experts from the FBI and other federal partner agencies (e.g., Centers for Disease Control and Prevention, United States Department of Agriculture, United States Department of Homeland Security and Environmental Protection Agency). In addition, WMDOU provides oversight to all WMD-related criminal investigations. The FBI has multiple operational capabilities to provide assistance in the event of a terrorist attack, including local assets such as the Hazardous Materials Response Team (HMRT) or Special Agent Bomb Technicians, and Headquarters assets such as the Hazardous Materials Science Response Unit (HMSRU), Hazardous Materials Response Team Unit (HMRTU), Hazardous Materials Operations Unit (HMOU), and the Chemical, Biological, Radiological, and Nuclear Science Unit (CBRNSU). Each team or unit provides specially trained assets and capabilities during the course of threat evaluations and investigations.

ROLE OF CDC AND STATE/LOCAL PUBLIC HEALTH

The response to a public health emergency, including incidents of bioterrorism, begins at the state and local level. Public health agencies at the state and local level will likely be the first agencies to recognize cases of illness associated with a bioterrorism incident. Upon recognition of an incident, public health will initiate an investigation and respond to determine the source and implement interventions to prevent additional illness. If the state and local public health agencies need additional resources then they will request federal assistance.

All response is LOCAL!

At the federal level, the Centers for Disease Control and Prevention (CDC) operates according to the National Response Framework (NRF). It primarily provides assistance under Emergency Support Function Annex 8 (ESF-8): Public Health and Medical Services, which is coordinated by the U.S. Department of Health and Human Services. CDC will provide assistance to the state/local public health agencies, as well as manage the federal public health response to the bioterrorism incident, in accordance with guidelines established in the NRF's Biological Incident Annex (BIO-1). This will include coordination with other federal departments and agencies (e.g., Federal Bureau of Investigation, Food and Drug Administration, Environmental Protection Agency, and the Department of Homeland Security) that may be involved in the response.

PUBLIC HEALTH

EPIDEMIOLOGICAL INVESTIGATION GOALS

Whether it is in response to a naturally occurring outbreak or a bioterrorism incident, public health will conduct an epidemiological investigation to determine the source of the disease and the extent of the outbreak. In either situation, the public health investigation may be triggered by the report of an unusual case of illness or the detection of a disease outbreak. When conducting an epidemiological investigation for a naturally occurring outbreak or a bioterrorism incident, public health has the following basic goals:

- ***To protect the public***–Public health professionals utilize surveillance of health trends and medical information to establish methods and implement interventions that protect the public from health threats. Vaccine campaigns, medical countermeasure distribution programs, disease surveillance, and health education all play a role in preventing serious health emergencies.
- ***To stop the spread of disease***–One of the most basic missions of public health is the prevention of illness in the population. While physicians focus on curing the sick and promoting health in the individual, public health practitioners strive for health promotion and disease prevention in the population. Epidemiologists use survey techniques and data analysis to identify the causative agent, determine the source, mode of transmission, and the population at risk for the illness under investigation to limit the spread of the outbreak.
- ***To protect public health and other response personnel***–A major consideration during an investigation is the protection of responders. Since epidemiologists and other responders may come in contact with potentially infectious individuals, provision of proper

protective equipment and other preventive medications or vaccines for investigative personnel is essential.

EPIDEMIOLOGICAL INVESTIGATIVE METHODS

Public health uses investigative techniques to identify the causative agent and to determine the source and extent of disease outbreaks. A public health investigation primarily involves the meticulous accumulation of information from patient interviews, as well as data collected from surveillance systems. Since interview or disease surveillance information may be relevant to a criminal investigation, law enforcement personnel should become familiar with the elements of a public health epidemiological investigation.

The following section provides a brief synopsis of the elements of an epidemiological investigation. The elements are listed sequentially; however, the nature of each outbreak and the availability of personnel will determine the sequence and scope of the actions that will be performed during the investigation.

Detect Unusual Events

The first indication of an unusual event is often an unexpected increase in the number of patients with similar symptoms (i.e, cases). This increase is detected either by monitoring disease surveillance systems or through reports of illness from a healthcare provider. When an unusual event occurs, public health officials will begin collecting information on the cases and the characteristics of the biological agent to determine whether a threat to public health exists. Based on the results of this determination, public health may classify this unusual event as an infectious disease outbreak and begin an investigation to determine the extent of the outbreak and identify the source of illness.

An outbreak is defined as an occurrence of cases that are associated in time, place or person. For example, the state health department may determine that 5 cases of *E. coli* O157:H7 were due to victims having recently consumed unpasteurized apple cider from a local orchard. Since all of the cases have an association with the orchard, the state health department may consider this an outbreak.

Case Reporting

All states possess laws requiring the reporting of specific infectious diseases by healthcare providers. Since there is not a standardized list for all states, the types of disease reported to public health vary from state to state. Generally, case reports of disease are submitted to public health officials by a physician, public health laboratory, hospital, or other healthcare practitioners. In 2002, the Centers for Disease Control and Prevention (CDC) published guidelines encouraging states to add regulations requiring the reporting of diseases likely to be associated with biological terrorism to the list of notifiable diseases for each state.

Public Health Surveillance Systems

Public health surveillance is defined as the ongoing collection, analysis, and interpretation of health data for use in the planning, implementation, and evaluation of public health practices. A surveillance system must include the capacity for collecting and analyzing data, as well as the means to disseminate the data to individuals or groups involved in disease prevention and control activities.

Ideally, a surveillance system will detect the occurrence of disease with sufficient time to initiate an investigation to limit the impact of the disease on the public by implementing prevention and control programs

to decrease morbidity and mortality. For example, the early detection of a contagious disease (e.g., influenza, measles, or smallpox) allows for the implementation of a vaccination program that would greatly reduce the spread of the disease and the number of people affected.

In light of the current potential for a terrorist attack using biological agents, some cities and states have set up syndromic surveillance systems that track a variety of healthcare indicators. Some health care indicators found in surveillance systems may include the following:

- The number of upper respiratory disease cases seen in emergency departments
- The number of ambulance runs within an allotted period of time
- The number of antibiotics or over-the-counter drugs sold at pharmacies

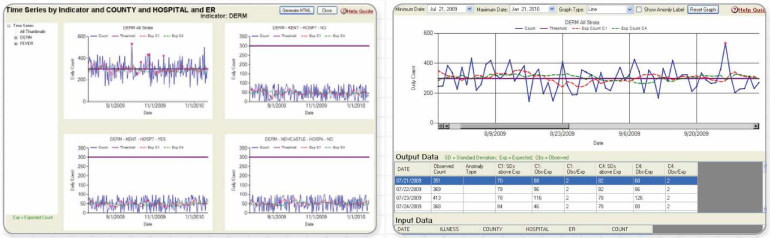


Figure 1: Syndromic Surveillance Data

This is an example of the output from the Early Aberration Reporting System (EARS), one of several syndromic surveillance systems available in the United States. The dash line is the expected number of cases that would be reported based on historical data. The solid line is the actual number of cases reported. The stars indicate where a disease might be out of the normal range expected in the given area. Public health investigators would follow up with healthcare providers to find out if something is going on.

It should be noted that syndromic surveillance systems are not guaranteed to detect the occurrence of an outbreak. Since many bioterrorism agents present with symptoms similar to common ailments, it is thought that monitoring and analyzing healthcare indicator data will allow for rapid detection of covert bioterrorism attacks.

Confirm the Diagnosis

Diagnosing the potential disease agent begins with medical personnel obtaining medical histories and conducting physical examinations of the affected individuals. A medical history is the record of medical conditions during a physical examination and usually includes information on recent events, symptoms, travel, or any unusual circumstances that may have contributed to the illness. Based on this information, the physician or public health official may request laboratory tests to aid in the diagnosis. Physicians are likely to make an initial diagnosis and initiate treatment before laboratory test results are available since early treatment of the disease increases the probability the patient will recover from the illness.

Perform Laboratory Analysis of Specimens and Samples

Diseases are often diagnosed by clinical signs and symptoms. This process can be imprecise based on the nature of illness, especially for many bioterrorism agents since they initially present with symptoms similar to common infectious diseases (i.e., influenza). Therefore, laboratory analysis of medically relevant samples is used to assist the physician in making a definitive diagnosis.

The materials that are typically collected to support a diagnosis or assist with a public health investigation may be clinical specimens

(e.g., tissues, blood, and sputum) or environmental samples (e.g., food, water, air, dusts, powders, surface swabs). Some environmental samples may be considered hazardous materials and require specialized training and equipment for collection. Other samples consist of living intact materials, necessitating refrigerated or frozen transport of materials and/or extremely rapid delivery. Not all laboratories possess the capabilities to test for every biological agent; this may require specimens or samples to be transported out-of-state to another facility.

Public health officials may develop a strong hypothesis about the cause of the outbreak as they accumulate additional clinical laboratory and investigative information; however, most senior health officials will wait for definitive laboratory results prior to confirming the diagnosis if biological terrorism is suspected. The principal reason for waiting for confirmation is that different analytical methods have different specificities. For example, some vendors claim their field assay tests quickly indicate the presence of a biological agent; however, the lack of specificity and comparably higher detection limits of these field assay tests make the use of an approved laboratory test critical. A field assay test combined with the clinical symptoms might suggest that a particular biological agent is present, but the field assay test alone cannot determine with absolute certainty that a particular biological agent is or is not present. Until the public health officials obtain the results from the confirmatory diagnostic test in an approved laboratory, the diagnosis is considered unconfirmed or presumptive.

Laboratory Response Network

Laboratories vary in their ability to test for biological agents. For example, forensic laboratories that process criminal evidence may not be equipped to test for biological or chemical agents or know how to handle these specimens appropriately. The FBI, CDC, and the Association of Public Health Laboratories (APHL) have established the Laboratory Response Network (LRN), which is a network of laboratories located across the country that possess the expertise to conduct appropriate analyses with approved equipment, qualified personnel, validated assays, and accepted practices. LRN laboratories meet certain standards and continue to demonstrate their readiness through proficiency tests that validate their ability to correctly identify biological and chemical threat agents. Sending a specimen to a non-LRN laboratory could dramatically delay the investigation and destroy material required to confirm the agent's identity and properly diagnose the causative agent of an illness. Additional information on the Laboratory Response Network is located in Appendix 3.

Due to their expertise and proficiency, only LRN facilities should be used to test clinical specimens or environmental samples for the presence of biological or chemical agents. Law enforcement agents should contact their local FBI WMD coordinator to determine the location and procedures for submitting samples to the nearest LRN.

Identify and Characterize Additional Cases

This element of a public health investigation has many similarities to a law enforcement investigation and is often referred to loosely as "shoe leather epidemiology" due to the time

and resources required to obtain the necessary case and contact information through interviews.

The first confirmed case of an outbreak is referred to as the index case. To prevent further impact from the disease and to try and find the source of the disease, there is a great need to identify new cases, unreported or unrecognized cases, and contacts. In the search for additional cases, public health officials will interview family members, associates, co-workers, and other possible contacts of the index case. These interviews require extensive time and personnel commitments. Interviewees may be contacted multiple times as the investigation proceeds if there is a need to obtain additional information. Information collected by public health investigators can include the following:

- Demographic data (name, address, age, race, ethnicity, gender)
- Clinical data (signs and symptoms, duration, onset, etc.)
- Exposure history (travel, meals, and significant events; all based on the type of illness suspected)
- Case contacts and knowledge of other cases

In addition to interviewing the case and contacts, public health officials will attempt to identify additional cases of disease by using a set of criteria called a case definition. The case definition allows public health officials to identify other reports of illness, both within and outside their jurisdiction, which may be related to the outbreak. The case definition is provided to hospitals, ambulatory clinics, and possibly private health practitioners to determine if anyone with a similar illness is currently, or was recently, in the hospital or received medical treatment. Public health officials may also solicit assistance from the media in trying

to identify additional cases. For example, public health may use the media to inform the public that anyone with a certain type of skin rash and fever may be potentially exposed to an agent and should report to their health practitioner for an examination. Once additional cases have been identified, public health officials will collect information on each one to determine whether their illness could be associated with the outbreak.

Determine the Source of Exposure

Once the case/contact interview information has been collected, it is reviewed and analyzed to identify common exposures and, ultimately, determine the source of the illness. This process is known as descriptive epidemiology.

Traditionally, an outbreak is analyzed by creating a histogram (bar graph that estimates a probability distribution) in which the number of disease cases are plotted by date or time of onset in order to visualize the progression of the outbreak. This bar graph, called an epidemic curve (epi curve), provides a visual representation of an outbreak's magnitude over a specific time period and can provide critical clues regarding the outbreak's onset and duration.

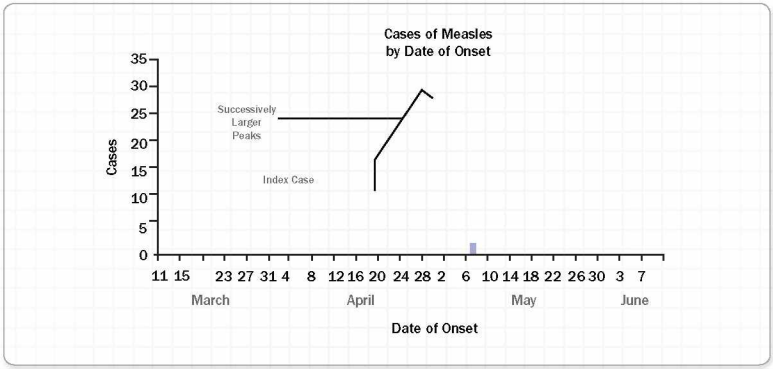


Figure 2: The Epi Curve

This is a diagram of the number of cases and when they occurred. It helps public health determine the source and spread of an outbreak.[1]

Once the descriptive epidemiology has been reviewed, public health investigators will try to develop a "best guess" for the source(s) of illness. This best or informed guess is known as a hypothesis. For example if multiple cases shared an exposure, such as attending the same organized event, then public health officials may develop a hypothesis that the common event is the source of the disease.

To determine whether a hypothesis is correct, public health investigators conduct a statistical analysis or study. This process is known as analytical epidemiology. The statistical analysis provides public health with mathematical evidence to confirm or reject the hypothesis. If the analysis confirms a hypothesis then public health personnel will develop and implement an intervention to prevent people

[1]Source–"Constructing an Epidemic Curve,"
http://www.cdc.gov/globalhealth/fetp/modules/MiniModules/Epidemic_Curve/page06.htm

from becoming ill. If a hypothesis is rejected by the analysis then public health will develop a new hypothesis regarding the source of illness and will continue to search for additional cases in order to obtain additional information.

Develop and Implement Interventions

The ultimate aim of a public health investigation is to identify the source of the disease and implement a plan to control the outbreak and protect public health. Often there is a need to develop and implement an intervention before the disease agent has been confirmed in order to ensure a successful intervention. Many illnesses, such as anthrax, can be treated successfully if prophylactic antibiotics are provided early in the course of the illness. Also quarantine or isolation measures, if required to control spread of disease, must be implemented early in an outbreak to be effective. Therefore, in the case of bioterrorism, interventions are often initiated based on the suspicion of disease rather than waiting for confirmation. Early suspicion, coordinated with law enforcement intelligence, can help public health intervene as quickly as possible and save lives.

LAW ENFORCEMENT

CRIMINAL INVESTIGATION GOALS

During a biological attack, law enforcement agencies have a set of primary goals just as the public health community does. These goals include the following:

- ***To prevent a criminal act and subsequent attacks***–Through ongoing surveillance, investigation, and intelligence-gathering techniques, law enforcement personnel obtain information to identify potential terrorists, their targets, and methods of attack before an attack takes place.
- ***To identify, apprehend, and prosecute the perpetrators***–Once a biological attack occurs, law enforcement obtains evidence and information to identify and apprehend the individual or individuals responsible for the attack. Collection of evidence includes interviewing victims and witnesses as well as obtaining and preserving physical evidence. A criminal investigation into a biological attack is not complete until there is a successful prosecution and conviction of those responsible for the attack.
- ***To protect law enforcement personnel***–Law enforcement personnel, including FBI agents, are likely to encounter situations where they may be at risk for exposure to a biological agent. Since some biological agents can be both infectious and contagious, provision of proper protective equipment and other preventive medications or vaccines for law enforcement personnel is essential.

PREVENTING BIOLOGICAL ATTACKS

The first step in preventing a biological attack is to attempt to identify potential terrorists or terrorist organizations that are both capable of and interested in executing a biological attack. This process allows

FBI and other law enforcement officials to identify potential targets and possible modes of attack. Despite all efforts, a biological attack may not be prevented; therefore, appropriate federal, state, and local agencies must be prepared to respond to an incident either while it is occurring or after it has been perpetrated.

FBI WMD Threat Credibility Evaluation—Real or Hoax

FBI/law enforcement personnel may be confronted with a number of situations involving the actual or threatened use of a biological agent as a weapon. Bioterrorism situations FBI/law enforcement will respond to include non-credible threats (hoaxes), announcements or indications that a release of a biological agent has occurred (overt), or unannounced releases of a biological agent (covert).

All situations involving the intentional use of a biological agent require an FBI-led threat credibility evaluation. In some jurisdictions, a local threat assessment (see Appendix 5) may support the FBI threat credibility evaluation. Upon notification of a WMD threat or incident (e.g., an overt release such as a white powder letter accompanied by a threat), state and local law enforcement or emergency responders will contact their FBI WMD Coordinator to initiate the threat credibility evaluation process. The WMD Coordinator will then contact FBIHQ Weapons of Mass Destruction Operations Unit (WMDOU), which is responsible for convening a conference call to support the evaluation. The threat credibility evaluation consists of the three following factors, plus an assessment of available intelligence and/or case information to determine the credibility of a threat:

- ***Behavioral Resolve***–Does the perpetrator display behavior indicating the resolve to carry out the attack?
- ***Operational Practicability***–Do the operational aspects of the attack make it possible?
- ***Technical Feasibility–***Do the technical aspects make an attack feasible?

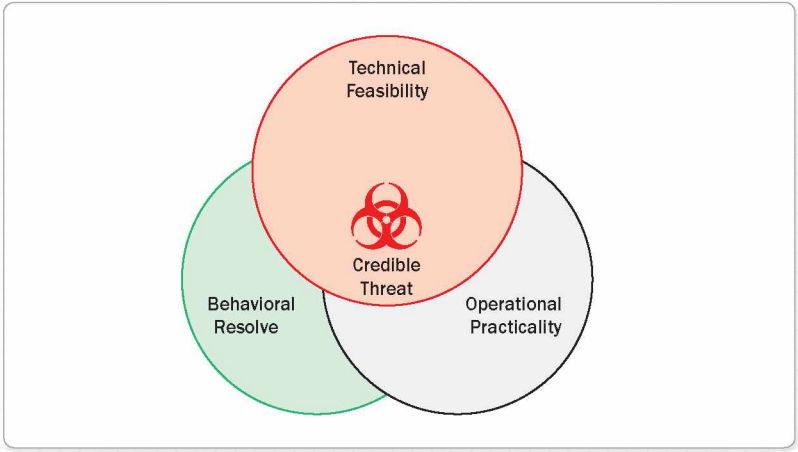


Figure 3: Diagram of FBI WMD Threat Evaluation Process
When a threat is made by a person or organization that has the technical know-how, the ability to pull it off and the willingness to carry out that threat, it is considered credible and must be managed appropriately.

During the course of the threat credibility evaluation, WMDOU may contact various federal partners and subject matter experts (e.g., CDC or United States Department of Agriculture) to assist in determining the threat credibility. In the event the threat is deemed credible, the FBI

Strategic Information and Operations Center (SIOC) will notify the DHS National Operations Center (NOC) immediately. After the threat has been deemed credible, the FBI WMD Coordinator, along with state and local responders, will consult with FBIHQ assets to determine the next course of action, specifically regarding how to best collect and analyze the evidence, including biological environmental samples and other evidence.

If the threat is deemed non-credible, FBI may initiate an investigation to identify and prosecute those responsible for creating the perception that there was a threat (i.e., a hoax). Under federal law (18 U.S.C. 2332a and 18 U.S.C. 175), a threat involving a disease-causing organism is a criminal act, whether or not the perpetrator actually possesses the biological agent.

During an unannounced or covert event, the public health and medical community will likely be the first to identify that a bioterrorism incident has occurred since the first indicator of an attack will be patients seeking treatment for an unexplained illness. As soon as public health suspects an intentional event, the local FBI WMD Coordinator should initiate the threat evaluation process to determine the likelihood of an intentional biological attack. If public health officials and FBI have established a working relationship prior to a bioterrorism incident, public health officials may feel more comfortable contacting FBI early in their investigation, which allows for more rapid initiation of the threat evaluation process.

CRIMINAL INVESTIGATIONS

FBI and law enforcement personnel conducting criminal investigations must operate within the applicable laws governing the investigations and the ensuing prosecution. As information is collected, it is necessary for the law enforcement investigator to develop a thorough understanding of the investigation and the unique circumstances of the case. This will help law enforcement to identify any missing or weak evidence, which may impact the ability to apprehend, prosecute, and convict the individual responsible for committing the crime. A brief summary of criminal investigation procedures is provided below. While the steps are presented sequentially, some aspects of the investigation may occur simultaneously.

Gather Evidence

The process of gathering evidence during the investigation of a bioterrorism incident will involve collection of physical evidence (e.g., dissemination devices, clothing of victims and suspects), clinical specimens (e.g., blood or other bodily secretions), documents, photographs, and witness statements. Law enforcement personnel must consider a variety of issues to ensure that any evidence they gather can ultimately be used in a criminal prosecution. The list below provides a summary of some of the key issues law enforcement must consider when gathering evidence.

- ***Chain of Custody***–Is there a methodology used to track and maintain control and accountability of all evidentiary items? This may include the initial collection of evidence through the final disposition of the specimens. Chain of custody is an issue of significant concern during a criminal investigation. Both law enforcement and public health personnel must provide accountability at each stage of

collection, handling, testing, storing, transporting the evidentiary items, and reporting any test results. Responders should implement formalized chain of custody procedures once there is suspicion that a crime has occurred. Failure to properly maintain the chain of custody may render the evidence unusable at trial.

- ***Delivery of Biological Samples to the LRN***–Only labs within the Laboratory Response Network (LRN) should be used to test for biological agents. Submitting evidentiary biological samples to a non-approved lab will not only delay proper analyses, but may result in unintentional contamination of the samples and may be used to create doubt about the validity of test results in court. The FBI WMD coordinators maintain a list of LRN laboratories within their field office's area of responsibility.
- ***Documents***–Original documents should be obtained by law enforcement when possible. Issues of authenticity and admissibility arise if copies are relied upon when original documents are available.[4]
- ***Witness Statements***–Witness descriptions of dissemination devices, vehicles, suspects, odors, tastes, sounds, and other specific information must be obtained as soon as possible after a bioterrorism incident. Witness information is "time sensitive" and the sooner the information can be obtained, evaluated, and disseminated to other investigators, the more value it adds to the investigation. As time passes, the danger increases that a witness's memories can fade or become influenced by the opinion of other individuals.

[4]Potentially contaminated documents should be stored and examined utilizing procedures which protect both the individuals handling the evidence and the evidence itself.

During a bioterrorism investigation law enforcement may need to decide between collecting evidence for public safety or for criminal prosecution. There may be an overriding need by authorities to identify the agents or materials as soon as possible to ensure that the proper response is implemented and steps are taken to protect the responders and the public. In this instance, the need for rapid collection and testing to save lives outweighs normal evidence collection procedures.

Evaluate Evidence

As evidence is gathered and collected, an ongoing evaluation of the evidence must be part of the investigative process. An understanding of evidence types and the rules governing its admissibility will lead to better evaluations of the evidence as the criminal investigation progresses. While not intended to be all-inclusive, Table 1 identifies and provides a brief explanation of some types of evidence collected during a criminal investigation.

TYPE OF EVIDENCE	EXPLANATION	EXAMPLE
Circumstantial	Facts, if proven, that allow the investigator to draw conclusions. In most jurisdictions, circumstantial evidence has the same probative value as direct evidence	Suspect was treated for cutaneous anthrax at or about the same time a release of anthrax was attempted
Direct	Documents, records, physical evidence, notes, computer data, videotapes, or other types of information that directly relate to the case	Vehicle rental agreements, purchase receipts, phone records, eyewitness statements, dissemination devices
Trace	Minute particles of matter that can be examined microscopically, physically, and/or chemically	Biological agent residue, fingerprints, DNA, biological properties of the agent

TYPE OF EVIDENCE	EXPLANATION	EXAMPLE
Hearsay	Statements offered to prove the truth of the matter asserted; the declarant is unavailable for cross-examination	A statement taken from a third party who heard another person describe seeing the suspect spray a substance during the time in question
Eyewitness Testimony	Observation or sensation personally seen, smelled, heard, felt, or tasted	Witness reported smelling a particular odor, hearing a specific sound, or seeing someone

Table 1. Types of Evidence Collected During an Investigative Process

Generally, law enforcement is accustomed to receiving results quickly when the event is significant, such as a death or high profile crime. Since evidence collected in a potentially contaminated environment must be assumed to be contaminated, this significantly complicates the evidence review and evaluation process. The FBI has specially trained teams to handle the apprehension and collection of evidence in contaminated WMD environments. There are 27 Hazardous Materials Response Teams that provide coverage of the FBI field offices, as well as specially trained FBI personnel, such as microbiologists and other scientists, trained to collect contaminated evidence. Following a bioterrorism attack, the FBI will need to have the collected evidence analyzed in a laboratory to support and guide their investigation. As mentioned before, only laboratories approved to handle biological evidence, such as those in the Laboratory Response Network, may accept samples. It is also possible that samples will go to approved FBI laboratories, but this needs to be carefully planned with public health to ensure that everything needed to protect health is available to them.

From the beginning of a criminal investigation of a bioterrorism incident and until the case is submitted to a jury for a verdict, all facts collected during the investigation must be verified and inconsistencies resolved. Documents must be carefully reviewed to ensure they have been thoroughly analyzed and interpreted correctly. Sometimes information contained in statements or reports is subject to differing interpretations. Law enforcement investigators must examine the evidence for conflicting interpretations and resolve these issues, or be prepared to explain the contradictions to the prosecutor. Once evidence has been collected and analyzed, it is important to submit all materials (e.g., statements, laboratory reports, documents, photographs) to the prosecutor in an organized manner to ensure all of the facts are identified before the trial. Sufficient time should be allowed to permit the prosecutor to meet with the investigators and witnesses to review all reports, evidence, and anticipated testimony.

During the investigation of a bioterrorism incident, similar to that of other criminal investigations, investigators never know what nuance or piece of information will be the crucial break needed to identify, arrest, and convict those responsible for the criminal act.

Apprehend Suspect(s)

Once the threat to public health and safety has been eliminated, the top priority for law enforcement is the apprehension and prosecution of those responsible for the attack. During the apprehension of a suspect or group of suspects, law enforcement involved in the arrest need to take precautions against possible injury from the perpetrator(s). It is also possible that the arresting officers will be confronted with either a contaminated environment or contaminated evidence. Therefore,

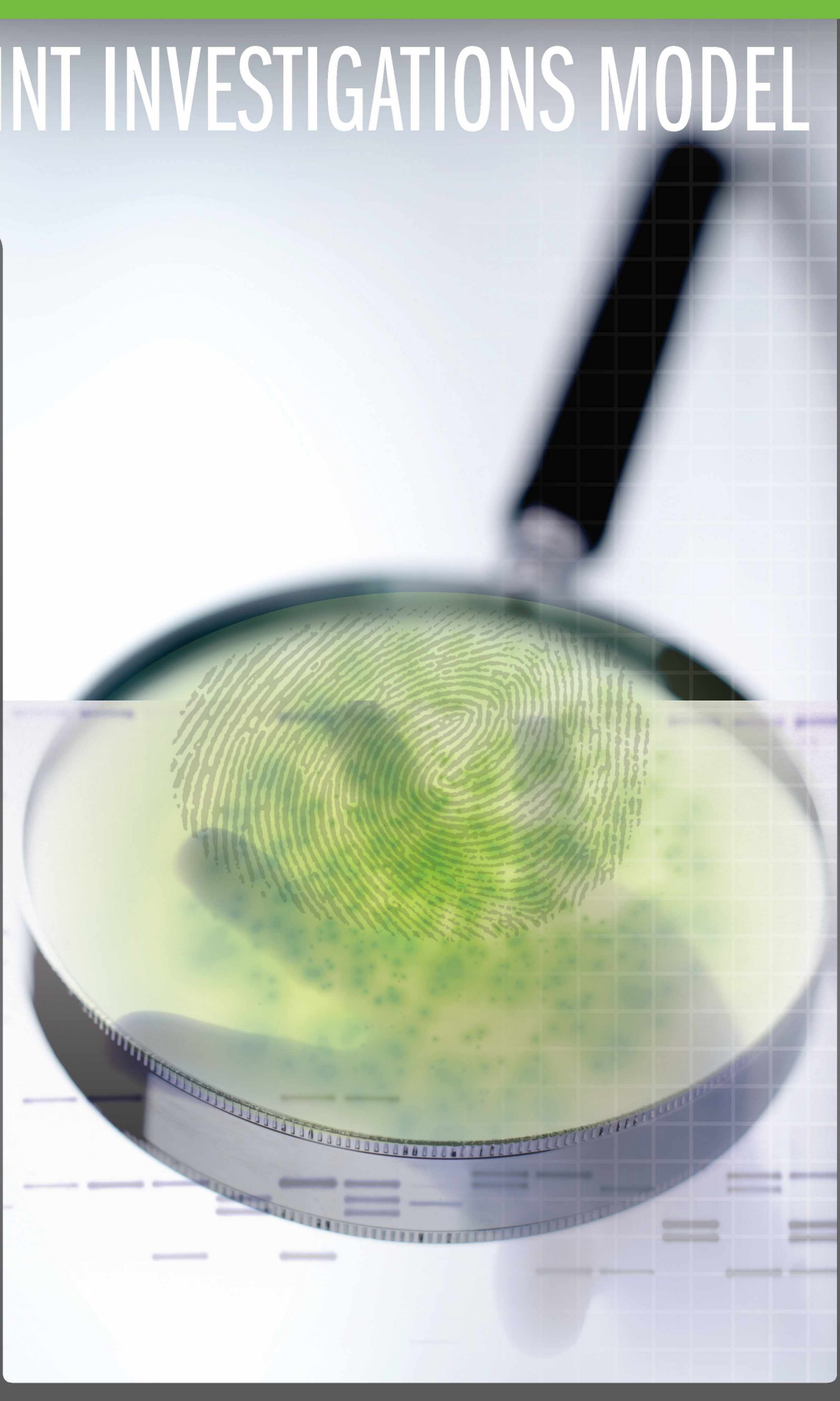
appropriate personal protective equipment (PPE) must be utilized to prevent contamination by any biological agent in the environment. While apprehending the suspects is a goal of the criminal investigation, the safety of the arrest team and the general public is paramount.

Render Testimony

Each potential government witness should be available to meet with the prosecutor before he or she testifies at trial. It is important for the prosecutor to have the opportunity to evaluate how each witness and his or her statements may appear to the jury. During this time, any issues, problems, discrepancies, or gaps in the evidence or testimony can be discussed and resolved.

The Joint Investigation Model highlights several practices and procedures that can be used by public health and law enforcement to increase collaboration and partnership. Since every agency and jurisdiction is different, it is possible that certain items may not be applicable.

JOINT INVESTIGATIONS MODEL



JOINT INVESTIGATIONS MODEL

INTRODUCTION

Collaboration between law enforcement and public health has not always been recognized as beneficial. In the past, it was not uncommon for law enforcement and public health to conduct separate and independent investigations during the response to a biological incident; however, since the 2001 anthrax mailings, law enforcement and public health have gained considerable experience. Experience gained from this and subsequent responses involving biological agents continue to emphasize the need for law enforcement and public health collaboration during a bioterrorism investigation. A mechanism for increasing cooperation and coordination between law enforcement and public health is the Joint Investigation Model. The Joint Investigation Model is not solely limited to the investigative process; rather, it incorporates a number of procedures and methodologies that require interaction between law enforcement and public health prior to the detection of a bioterrorism incident and through its resulting investigation. The Joint Investigation Model is composed of several elements:

- Memorandum of Understanding/joint protocols,
- Information sharing,
- Joint threat assessments, and
- Joint interviews.

Benefits of Joint Investigations

Public health and law enforcement share a set of common goals during the response to a bioterrorism incident:

- Protecting the public,
- Preventing or stopping the spread of disease, and
- Identifying those responsible and
- Preventing future attacks.

The Joint Investigation Model allows law enforcement and public health to achieve their common goals by enabling a more efficient response to a bioterrorism incident, which results in earlier detection of an attack, identification of a source, and implementation of interventions, which can mitigate the effects of the outbreak. Additionally, the Joint Investigation Model highlights the need to combine the investigative efforts of law enforcement and public health, which minimizes potential discrepancies between investigators and maximizes the opportunities to identify, apprehend, prosecute and convict the perpetrator of the attack.

Law Enforcement Benefits:

When operating under the Joint Investigation Model, law enforcement personnel have

- Access to experts who understand disease epidemiology (e.g., symptoms, diagnosis, possible causes) and
- Access to relevant public health/medical information (e.g., results of the epidemiological investigation that may inform the criminal investigation).

Public Health Benefits:

When operating under the Joint Investigation Model, public health officials have

- Access to law enforcement case information that helps determine the source of the illness and
- Assistance in containing the outbreak from law enforcement personnel (who can help identify information that may lead to apprehending the perpetrator, thus preventing future exposure and illness)

The remainder of this section describes how law enforcement and public health can implement the joint investigation methodologies for their agencies and jurisdictions.

Joint Protocols/Memorandum of Understanding

The creation of a Memorandum of Understanding (MOU) and/or joint protocols helps to establish joint investigative guidelines between law enforcement and public health. Guidelines identify jurisdiction roles and responsibilities for law enforcement and public health agencies, as well as investigational procedures for the response to a bioterrorism incident or other naturally occurring biological incidents. In general, the MOU/joint protocols may outline the following components:

- Triggers/indicators
- Threat assessments procedures
- Investigative procedures
- Interviews of cases and contacts
- Sharing of investigative results
- Analysis of information

The development of a MOU/joint protocols is a difficult task, requiring the input and agreement of many entities within law enforcement and public health. To assist agencies and jurisdictions with the creation of an MOU/joint protocols, the CDC (U.S. Department of Health and Human Services) and the Bureau of Justice Assistance (U.S. Department of Justice) convened a Public Health and Law Enforcement Emergency Preparedness Workgroup that developed a model MOU for joint public health and law enforcement investigations.[5]

INFORMATION SHARING

Public health and law enforcement officials are encouraged to notify and involve each other early in a potential investigation of a biological threat, even if it turns out to be a non-criminal event. The establishment of pre-incident communication mechanisms is essential for the expeditious exchange of information during an actual biological incident. This exchange of information requires law enforcement and public health personnel to be familiar with one another, and to know who should receive the information.[6]

Potential Challenges to Information Sharing

There are challenges to sharing information between public health and law enforcement. The challenges are both perceived and real, and should be addressed before both agencies can legally and safely share information and conduct joint investigations.

[5]The model Memorandum of Understanding can be found online at: http://www.nasemso.org/Projects/DomesticPreparedness/documents/JIMOUFinal.pdf

[6]The NRF includes a requirement to notify the National Response Center at 1-800-424-8802.

Public Health Challenges

The first potential challenge is that the public health community is concerned it will be held legally liable for the release of patient information without the patient's consent. Due to the Health Insurance Portability and Accountability Act (HIPAA) and applicable state laws, public health considers patient medical information as confidential. Challenges arise when law enforcement requires access to patient clinical samples and/or sample results, as well as specific information from patient health records at hospitals, health maintenance organizations, or the Centers for Medicare and Medicaid Services. Due to the protected nature of the information, certain challenges are posed to public health when law enforcement requires this information because it may be potential evidence of a crime.

A second potential challenge to the exchange of patient information is based on issues of ethics and trust. Patients provide detailed information to the medical community with the tacit understanding that physicians and public health professionals will retain the information in confidence. The public health community has expressed concern that providing confidential patient information to the law enforcement community, regardless of reason or intent, may jeopardize their future ability to obtain data critical to identifying and treating patients.

Law Enforcement Challenges

The law enforcement community may also have concerns regarding the exchange of investigative information. It may be reluctant to provide information that may jeopardize the safety of confidential informants or the security of classified sources. Information obtained by law enforcement personnel from informants is frequently so sensitive that if the information were exposed, the suspects would be able to

determine exactly who provided the information to law enforcement officials. As a result, the more people who have access to the sensitive information, the greater the possibility the information source will be exposed.

Additionally, the law enforcement community is concerned that suspects might avoid detection as a result of the exchange of sensitive information. For example, if law enforcement personnel ask the public health community to look for a specific individual or group, the number of individuals that know the specifics of the case will increase. As in any investigation, the more people that have access to sensitive information, the more opportunities exist for inadvertent disclosure of the information. As a result, there is a greater opportunity for the sensitive information to inadvertently leak back to the suspected perpetrators, thus giving them the advanced warning needed to facilitate the destruction of evidence, possibly avoid detection, and potentially affect a successful prosecution of the perpetrator(s).

Legal Issues Related to Information Sharing

Each agency's Office of General Council is encouraged to evaluate federal, state, and local laws and regulations to determine ways to share information. A review of the applicable federal and state statutes should be conducted to determine the actual limitations and the exceptions that may exist. For example, the HIPAA prevents an individual's health information from being released without that individual's consent; however, there are specific exemptions in HIPAA that allow for the release of patient medical information to public health officials and law enforcement. One exemption relevant to a law

enforcement investigation is often identified as the "imminent threat exemption." According to this exemption:

> **"A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the covered entity, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and the disclosure is made to a person reasonably able to prevent or lessen the threat (See 45 CFR 164.512 (j)(1)(i)).**"

The legal basis for allowing patient medical information to be shared with law enforcement should be researched and incorporated into a MOU/joint protocol so all entities are properly informed and can comply with the legal requirements to share information.

Proposed Solutions to Increase Information Sharing

Law enforcement and public health need to overcome these barriers or challenges for information sharing. A first step is to develop a working relationship. Many of the perceived barriers to sharing information will be addressed as each discipline begins to understand each other's role and information needs and develop trust that information will be properly protected by their counterpart.

Law enforcement and public health communities are usually more willing to exchange information once they have confirmed the existence of a criminal act or an outbreak, but in many cases this may be too late. The timely exchange of information in the early stages of a response is critical to contain the outbreak and apprehend the perpetrators. Table 2 identifies ways for law enforcement and public health to improve information exchange before and during a naturally-occurring outbreak or a bioterrorism incident.

RECOMMENDATIONS
Develop Close Personal Relationships–Strong personal ties between law enforcement and public health personnel tend to foster increased information exchange. Law enforcement and public health personnel have indicated they would be more likely to provide information to their counterparts early in the process if they had worked, talked, or met with them on a regular basis.
Establish a Bioterrorism Working Group–This group can be created from an existing group, such as the local FBI Field Office WMD Working Group, or it may be a new group. The working group should include representatives from all the agencies that may be involved in a response to a biological incident in the jurisdiction. This forum permits each individual to identify agency needs, bioterrorism response gaps, and recommended ways forward. Moreover, a working group helps foster personal relationships between response officials.
Create a Memorandum of Understanding–between the local FBI field office, local law enforcement, and public health which details the procedures for information exchange, threat assessments, joint interviews, and training. Establishing agreements that identify the rules for information exchange and release will help address many of the actual or perceived challenges and barriers. These agreements should identify the type of information to be shared and restrictions on release to prevent access by unauthorized personnel. (Appendix 6)
Conduct Training–Statements offered to prove the truth of the matter asserted; the declarant is unavailable for cross-examination
Create a State or Local Bioterrorism Response Plan–As applicable, establish a group of the relevant local, state, and federal responder communities, particularly those in public health and law enforcement, to create the state (or local) Bioterrorism Response Plan. Procedures should include responses to both overt and covert incidents.

Table 2. Information Exchange Recommendations

Information Exchange Triggers

During a bioterrorism incident, certain information or a specific event should trigger the exchange of information between law enforcement and public health. For example, law enforcement conducts criminal investigations every day, and in recent years, there have been numerous biological hoaxes. What should prompt the law enforcement community to contact public health and involve them in the investigation of such an incident? Similarly, epidemiological investigations take place routinely. Most epidemiological investigations have nothing to do with terrorism. At what point during an epidemiological investigation should public health be prompted to contact law enforcement?

Many factors could provide clues to potential biological threats or events. The difficulty of trying to use definitive criteria is that almost all infections produce symptoms that mimic other diseases in their early presentation. Furthermore, many classic bioterrorism agents cause rare, non-endemic, or eradicated diseases often with unknown or poorly characterized etiology; as a result, general practitioners may not recognize the disease until it has progressed to the more serious and unique symptoms associated with it. In these cases, there may be a reluctance to report this "unknown" illness until a diagnosis is made.

The following tables provide a preliminary list of factors that could trigger public health (Table 3) or law enforcement (Table 4) to share information. These tables are not intended to be all-inclusive. Law enforcement and public health may want to add or remove triggers to suit their individual needs.

PUBLIC HEALTH TRIGGERS
· Any specimens or samples (clinical or environmental) submitted to public health for analysis that test positive for a potential bioterrorism-related organism
· Single case of disease caused by a Category A agent (i.e., anthrax, tularemia, smallpox, botulism, viral hemorrhagic fevers, or plague)
· Large numbers of patients with similar symptoms or disease
· Large numbers of unexplained symptoms, diseases, or deaths
· Higher than expected morbidity and mortality associated with a common disease and/or failure of patients to respond to traditional therapy
· Single case of disease caused by an uncommon agent (i.e., Burkholderia mallei or B. pseudomallei, variola virus, viral hemorrhagic fever viruses, Bacillus anthracis)
· Multiple unusual or unexplained diseases in the same patient
· Disease with an unusual geographic or seasonal distribution (e.g., tularemia in a non-endemic area or influenza in the summer)
· Unusual "typical patient" distribution (i.e., several adults with an unexplained rash)
· Unusual disease presentation (i.e., inhalational vs. cutaneous anthrax)
· Similar genetic type among agents from temporally or spatially distinct sources
· Unusual, atypical, genetically engineered, or antiquated strain of a biological agent
· Endemic disease with unexplained increase in incidence (i.e., tularemia, plague)
· Simultaneous clusters of similar illness in non-contiguous areas, domestic or foreign
· Disease agents transmitted through aerosol, food, or water; suggestive of sabotage
· Ill persons presenting near the same time; point source with compressed epidemic curve
· No illness in persons in locations where there are ill persons in close proximity and they are not sharing common ventilation systems (all have separate closed ventilation systems)
· Death or illness in humans preceded or accompanied by death or illness in animals that is unexplained or attributed to a zoonotic biological agent

Table 3: Public Health Triggers

LAW ENFORCEMENT TRIGGERS
· Any intelligence or indication that any individual or group is unlawfully in possession of any biological agents
· Seizure of bio-processing equipment from any individual, group, or organization
· Seizure of potential dissemination devices from any individual, group, or organization
· Identification or seizure of literature pertaining to the development or dissemination of biological agents
· Any assessments that indicate a credible biological threat exists in an area
· A HAZMAT response that involves the presence of biological agents

Table 4: Law Enforcement Triggers

The identification of law enforcement and public health triggers is intended to be a starting point to improve information sharing between agencies or jurisdictions. The most important aspect of this process is to overcome the hesitation or reluctance to share information before all of the facts are known. Early notification provides an early warning and should not be viewed negatively.

JOINT THREAT ASSESSMENTS

To complement and support the threat credibility evaluation process coordinated by the FBI WMDOU, it is recommended that local FBI field offices, local law enforcement, and public health establish protocols for conducting a local joint threat assessment. Determining the nature of a reported incident (i.e., natural or intentional) and implementing appropriate response activities requires a joint assessment by law enforcement and public health. Procedures for conducting joint threat assessments can be incorporated into a joint protocol or MOU. An

example of a procedure for conducting a joint threat assessment is located in Appendix 6.

JOINT INVESTIGATIONS

The objective of the joint investigations is to maximize the efficiency of both law enforcement and public health investigators through the exchange of real-time information. When a joint investigation is initiated and approved, law enforcement and public health are empowered to share information through the course of conducting joint interviews and joint command post operations.

The goals of joint investigations are to:

- Identify the disease causing agent,
- Identify the source and perpetrators of the attack,
- Determine the mode(s) of spread or transmission of the biological agent,
- Determine where and when exposure to the biological agent may have occurred, and
- Identify who may have been exposed.

Joint Investigation Criteria

The following criteria may be used to establish a threshold for determining whether to conduct a joint investigation of a suspect bioterrorism incident:

- Case-patient(s) positive for a select agent,
- No known natural source to explain infection,
- No known risk factors for disease occurrence, ***and/or***
- FBI intelligence suggests that the incident is criminal/intentional

These criteria are not all-inclusive and may not cover every possible bioterrorism scenario. Once a decision has been made to work jointly, law enforcement and public health should follow the procedures developed to guide a joint investigation between their agencies or jurisdictions. These procedures can be incorporated into a MOU/joint protocol.

JOINT INTERVIEWS

Collaboration between law enforcement and public health officials has not always been recognized as beneficial when conducting interviews. There are concerns that the presence of law enforcement would compromise the collection of sensitive medical information (e.g., illegal drug use) by public health officials. Law enforcement investigation of bioterrorism incidents, however, requires interviewing all potential witness and victims. Separate questioning by law enforcement and public health investigators may lead to conflicting statements, which can jeopardize the outcome of the investigation. Conducting joint interviews affords the opportunity to examine relevant facts based on the unique perspectives of both criminal and epidemiological investigators.

A process should be established whereby joint interviews by law enforcement and public health officials are conducted, with the opportunity for confidential communications between public health and the interviewee regarding specific health-related issues that the interviewee may be unwilling to share with law enforcement personnel. Special consideration should be made to protect the identifying information of the interviewees, due to privacy as well as the integrity of a criminal investigation.

Although a joint interview with law enforcement can provoke anxiety in the patient, one interview with both agencies present may be less disruptive to the patient than two or more separate interviews repeating similar information. When joint interviews are not possible (e.g., the interviewee requests that law enforcement not be present), each discipline should be aware of the types of information their counterpart is seeking. For reference, an example of questions that may be asked by law enforcement and public health is located in Appendix 7.

Much of the joint investigation will initially focus on interviews with case-patients and potential contacts that will primarily address where and when exposures to bioterrorism agents may have occurred. An example of a protocol for planning for and conducting joint interviews is included in Appendix 6.

A joint interview may determine that the disease outbreak is not the result of a crime and therefore no further law enforcement action is required. If the interview indicates that a crime has occurred, law enforcement and public health will continue to work on the investigation jointly.

Investigative Information Needs

The timely exchange of information is critical to an effective response to a bioterrorism incident; however, it may be difficult to know the type of information to freely exchange during a joint investigation. As a general rule, when conducting joint investigations, law enforcement should share relevant criminal investigative information that will be helpful to public health in mitigating the effects of the outbreak. Likewise, public health should share any epidemiological investigative

information that may assist law enforcement to identify, apprehend, prosecute, and convict the perpetrator(s).

The following tables (Table 5 and Table 6) were developed to assist law enforcement and public health in determining the type of information needed by the other discipline.

· Hypotheses generated by the epidemiological investigation
· Any information developed by public health related to the exposure or dissemination of the biological agent
· Case definition (signs, symptoms, and clinical picture of disease)
· National or international health alerts that may be related to the current bioterrorism incident
· Laboratory results from CDC used to characterize the specific biological agent (e.g., strain, genetic sequencing, antimicrobial resistance)
· Notification about when public health is planning to conduct interviews with case-patients or contacts

Table 5: Public Health Information for FBI/Law Enforcement

INFORMATION
· Law enforcement investigative information (e.g., interviews scheduled, possible subjects identified, positive results on criminal/terrorism database checks, and planned search warrants) that may assist public health with the identification of the agent and determination of source of the outbreak
· Information regarding the bioterrorism incident reported to the Joint Operations Centers from a fusion center, other federal/state/local agency, or the general public
· Information regarding any known group or sector that may be targeted (e.g., government or financial, entertainment, religious/ethnic groups) for an attack
· Local FBI WMD cases which may have ties to the existing bioterrorism incident investigation
· Information related to counterterrorism or domestic terrorism subjects who have expertise in biological matters or are associates of persons with that expertise, who may be related to the current bioterrorism incident
· Pre-incident indicators (e.g., videotaping, sketching maps, break-ins, perimeter breaches at facilities) that may be related to the bioterrorism incident
· Information developed by the FBI or law enforcement regarding the biological agent used, mechanism for delivery/dissemination, date, time and locations of exposures
· Information regarding any medical equipment, chemicals, toxins, biological agents or laboratory supplies stolen, developed, or uncovered that may be related to the bioterrorism incident
· Intelligence information regarding the characteristics of the biological agent (e.g., strain, antimicrobial resistance, or weaponized nature)

Table 6: FBI/Law Enforcement Information for Public Health

JOINT INVESTIGATIONS AND THE MEDIA

It is important for the FBI, law enforcement staff and public health officials to coordinate their interaction with the media. The media will have a significant impact on the response and the public reaction to a bioterrorism incident. With public fear and the psychological impact of a biological attack, the media will aggressively seek information from the investigators. Therefore, the FBI, law enforcement, and public health must develop a working relationship with the media to help ensure that timely, useful information is shared with the media to keep the public accurately informed, but not overly alarmed.

SUMMARY

SUMMARY

This handbook provides recommendations for law enforcement and public health to increase collaboration by conducting joint investigations during the response to a bioterrorism incident. The procedures and methodologies described are intended to serve as a guide. Law enforcement and public health should modify this guidance to accommodate the needs and characteristics of their specific agency or jurisdiction. The recommendations outlined in this handbook should not be viewed as policy directives from the federal government, requiring immediate implementation.

The primary goal of this handbook is to promote increased interaction and communication among law enforcement and public health during the investigation following a bioterrorism incident. By increasing information sharing, conducting joint threat assessments and conducting joint investigation/joint interviews, law enforcement and public health can maximize their resources and achieve their individual and common goals during the response to a bioterrorism incident.

APPENDIX 1: Applicable Federal Weapons of Mass Destruction Statutes Regarding the Criminal Use of Biological Agents

I. STATUTE CITATIONS

Weapons of Mass Destruction (WMD) Statute

Title 18 United States Code (U.S.C.) Section 2332a

- It is illegal to use, threaten, or attempt or conspire to use a weapon of mass destruction, including any biological agent, toxin, or vector (as defined in Title 18 U.S.C. Section 178) against a U.S. national, within the United States and affecting interstate or foreign commerce, or against any property of the United States.
- The term WMD includes "any weapon involving a disease organism."
- Such an offense does not require the actual use of a biological agent. A threat or conspiracy to use a biological agent is sufficient.
- Such an offense does not require that the biological agent be a "select agent," only that the agent be capable of causing biological malfunction, disease, or death in a living organism (Title 18 U.S.C. Section 178).
- The U.S. Government must demonstrate evidence that a biological agent was used, or would be used, or that a person or persons threatened or conspired to do so. Such crime is punishable by as much as life in prison; if death results from the violation, the penalty may also include death.
- There is an 8-year statute of limitation for noncapital cases (if the interstate-commerce element is present).
- There is no state-of-mind requirement.

SUMMARY

Prohibitions with Respect to Biological Weapons

Title 18 U.S.C. Section 175a

- It is illegal to knowingly develop, produce, stockpile, transfer, acquire, retain, or possess any biological agent, toxin, or delivery system for use as a weapon, or to knowingly assist a foreign state or organization in doing so.
- It is illegal to attempt, threaten, or conspire to do the same.
- Such an offense does not require that the biological agent be a "select agent," only that that agent be capable of causing biological malfunction, disease, or death in a living organism (Title 18 U.S.C. Section 178).
- "For use as a weapon" is further defined as "the development, production, transfer, acquisition, retention, or possession of any biological agent, toxin, or delivery system for other than prophylactic, protective, bona fide research, or other peaceful purposes."
- "For use as a weapon" is a requirement of such an offense.
- Such an offense carries the penalty of fines, a term of as much as life in prison, or both.
- There is an 8-year statute of limitation for noncapital cases (no interstate-commerce element is necessary).

Prohibitions with Respect to Biological Weapons, Additional Offense

Title 18 U.S.C. Section 175b

- It is illegal to knowingly possess any biological agent, toxin, or delivery system of a type or in a quantity that, under the circumstances, is not reasonably justified by prophylactic, protective, bona fide research, or other peaceful purposes.

- Such an offense does not require that the biological agent be a "select agent," only that the agent is capable of causing biological malfunction, disease, or death in a living organism (Title 18 U.S.C. Section 178).
- Such an offense carries the penalty of fines, imprisonment of as much as 10 years, or both.
- 8-year statute of limitation for noncapital cases (no interstate-commerce element is necessary).

Possession by Restricted Persons

Title 18 U.S.C. Section 175b

- It is illegal for any restricted person to ship, transport, or receive a biological agent or toxin through interstate or foreign commerce, if the agent or toxin is listed as a select agent in 42 Code of Federal Regulations (CFR) part 72.6(j).
- The term "select agent" does not include any biological agent or toxin that is in its naturally occurring environment, if the biological agent or toxin has not been cultivated, collected, or otherwise extracted from its natural source.
- A "restricted person" includes an individual who—
  - — Is under indictment for a crime that is punishable by imprisonment for a term exceeding 1 year
  - — Has been convicted in any court of a crime that is punishable by imprisonment for a term exceeding 1 year
  - — Is a fugitive from justice

  - — Is an unlawful user of any controlled substance (as defined in section 102 of the Controlled Substances Act [21 U.S.C. Section 802])
  - — Is an alien illegally or unlawfully in the United States
  - — Has been 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 the Secretary of State has identified as having provided support to terrorism
  - — Has received a dishonorable discharged from the armed services of the United States.
- Carries a penalty of imprisonment as much as 10 years, fines, or both.
- There is an 8-year statute of limitation for noncapital cases (no interstate-commerce element is necessary).

II. DEFINITIONS

The terms biological agent, toxin, delivery system, and vector are defined for all references in Title 18 U.S.C. Chapter 10, Sections 175 through 178 provisions:

- **Biological Agent:** Any microorganism, virus, infectious substance, or biological product that might be engineered as a result of biotechnology, or any naturally occurring or bioengineered component of any such microorganism, virus, infectious substance, or biological product, that is capable of causing—
  - — Death, disease, or other biological malfunction in a human, animal, plant, or other living organism

  - — Deterioration of food, water, equipment, supplies, or material of any kind
  - — Deleterious alteration of the environment.
- **Toxin:** The toxic material of plants, animals, microorganisms, viruses, fungi, or infectious substances, or a recombinant molecule (whatever its origin or method of production), including—
  - — Any poisonous substance or biological product that might be engineered as a result of biotechnology produced by a living organism
  - — Any poisonous isomer or biological product, homolog, or derivative of such a substance.
- **Delivery System:** Any apparatus, equipment, device, or means of delivery specifically designed to deliver or disseminate a biological agent, toxin, or vector.
- **Vector:** A living organism, molecule (including a recombinant molecule), or biological product that might be engineered as a result of biotechnology and that is capable of carrying a biological agent, toxin, or host.

III. LIST OF SELECT AGENTS AND TOXINS

U.S. Department of Health and Human Services (HHS) and U.S. Department of Agriculture (USDA) Select Agents and Toxins

7 CFR Part 331, 9 CFR Part 121, and 42 CFR Part 73

HHS SELECT AGENTS AND TOXINS
· Abrin
· Botulinum neurotoxins
· Botulinum neurotoxin producing species of *Clostridium*
· Cercopithecine herpesvirus 1 (Herpes B virus)
· *Clostridium perfringens* epsilon toxin
· *Coccidioides immitis*
· *Coccidioides posadasii*
· Conotoxins
· *Coxiella burnetii*
· Crimean-Congo haemorrhagic fever virus
· Diacetoxyscirpenol
· Eastern equine encephalitis virus
· Ebola viruses
· *Francisella tularensis*
· Lassa fever virus
· Marburg virus
· Monkeypox virus
· Reconstructed replication competent forms of the 1918 pandemic influenza virus containing any portion of the coding regions of all eight gene segments (reconstructed 1918 influenza virus)
· Ricin

· *Rickettsia prowazekii*
· *Rickettsia rickettsii*
· Saxitoxin
· Shiga-like ribosome inactivating proteins
· Shigatoxin
· Staphylococcal enterotoxins
· South American haemorrhagic fever viruses – Flexal –Guanarito –Machupo –Junin –Sabia
· T-2 toxin
· Tetrodotoxin
· Tick-borne encephalitis complex (flavi) viruses - Central European tick-borne encephalitis - Far Eastern tick-borne encephalitis · Kyasanur forest disease · Omsk hemorrhagic fever · Russian spring and summer encephalitis
· *Variola major* virus (Smallpox virus)
· *Variola minor* virus (Alastrim)
· *Yersinia pestis*

OVERLAP SELECT AGENTS AND TOXINS

· *Bacillus anthracis*	· *Coxiella burnetii*
· Botulinum neurotoxins	· Eastern Equine Encephalitis virus
· Botulinum neurotoxin producing species of Clostridium	· Francisella tularensis
· *Brucella abortus*	· Hendra virus

SUMMARY

· *Brucella melitensis*	· Nipah virus
· *Brucella suis*	· Rift Valley fever virus
· *Burkholderia mallei* (formerly *Pseudomonas mallei*)	· Shigatoxin
· *Burkholderia pseudomallei* (formerly *Pseudomonas pseudomallei*)	· Staphylococcal enterotoxins
· *Clostridium perfringens* epsilon toxin	· T-2 toxin
· *Coccidioides immitis*	· Venezuelan Equine Encephalitis virus

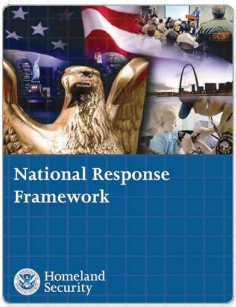
USDA SELECT AGENTS AND TOXINS	
· African horse sickness virus	· Lumpy skin disease virus
· African swine fever virus	· Malignant catarrhal fever virus (Alcelaphine herpesvirus type 1)
· Akabane virus	· Menangle virus
· Avian influenza virus (highly pathogenic)	· Mycoplasma capricolum/ M.F38/M. mycoides
· Bluetongue virus (Exotic)	· *Mycoplasma capricolum capripneumoniae* (contagious caprine pleuropneumonia)
· Bovine spongiform encephalopathy agent	· *Mycoplasma mycoides mycoides* (contagious bovine pleuropneumonia)
· Camel pox virus	
· Classical swine fever virus	· Peste des petits ruminants virus
· *Ehrlichia ruminantium* (Heartwater)	· Rinderpest virus
· Foot-and-mouth disease virus	· Sheep pox virus

· Goat pox virus	· Swine vesicular disease virus
· Japanese encephalitis virus	· Vesicular stomatitis virus (Exotic)
	· Virulent Newcastle disease virus (velogenic)
· Newcastle disease virus (velogenic)	

USDA PLANT PROTECTION AND QUARANTINE (PPQ) SELECT AGENTS AND TOXINS	
· *Peronosclerospora philippinensis*	· *Synchytrium endobioticum*
· *Ralstonia solanacearum* race 3, biovar 2	· *Xanthomonas oryzae* pv. *Oryzicola*
· *Schlerophthora rayssiae* var. *zeae*	· *Xylella fastidiosa* (citrus variegated chlorosis strain)

APPENDIX 2: National Response Framework Biological Incident Annex[1]

National Response Framework



The National Response Framework (NRF) presents the guiding principles that enable all response partners to prepare for and provide a unified national response to disasters and emergencies, from the smallest incident to the largest catastrophe. The NRF defines the key principles, roles, and structures that organize the way the United States respond as a nation. This framework is built on scalable, flexible, and

[1]Federal Emergency Management Agency (FEMA). *National Response Framework*. December 2008. Retrieved from http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf.

adaptable coordinating structures to align key roles and responsibilities across the nation. The NRF describes specific authorities and best practices for managing incidents that range from the serious but purely local, to large-scale terrorist attacks or catastrophic natural disasters. This framework describes how communities, tribes, states, the Federal Government, and private-sector and nongovernmental partners should apply these principles for a coordinated, effective national response. The NRF is always in effect, and elements can be implemented at any level at any time.

The NRF is an outgrowth of previous iterations of federal planning documents. A brief discussion of its history underscores important elements and highlights improvements to the previous *National Response Plan* (NRP).

Audiences

The NRF is written especially for government executives, private-sector business, and nongovernmental leaders and emergency management practitioners. The NRF's clear, simple style makes the serious work of incident management equally understandable for newly elected or appointed government officials, business executives, and seasoned practitioners.

- The NRF is addressed to senior elected and appointed leaders, such as federal department or agency heads, state governors, mayors, tribal leaders or city managers: all those who have a responsibility
  to provide for effective emergency management.
- The NRF also informs emergency-management practitioners,

explaining the operating structures and tools that first responders and emergency managers use routinely at all levels of government.

- The NRF Resource Center (www.fema.gov/NRF) is an important online reference center that provides stakeholders at all levels of government, the private sector, and nongovernmental organizations (NGO) access to the NRF and supporting documents.

NRF Organization

The NRF comprises the core document; the Emergency Support Function (ESF), Support, and Incident Annexes; and the Partner Guides. The core document describes the doctrine that guides our national response, roles and responsibilities, response actions, response organizations, and planning requirements to achieve an effective national response to any incident that occurs. The remaining documents provide more detailed information to assist practitioners in implementing the NRF:

- The ESF Annexes group federal resources and capabilities into functional areas that are needed most frequently in a national response (e.g., transportation, firefighting, mass care).
- Support Annexes describe essential supporting aspects that are common to all incidents (e.g., financial management, volunteer and donations management, private-sector coordination).
- Incident Annexes address the unique aspects of how we respond to seven broad incident categories (e.g., Biological, Nuclear/ Radiological, Cyber, Mass Evacuation).
- Partner Guides provide ready references that describe key roles and actions for local, tribal, state, federal, and private-sector response partners.

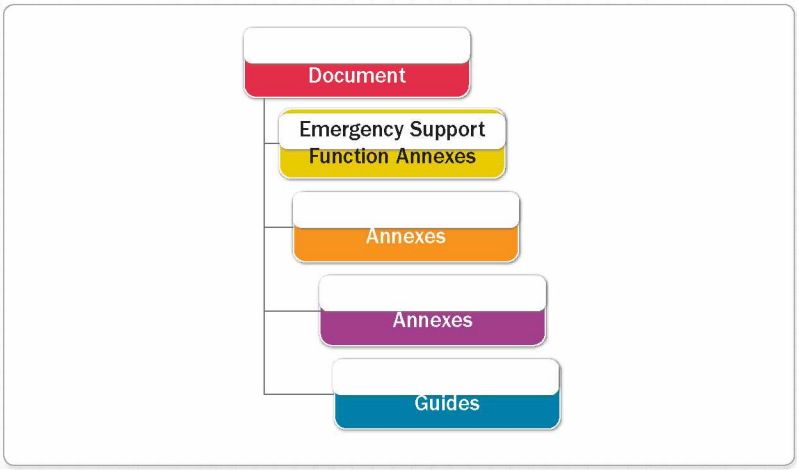


Figure 4: Organization of the Framework

These documents are available at the NRF Resource Center (http://www.fema.gov/NRF).

The National Incident Management System (NIMS) is a companion document that provides standard command and management structures that apply to response activities. This system provides a consistent, nationwide template to enable the Federal Government; state, tribal, and local governments; the private sector; and NGOs to work together to prepare for, prevent, respond to, recover from, and mitigate the effects of incidents regardless of cause, size, location, or complexity. This consistency provides the foundation for use of the NIMS for all incidents, ranging from daily occurrences to incidents that require a coordinated federal response.

Guided by the input and help of many hundreds of stakeholders, the NRF represents a natural evolution of the national response architecture. Specifically, the NRF—

- Reflects lessons learned and defines the core principles for managing incidents
- Broadens the focus from a purely federal plan to one that is truly national
- Methodically describes the "who, what, and how" of emergency preparedness and response
- Articulates the five key principles of response doctrine.

Response Doctrine Five Key Principles

1. Engaged partnership
2. Tiered response
3. Scalable, flexible, and adaptable operational capabilities
4. Unity of effort through unified command
5. Readiness to act

Response Doctrine

Response doctrine defines basic roles, responsibilities, and operational concepts for response across all levels of government and with NGOs and the private sector. The overarching objective of response activities centers upon saving lives and protecting property and the environment. Five key principles of operations define response actions in support of the nation's response mission. Taken together, these five principles of operation constitute national response doctrine.

Engaged Partnerships

Leaders at all levels must communicate and actively support engaged partnerships by developing shared goals and aligning capabilities so that no one is overwhelmed in times of crisis. Layered, mutually supporting capabilities at federal, state, tribal, and local levels allow

for coordinated planning in times of calm and effective response in times of need. Engaged partnerships include ongoing communication of incident activity among all partners to the NRF, as well as shared situational awareness for a more rapid response. In particular, the potential for terrorist incidents requires a heightened state of readiness and nimble, practiced capabilities at the core of our preparedness and response planning.

Tiered Response

Incidents must be managed at the lowest possible jurisdictional level and supported by additional capabilities when needed. Each level should not need to be overwhelmed before requesting resources from another level. Incidents begin and end locally, and most are wholly managed at the local level. Many incidents require unified response from local agencies, NGOs, and the private sector, and some require additional support from neighboring jurisdictions or the state. A few require federal support. National response protocols recognize these requirements and are structured to provide additional, tiered levels of support when more resources or capabilities are needed to support and sustain the response and initial recovery. All levels should be prepared to respond, anticipating the resources that might be required.

Scalable, Flexible, and Adaptable Operational Capabilities

As incidents change in size, scope, and complexity, the response must adapt to meet requirements. The number, type, and sources of resources must be able to expand rapidly to meet the needs that are associated with a given incident. The NRF's disciplined and coordinated process can provide for a rapid surge of resources from all levels of

government, appropriately scaled to need. Execution must be flexible and adapted to fit each incident.

Unity of Effort Through Unified Command

Effective unified command is indispensable to response activities and requires a clear understanding of the roles and responsibilities of each participating organization. Success requires unity of effort, which respects the chain of command of each participating organization while harnessing seamless coordination across jurisdictions, in support of common objectives.

Readiness to Act

Effective response requires readiness to act balanced with an understanding of risk. From individuals, households, and communities to local, tribal, and state governments as well as the Federal Government, national response depends on the instinct and ability to act. A forward-leaning posture is imperative for incidents that have the potential to expand rapidly in size, scope, or complexity, and for no-notice incidents.

National Strategy for Homeland Security

The NRF is required by, and integrates under, a larger *National Strategy for Homeland Security* (the *Strategy*) that serves to guide, organize, and unify our Nation's homeland security efforts. The *Strategy* reflects our increased understanding of the threats that confront the United States, incorporates lessons learned from exercises and real-world catastrophes, and articulates how we should ensure our long-term success by strengthening the homeland security foundation that we

SUMMARY

have built. The *Strategy* provides a common framework by which our entire Nation should focus its homeland security efforts on achieving the following four goals:

1. Prevent and disrupt terrorist attacks.
2. Protect the American people and our critical infrastructure and key resources.
3. Respond to and recover from incidents that do occur.
4. Continue to strengthen the foundation to ensure our long-term success.

Although the first three goals help to organize our national efforts, the last goal entails creating and transforming our homeland security principles, systems, structures, and institutions. This goal includes applying a comprehensive approach to risk management, building a culture of preparedness, developing a comprehensive Homeland Security Management System, improving incident management, better utilizing science and technology, and leveraging all instruments of national power and influence.

The NRF focuses primarily on the third goal: Respond to and recover from incidents that do occur. The *Strategy* also provides the context that given the certainty of catastrophes on our soil—no matter how unprecedented or extraordinary—it is our collective duty to provide the best response possible. The NRF states that, when needed, we will bring to bear the nation's full capabilities and resources to save lives, mitigate suffering, and protect property. The *Strategy* also reminds us that as the nation responds to an incident, we must also begin to lay the foundation not only for a strong recovery over the short term, but also for the rebuilding and revitalization of affected communities and regions over the long term.

ESF AND INCIDENT ANNEXES

The ESF Annexes provide the structure for coordinating federal interagency support for a federal response to an incident. These annexes are mechanisms for grouping functions that most frequently are used to provide federal support to states and federal agencies, both for declared disasters and emergencies under the Stafford Act and for non-Stafford Act incidents. The Incident Annexes describe the concept of operations to address specific contingency or hazard situations or an element of an incident that requires specialized application of the NRF. For additional information that might be pertinent to a joint criminal and epidemiological investigation during a potential or actual bioterrorism incident, see the following annexes to the NRF. Complete versions of these specific annexes are available at the NRF Resource Center (http://www.fema.gov/NRF).

EMERGENCY SUPPORT FUNCTION #8: PUBLIC HEALTH AND MEDICAL SERVICES ANNEX

Emergency Support Function (ESF) #8–provides the mechanism for coordinated federal assistance to supplement state, tribal, and local resources in response to a public health and medical disaster, potential or actual incidents that require a coordinated federal response, or a developing potential health and medical emergency. The phrase "medical needs" is used throughout this annex. "Public health and medical services" include responding to medical needs that are associated with psychological health, behavioral health, or substance-abuse considerations of incident victims and response workers. Services also cover the medical needs of members of the "at risk" or "special needs" population, as described in the Pandemic and All-Hazards Preparedness Act and in the NRF Glossary, respectively.

This population includes members who might have medical and other functional needs before, during, and after an incident. ESF #8 is coordinated by the Secretary of HHS, principally through the Assistant Secretary for Preparedness and Response (ASPR).

TERRORISM INCIDENT LAW ENFORCEMENT AND INVESTIGATION ANNEX

The purpose of this annex is to facilitate an effective Federal law enforcement and investigative response to all threats or acts of terrorism within the United States, regardless of whether they are deemed credible and/or whether they escalate to an Incident of National Significance. To accomplish this, the annex establishes a structure for a systematic, coordinated, unified, timely, and effective national law enforcement
and investigative response to threats or acts of terrorism within the United States. This annex is coordinated by the Federal Bureau of Investigation (FBI).

BIOLOGICAL INCIDENT ANNEX

The purpose of the Biological Incident Annex is to outline the actions, roles, and responsibilities that are associated with response to a human disease outbreak, of known or unknown origin, and that requires federal assistance. In this annex, a "biological incident" includes naturally occurring biological diseases (communicable or noncommunicable) in humans, as well as terrorist events. This definition also includes those biological agents that are found in the environment, or diagnosed in animals, and that have the potential for transmission to humans (i.e., zoonosis). Incidents that are restricted to animal, plant, or food health or safety are reviewed in other annexes.

Actions that are described in this annex take place with or without a Presidential Stafford Act declaration or a public health emergency declaration by the Secretary of HHS. This annex outlines biological incident response actions, including threat-assessment notification procedures, laboratory testing, joint investigative or response procedures, and activities related to recovery.

Complete versions of these specific annexes are available at the NRF Resource Center, http://www.fema.gov/NRF.

APPENDIX 3: Laboratory Response Network

History

The Laboratory Response Network (LRN) became operational in 1999, in response to Presidential Decision Directives (PDD) 39 and 62, which outlined national antiterrorism policies and assigned specific missions to federal departments and agencies. The LRN's objective was to ensure an effective counter-terrorism response by addressing crisis- and consequence-management issues, including the ability to rapidly detect biothreat agents. Since 1999, the LRN has evolved to include preparedness and response activities for emerging infectious diseases, such as severe acute respiratory syndrome (SARS) and avian influenza, as well as other public health emergencies.

SUMMARY

Mission

The LRN and its partners will develop, maintain, and strengthen an integrated national and international network of laboratories that can respond quickly to needs for rapid testing, timely notification, and secure reporting of results that are associated with acts of biological terrorism or other high-consequence public health emergencies.

The LRN has chemical-threat testing capabilities. However, those activities are not covered in this appendix, which is dedicated to the LRN's biological-threat testing capabilities.

Membership and Function—Biological

The LRN is a national network of approximately 170 laboratories. Participation in the LRN is voluntary, and all member laboratories work under a single operational plan and adhere to strict policies of safety and security. Because an event can occur in a variety of locations and populations, the LRN has created a diverse network of laboratories that can detect top-tier biothreat agents in human and animal clinical specimens, environmental samples (e.g., powders, soil, water), and food. The network includes these types of labs:

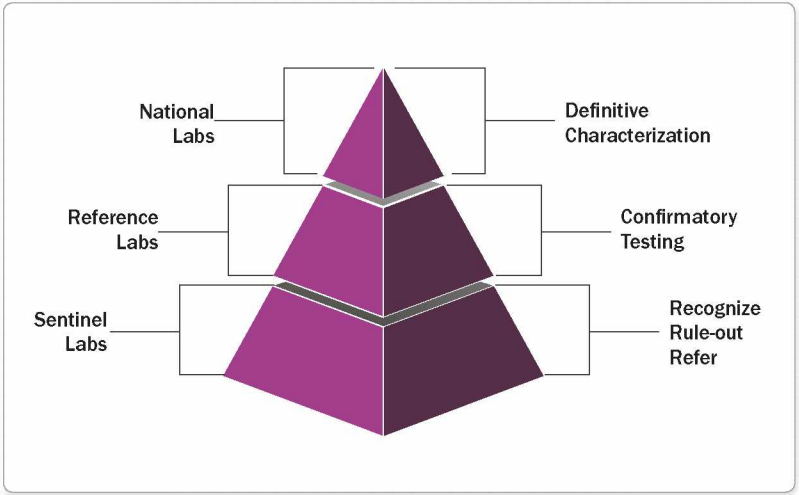
- State and local public health
- U.S. military food testing
- Environmental
- Veterinary
- International (Canada, United Kingdom, Australia. Mexico [pending] and some U.S. military bases abroad)

The LRN Structure for Bioterrorism

LRN biological laboratories are designated as either national, reference, or sentinel. Designation depends on the types of tests that the laboratory can perform and how it handles infectious agents to protect workers and the public:

- **National Laboratories:** National laboratories have unique resources to handle highly infectious agents and can identify specific agent strains.
- **Reference Laboratories:** Reference laboratories can rapidly perform tests to detect and confirm the presence of a threat agent. Testing occurs at the local level, allowing a more rapid public health response.
- **Sentinel Laboratories:** Sentinel laboratories represent the thousands of hospital-based facilities that are on the front lines. Sentinel laboratories have direct contact with patients. In an unannounced or covert terrorist attack, sentinel laboratories can be the first to identify a suspicious sample. A sentinel laboratory's responsibility is to refer samples to an LRN reference laboratory if the sentinel laboratory cannot rule out suspicion of a biothreat agent while performing routine diagnostic tests.

SUMMARY



Partnerships

The LRN has multiple partnerships with other government agencies and private organizations that have a stake in bioterrorism and chemical preparedness. These agencies and organizations include but are not limited to the following:

- FBI (founding partner)
- Association of Public Health Laboratories (founding partner)
- Army Medical Research Institute (founding partner)
- American Association of Veterinary Laboratory Diagnosticians
- American Society for Microbiology
- U.S. Environmental Protection Agency (EPA)

- USDA
- U.S. Department of Defense (DoD)
- U.S. Food and Drug Administration (FDA)
- U.S. Department of Homeland Security (DHS)

APPENDIX 4: Health Insurance Portability and Accountability Act Medical Privacy Rules: Exemptions

These exceptions to the Health Insurance Portability and Accountability Act (HIPAA) permit the covered entity to disclose patient medical information to law enforcement that are not performing health-oversight investigations (45 CFR Part 164.512):

1. **When required by law.** If another law requires reporting; see 45 CFR Part 164.512(f)(1)(i)
2. **By court order or by warrant of subpoena or summons issued by a judicial officer.** See 45 CFR Part 164.512(f)(1)(ii)(A)
3. **By grand jury subpoena.** See 45 CFR Part 164.512(f)(1)(ii)(B)
4. **By administrative subpoena.** If the subpoena complies with three specific requirements:
   a. "Information sought is relevant and material to a legitimate law enforcement inquiry" (i.e., ask only for information that is needed for a real investigation)
   b. "The request is specific and limited in scope to the extent reasonable practicable in light of the purpose for which the information is sought" (i.e., do not ask for more information than necessary)

   c. "De-identified information could not reasonably be used" (i.e., if a person's name, SSN, etc. is removed from the record, then the record would be useless to the investigation); see 45 CFR Part 164.512(f)(1)(ii)(C).

5. **To locate and identify.** For example, to find a suspect, fugitive, material witness, or missing person; only eight types of information may be requested and obtained:
   a. Name and address
   b. Date and place of birth
   c. Social security number
   d. Blood type and Rh factor
   e. Type of injury
   f. Date and time of treatment
   g. Date and time of death
   h. Observable physical characteristics, such as eye color and hair color, tattoos, gender, race, height, weight, or facial hair; see 45 CFR Part 164.512(f)(2)
6. **For a crime on the premises.** If the covered entity believes that the protected health information constitutes evidence of criminal conduct that occurred on the premises of the covered entity; see 45 CFR Part 164.512(f)(5)
7. **Information about the victim of a crime.** When the information will not be used against the victim *and* law enforcement activity will be adversely and materially affected by delay until the victim is able to agree and giving law enforcement the information is in the

best interest of the victim (e.g., the victim is incapacitated or other emergency circumstances exist); see 45 CFR Part 164.512(f)(3)

8. **Emergency health care workers reporting crimes, victims, or perpetrators.** See 45 CFR Part 164.512(f)(6)
9. **To assist a victim of abuse, neglect, or domestic violence.** Under any of the following circumstances:
   a. The disclosure is required by law.
   b. The individual has agreed to the disclosure.
   c. The disclosure is expressly authorized by law and is necessary to present serious harm.
   d. The disclosure is authorized by law and the law enforcement agency represents that the information will not be used against the individual and law enforcement activity depends on the disclosure and would be materially and adversely affected by waiting until the individual is able to agree; see 45 CFR Part 164.512(c).
10. **Disclosure to coroner or medical examiner.** See 45 CFR Part 164.512(g).
11. **To avert serious threat to health and safety.** Se 45 CFR Part 164.512(j).
12. **For national security and intelligence.** Protected health information may be disclosed to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act (50 U.S.C. 401, et seq.) and implementing authority (e.g., Executive Order 12333); see 45 CFR Part 164.512(k)(2).

13. **Protective services for the President and others.** See 45 CFR Part 164.512(k)(3).
14. **Jails, prisons, law enforcement custody.** See 45 CFR Part 164.512(k)(5).

Protecting the Confidentiality of the Investigation

In all cases, health oversight or otherwise, when it is necessary to stop a medical provider from telling patients that law enforcement has requested their medical information, in accordance with 45 CFR Part 164.528(a)(2):

1. Make an oral request that the provider not disclose.
2. Follow up within 30 days, with a written request on law enforcement stationary.

When requesting patient medical information, law enforcement representatives should show their badges and, if possible, make requests in writing on official letterhead.

Additional Considerations

There are two additional considerations:

- **Substance Abuse Patients Records.** Stricter protections are afforded to the records of bona fide providers of substance abuse treatment; see 42 CFR Part 2.
- **Health Oversight.** Disclosure is permitted even when conducted by a law enforcement agency; see 45 CFR Part 164.512(d).

APPENDIX 5: Sample Procedure for a Local Bioterrorism Threat Assessment

To assist in the response to a bioterrorism incident at the local level, law enforcement and public health should develop protocols to conduct a local bioterrorism threat assessment between agencies and jurisdictions. The following procedure is intended to serve as a guide for agencies and jurisdictions that are developing protocols for conducting a local bioterrorism threat assessment. Law enforcement and public health might want to adapt this procedures outline to suit the needs of their agencies or jurisdictions.

After receiving a report that indicates a potential bioterrorism incident, public health should immediately notify the local FBI WMD coordinator so that he or she can conduct a local bioterrorism threat assessment. The local bioterrorism threat assessment should be conducted by conference call and may include these officials:

- Local FBI WMD coordinator
- Local law enforcement representative (trained in WMD response)
- WMD representative from the jurisdiction's fusion center
- Public health bioterrorism coordinator
- LRN bioterrorism coordinator
- Epidemiological investigator
- Public health surveillance
- Environmental health
- Health communications

SUMMARY

The purpose of the conference call is to conduct a bioterrorism threat assessment to determine the likelihood of a bioterrorism incident and to identify the initial response actions that law enforcement and public health should perform.

The conference call agenda may include these items:

- Incident briefing by public health
  - Why public health is concerned
  - Update on confirmed or suspect cases
    - Demographic information: gender, age, race, ethnicity, occupation, religious affiliation, membership in any groups or associations (personal identifying information may not be exchanged at this point)
    - Description of where the patient lives (e.g., urban, rural)
    - Patient's recent travel history (e.g., domestic, international)
    - Recent activities that might be related to exposure and illness
  - Current laboratory test results
  - Hypotheses regarding source of exposure
- Additional public health information
  - **Syndromic surveillance:** any unusual patterns of disease presentation or geographical clustering of disease
  - **BioWatch Actionable Results (BAR) information:** any BARs for the biological agent, in the jurisdiction or within the nation
- FBI or law enforcement information or intelligence
  - Information on existing threats in the jurisdiction (WMD or otherwise)
  - WMD intelligence that might be connected to case exposure (e.g.,

religious affiliation, group, association)

— Intelligence regarding acquisition or intended use of any bioterrorism agent that might relate to the case symptoms

The conference call members will then assess the possibility that the incident might be bioterrorism. If the information that is needed to conduct an initial assessment is unavailable, then judgment may be temporarily suspended until such information is obtained. If there is enough information to make a determination, then the incident may be classified into one of three risk categories:

— **No Risk.** it is highly likely that the source of exposure occurred naturally (not an intentional release).

— **Possible Bioterrorism Risk.** Information suggests that exposure might be a result of an intentional exposure:

- Public health investigation has not revealed a likely natural source of exposure.
- Unusual or unexplainable circumstances exist regarding the patient's infection with the biological agent (e.g., bubonic plague in an urban area with no history of patient travel, an agent that is not common or endemic to an area).
- The event itself, although appearing to be noncredible, might draw media or law enforcement attention, implying bioterrorism.

— **Likely Bioterrorism Risk.** There is a reasonable belief that the exposure was caused intentionally:

- LRN lab results are polymerase chain reaction (PCR) positive for a select agent or toxin.
- No known natural source explains the infection.

- There are no known risk factors for disease occurrence.
- FBI intelligence or law enforcement information suggests that the event is criminal or intentional.

Following the joint conference call and assessment, the joint investigation team will make these recommendations to FBI or law enforcement and public health, based on the level of risk:

- **No Risk**
  - — Public health will continue to manage the incident
  - — No further law enforcement actions will be needed.
- **Possible Bioterrorism Risk:**
  - — The local FBI WMD coordinator contacts FBI Headquarters (FBIHQ) WMD Operations Unit (WMDOU), which queries intelligence databases for any relevant information or intelligence.
  - — Public health conducts an epidemiological investigation to determine the source of the exposure and the likelihood that it was intentional.
  - — Public health reports the results of the epidemiological investigation (but no personally identifying information) to law enforcement.
- **Likely Bioterrorism Risk:**
  - — The local FBI WMD coordinator contacts FBIHQ WMDOU, which sets up a conference call with local FBI, public health, and relevant FBIHQ units and CDC to conduct a WMD threat credibility evaluation.
  - — FBI or law enforcement and public health initiate a joint

investigation (unified command is established).

— FBI opens a case file to investigate criminal intent or suspicious circumstances.

— An FBI Joint Operations Center (JOC) is established, if required.

Although the incident must be initially assessed at one of these risk levels, that assessment may be changed as the investigation begins and new information is collected.

APPENDIX 6: Sample Procedure for Joint Interviews

An initial component of the joint investigation will focus on interviews with patients, relatives and potential contacts to determine the source of exposure to the biological agent. The purpose of this appendix is to provide law enforcement and public health with sample procedures for conducting joint interviews. This procedure is intended to serve as a guide and might not be applicable in all circumstances. Law enforcement and public health might want to adapt the procedures outlined to suit the needs of their agencies or jurisdictions.

Law enforcement and public health should exchange information as soon as possible to assess the possibility that a biological threat exists. Therefore, joint interviews likely will occur as a part of the initial response activities to a suspected bioterrorism incident.

Initial Meeting

Prior to conducting an interview, law enforcement and public health should meet in person to discuss the current investigative information and to review procedures for the joint interview. If an in-person meeting is not feasible because of time constraints, then a conference call

between joint-interview participants is an alternative. If multiple joint interviews are going to be conducted at one location, then a joint interview team lead should be assigned to coordinate interview teams and to arrange follow-up meetings or conference calls.

A suggested agenda for the initial meeting or conference call is as follows:

- The public health investigator will—
  - — Provide a briefing of the current epidemiological investigation
  - — Provide a short briefing regarding the disease agent (e.g., the incubation period, method of transmission, cases per year in the immediate area and in the country)
  - — Recommend the appropriate level of personal protection equipment (PPE) and prophylaxis.
- The FBI or law enforcement investigator will review all current WMD threats, intelligence, and reporting that might be relevant to the situation.
- The joint interview team leader will create law enforcement or public health interview teams and address any specific logistical requirements (e.g., translators).

When the decision to conduct joint interviews has been made, agencies and jurisdictions should continue to re-evaluate the needs and the benefits that are gained by having both law enforcement and public health present during interviews. In some cases, information that the interview team gains might suggest that a joint interview is not the ideal process to collect information from the individual. For example, gathered information might indicate that the patient might be involved with the incident; therefore, FBI or law enforcement might

decide to conduct the interview without public health. Alternatively, an individual might feel more comfortable discussing private personnel issues with public health, without law enforcement presence. If interviews are conducted separately or by only one agency, relevant investigative information regarding the possible bioterrorism incident should be shared following the interview or interviews.

Staging Operations

Prior to arriving at the interview location (e.g., hospital, clinic, home), each joint interview team should meet at a staging area to review the interview strategy, determine how introductions to the subject of the interview will occur, and identify any other miscellaneous items that need to be considered. According to standard FBI or law enforcement procedures, background checks (i.e., criminal history) will be conducted on patients or contacts who are interviewed. Any relevant law enforcement data, including related intelligence or threat information, will be shared with public health at this staging area, before the interview. If appropriate, modifications to the interview questions should be made based upon information that law enforcement provides. Following the interview, FBI or law enforcement and public health should use the same or alternate staging area to discuss the interview and review notes.

Introduction to Hospital Administrator and Interview of Attending Physician (or Infection Control Practitioner)

If the interview is being conducted in a hospital or other medical facility, then the interview team likely will need to brief the hospital or facility administration on the current incident and provide them with an update on the activities that will be performed at the location. Public

health should initiate contact with the administration because they might have a prior working relationship. The interview team will explain that public health and law enforcement personnel will be interviewing a patient or patients at the facility. Whenever possible, the interview will be conducted in a manner that minimizes disruption to typical hospital operations and patient care. It should be determined whether the patient is in a private room; if not, a request should be made to move the patient to a private area where the interview can be conducted, if feasible.

When arriving at the hospital or medical facility, public health will ask to speak first with the patient's attending physician. Public health will explain the purpose of the patient interview and the reason for the presence of law enforcement. The following information should be collected from the attending physician:

- Why the patient was admitted to the hospital
- When and why the physician became involved with the case
- Background information on the case
- Opinion as to the level of cooperation that can be expected by the patient and any suggestions that might facilitate the interview process
- Whether the physician is willing to make introductions between patient and interviewers (the physician would not typically be present during the interview)

Interview

During the interview of a patient in a hospital, the joint interview team should make every effort to be sensitive to the patient's concerns and needs. During the interview, the patient's medical needs take priority over conducting the interview. There might be numerous interruptions by medical staff to attend to the needs of the patient. During this time, any discussion of sensitive information should be temporarily discontinued. Generally, the first part of the interview is conducted by public health and the second part by the FBI or law enforcement.

Before entering the patient's room, the interview team should apply the appropriate level of PPE, as instructed by medical personnel or public health. In some situations, the patient might feel vulnerable because of his or her condition, and the presence of law enforcement officers, even when not in uniform, can create additional anxiety. Therefore, the interview team should try to minimize the patient's stress during the interview. For example, the interviewers should sit in chairs during the interview rather than standing over the patient.

If not already introduced by the attending physician, the public health representative will introduce herself or himself, identify the law enforcement investigators, and explain the purpose of the joint interview and the reason for the law enforcement's presence (i.e., to determine whether the patient might have been a victim of a crime).

An example of what public health might say to the patient is as follows:

- "Because of the nature of your illness, we need to ensure that you have not been a victim of a crime. To do that, we will be asking standard questions to determine the nature of your exposure.

Because much of this information is relevant to ensuring that you have not been a victim of a crime, our standard procedure for [disease agent] is to ask law enforcement to be present during this interview."

- "Our public health protocol for cases of [illness or disease] is to involve law enforcement, to rule out the possibility that a crime has occurred."

For many reasons (e.g., the patient might be worried about crimes that he or she might have committed, the patient might be an illegal alien), the patient might refuse to have law enforcement present during the interview. If the patient states that he or she is unwilling to answer any questions with law enforcement present but will answer questions from public health, then law enforcement will leave the room and public health will continue with the standard public health interview. If this occurs, public health needs to be mindful of the types of information that might be relevant to law enforcement. Public health should try to collect this additional information as part of its interview. When the interview is complete, FBI or law enforcement will meet with public health at a predesignated area to discuss the interview results.

Law enforcement should not pursue prosecutorial efforts related to minor or petty crimes that the patient discloses during the interview, because doing so might be unrelated to the bioterrorism incident investigation. In addition, pursuing these minor or petty crimes might compromise the public health investigation, which can delay or prevent the identification of the exposure. Although law enforcement should prioritize investigative efforts related to the bioterrorism incident, it might need to seek prosecution of those minor crimes at a later date.

This issue should be discussed openly with public health.

Because a possibility exists that one of the interviewed individuals might be the subject (or related to the subject) who is responsible for committing the biological attack, public health should be aware that during its portion of the interview, FBI or law enforcement might try several techniques to determine the credibility of the patient. Law enforcement might ask questions which seem repetitive or awkward to public health. Public health should allow law enforcement to proceed without interruption, unless there is an urgent need to meet outside the room to discuss the interview strategy.

As a general rule, the patient will not be physically examined in the presence of law enforcement, unless circumstances dictate that law enforcement be present in the room. In addition, if the patient is a minor, the parents must be present during the FBI or law enforcement portion of the interview.

If appropriate, the joint interview team members will leave their personal business cards with the individual. The FBI or law enforcement investigators should advise the patient that if it is determined that the patient has been a victim of a crime, the FBI victim assistance coordinator will contact the patient.

Post-Interview Review

When the interview is complete, FBI or law enforcement and public health should meet to discuss their interview notes and ensure that there are no discrepancies. If FBI or law enforcement requires copies of patient medical information, public health will provide this information to FBI or law enforcement after it has checked to determine applicability under federal and state or local privacy statutes and has

removed any sensitive patient medical information that is not pertinent to the criminal investigation. Further questioning of the individual should be coordinated between the agencies and jurisdictions, to ensure that FBI or law enforcement and public health have an opportunity to participate.

Information Sharing Considerations following the Interview

These considerations are relevant after the interview:

- Information that is provided to FBI or law enforcement is considered "public health sensitive" and should be marked as such; before releasing such information to other agencies, public health must authorize the release.
- Information that FBI or law enforcement provides to public health is considered "law enforcement sensitive" and should be marked as such; this information should not be disseminated unless FBI or law enforcement approves the release.
- Information such as immigration status is particularly sensitive information, and release of such information could jeopardize the patient's willingness to cooperate with public health.
- Information that indicates that the patient has history of violent crime must be passed immediately back to public health, because of safety considerations.
- If the criminal database check reveals a nonterrorism criminal history (e.g., a warrant for arrest, the location of the fugitive in a local, state, or federal warrant), then law enforcement might need to pursue its own investigation, but only after first consulting with public health to minimize any impact on the epidemiological investigation.

- Information that is obtained or developed by FBI or law enforcement might be sensitive or classified, but might relate to the epidemiological investigation. Should this situation arise, this information will be provided to public health by FBI or law enforcement, through an authorized procedure.

APPENDIX 7: Sample Joint Interview Questions

Personal Information

1. Patient's name*
2. Patient's date of birth*
3. Patient's social security number[2]
4. Sex*
5. Patient's address*
6. Patient's occupation or employment (describe job and where patient works or goes to school)*
7. Patient's race, ethnicity, or nationality*
8. Patient's level of education
9. Personal information 1 through 8 might also be needed for family members.*

Travel Information

1. Has the patient traveled outside of the United States (during the incubation period)? If yes, where?
2. Has the patient traveled away from home (during the incubation period)? If yes, where?

3. What is the patient's normal mode of transportation and route to and from work (during the incubation period)?
4. Has the patient been to new or unique locations (e.g. a park, farm, wilderness area or body of water)?

Patient's Address (or Location Where Exposure May Have Taken Place)

1. Describe the location (e.g., type of community [rural versus urban], heavy crime area).
2. If the patient rents his or her home, what is the landlord's name?
3. Determine who has access (keys) to the patient's residence (e.g., landlord).

Incident Information

1. Has the patient received or heard any threats or unusual statements? Does the patient know whether he or she is the subject of a threat (future or past)? Does the patient know anyone who has been the recipient of a threat? Has the patient's employer been the subject of a threat?
2. Did the patient see an unusual device, anyone spraying something, or anything that could disperse a biological agent (e.g., envelope with white powder)?
3. If the patient attended a large event in the past 30 days, did anything suspicious occur during the event? Were any threats received at the event (or prior to it)?

* Refers to information that public health may typically collect by using its standard public health questionnaire.

4. Did the patient come in contact with laboratory equipment or a lab? Does the patient know of anyone who works in a lab with biological or chemical agents?
5. Ask the patient to provide an account of why he or she feels that they might have become sick.
6. Does the patient know anyone else who is sick (e.g., someone with a fever, cough, or unusual looking sores or rashes)?
7. Has the patient seen or touched any dead animals? Does the patient have pets that might be sick?
8. Does the patient have any affiliations with high-profile people (e.g., actors, politicians)?
9. Has the patient received anything unusual from a foreign country (e.g., a letter in the mail)?
10. Has the patient consumed anything unusual?
11. Does the patient report being bitten by insects or arthopods?

* Refers to information that public health may typically collect by using its standard public health questionnaire.

[2]Social Security Numbers typically are collected by law enforcement.

APPENDIX 8: Acronyms

The following list of acronyms is provided to help the investigator become familiar with some of the terms that might be encountered during an investigation involving WMD agents. Not all of these acronyms appear in this handbook.

AAR	After action review or after action report
APHL	Association of Public Health Laboratories
ASPR	Assistant Secretary for Preparedness and Response
BAR	BioWatch Actionable Result
BIO-1	Biological Incident Annex
CFR	Code of Federal Regulations
CBRNSU	Chemical, Biological, Radiological, and Nuclear Science Unit
DHS	Department of Homeland Security
DPEI	Division of Preparedness and Emerging Infections
EARS	Early Aberration Reporting System
EPA	Environmental Protection Agency
ESF	Emergency Support Function
FBI	Federal Bureau of Investigation
FBIHQ	Federal Bureau of Investigation Headquarters
HIPAA	Health Insurance Portability and Accountability Act
HMOU	Hazardous Materials Operations Unit
HMRTU	Hazardous Materials Response Team Unit
HMRSU	Hazardous Materials Science Response Unit

HSPD-5	Homeland Security Presidential Directive-5
JTTF	Joint Terrorism Task Force
MOU	Memorandum of Understanding
NCEZID	National Center for Emerging and Zoonotic Infectious Diseases
NGO	Nongovernmental Organization
NIMS	National Incident Management System
NOC	National Operations Center
NRF	National Response Framework
SIOC	Strategic Information and Operations Center
SME	Subject Matter Expert
BW	Biological Warfare or Biological Weapon
BWAT	Biological Weapons Anti-Terrorism
CDC	U.S. Centers for Disease Control and Prevention
CI	Confidential Informant
CONPLAN	Concept of Operations Plan (Federal)
CST	Civil Support Team (National Guard)
DHHS	U.S. Department of Health and Human Services
DoD	Department of Defense
DOJ	U.S. Department of Justice
DOS	U.S. Department of State
DOT	U.S. Department of Transportation
EOC	Emergency Operations Center

SUMMARY

ER	Emergency Room
FDA	U.S. Food and Drug Administration
FEMA	Federal Emergency Management Agency
FOUO	For Official Use Only
HAZMAT	Hazardous Materials
HMRT	FBI Hazardous Materials Response Team
HMRU	FBI Hazardous Materials Response Unit
HQ	Headquarters
HVAC	Heating, Ventilating, and Air Conditioning
ICS	Incident Command System
JIC	Joint Information Center
JOC	Joint Operations Center
LRN	Laboratory Response Network
PCR	Polymerase Chain Reaction
PDD	Presidential Decision Directive
PIO	Public Information Officer
POC	Point of Contact
PPE	Personal Protective Equipment
SITREP	Situation Report
TCE	Threat Credibility Evaluation
UC	Unified Command
USAMRIID	U.S. Army Medical Research Institute of Infectious Diseases

U.S.C.	United States Code
USDA	U.S. Department of Agriculture
WHO	World Health Organization
WMD	Weapons of Mass Destruction
WMDOU	Weapons of Mass Destruction Operations Unit

APPENDIX 9: Glossary

The following glossary is provided to help the investigator become familiar with some of the terms that might be encountered during an investigation involving WMD agents. Not all of these terms appear in this handbook.

ADENOPATHY	Swelling of the lymph nodes
ANTHRAX *[BACTERIA]	Disease caused by infection with the bacterium *Bacillus anthracis*
ANTITOXIN	Antibody formed in response to and capable of neutralizing a biological poison
ASTHENIA	Weakness or debility
ATAXIA	Inability to coordinate muscle activity during voluntary movement; incoordination of the gait
BLOOD AGAR	Mixture of blood and nutrient agar, used for the cultivation of many medically important microorganisms

SUMMARY

BOTULINUM TOXIN [TOXIN]*	Toxin produced by the bacterium *Clostridium botulinum*
BRADYCARDIA	Slow heartbeat
BRUCELLOSIS (UNDULANT FEVER) **[BACTERIA]**	Disease caused by bacteria of the genus *Brucella*. (e.g., *Brucella suis, Brucella abortus,* and *Brucella melitensis*)
COAGULOPATHY	Disease affecting the coagulability of the blood
COCCOBACILLUS	A short, thick bacterial rod in the shape of an oval or slightly elongated coccus
CUSTODY	Under the care or control of a legal authority; usually relating to persons or items (i.e., evidence.)
CUTANEOUS	Relating to the skin
CYANOSIS	A dark bluish or purplish coloration of the skin and mucous membrane, caused by deficient oxygenation of the blood
DISTAL	Situated away from the center of the body or from the point of origin; specifically applied to the extremity or distant part of a limb or organ
DYSPHAGIA, DYSPHAGY	Difficulty in swallowing
DYSPNEA	Shortness of breath or difficulty breathing

*These terms refer to the causative agent (i.e., bacteria, virus, toxin, or rickettsia) for the specified disease.

EDEMA	An accumulation of an excessive amount of watery fluid in cells, tissues, or cavities
ENCEPHALITIS	Inflammation of the brain
ENDOTOXEMIA	Presence of endotoxins in the blood
EPISTAXSIS	Bleeding from the nose
ERYTHEMA	Redness of the skin caused by capillary dilation
EXANTHEMA	Skin eruption occurring as a symptom of acute viral or coccal disease
FOMITE	Items, such as articles of clothing or eating utensils, that might harbor a disease and can transmit the disease
GLANDERS [BACTERIA]	Disease caused by infection with the bacterium *Burkholderia mallei* (formerly known as *Pseudomonas mallei*)
HEMATEMESIS	Vomiting blood
HEMATURIA	Blood or red blood cells in the urine
HEMOPTYSIS	Spitting blood from the lungs or bronchial tubes because of pulmonary or bronchial hemorrhage
HYPOTENSION	Low blood pressure

*These terms refer to the causative agent (i.e., bacteria, virus, toxin, or rickettsia) for the specified disease.

SUMMARY

HYPOTHERMIA	Low body temperature
MEIOSIS	Constriction of the pupil
MELIOIDOSIS (WHITMORE'S DISEASE) **[BACTERIA]**	Disease caused by infection with the bacterium *Burkholderia pseudomallei*
MYALGIA	Muscular pain
MYDRIASIS	Dilation of the pupil
PLAGUE [BACTERIA]	Disease caused by infection with the bacterium *Yersinia pestis*
PHYSICAL EVIDENCE	Tangible items that contain or bear information related to the facts of the case or investigation
PROBATIVE VALUE	The value of a piece of evidence in proving information in a legal trial
PROSTRATION	Marked loss of strength; extreme weakness
PRURITUS	Itching
PULMONARY EDEMA	Fluid in the lungs
PYROGENIC	Causing fever
RHINORRHEA	Watery discharge from the nose

RICIN [TOXIN]	Toxin made from the waste material (i.e., mash) remaining from processing castor beans
Q FEVER [BACTERIA]	Disease caused by infection with the bacterium *Coxiella burnetii*
TYPHUS FEVERS [BACTERIA]	Disease caused by the bacteria *Rickettsia prowazekii* (epidemic louse-borne) and *Rickettsia typhi* (endemic flea-borne or murine typhus)
SMALLPOX [VIRUS]	Disease caused by the infection with the *Variola* virus (species of Orthopox virus)
STAPHYLOCOCCUS ENTEROTOXIN B [TOXIN]	Toxin produced by bacterium *Staphylococcus aureus*
TACHYCARDIA	Rapid heartbeat
THREAT ASSESSMENT (JOINT)	Joint evaluation of a potential incident involving a biological agent or toxin, by both public health and law enforcement agencies
THREAT CREDIBILITY EVALUATION	A threat credibility evaluation is a real-time, interagency, coordinated process facilitated by the FBI WMDOU
TRICHOTHECENE MYCOTOXINS (T-2 MYCOTOXINS) **[TOXIN]**	Toxin produced by filamentous fungi primarily of the genera *Fusarium, Myrotecium, Trichoderma, Stachybotrys*

SUMMARY

TULAREMIA (RABBIT FEVER OR DEERFLY FEVER) **[BACTERIA]**	Disease caused by infection with the bacterium *Francisella tularensis*
TYPHOID FEVER DISEASE [BACTERIA]	Disease caused by infection with the bacterium *Salmonella typhi*
VARIOLA [VIRUS]	A virus that is the causative agent for smallpox
VIREMIA	Presence of virus in the blood
ZOONOSIS	Disease of humans acquired from animal source

APPENDIX 10: Acknowledgements

This handbook was the result of contributions and input from a host of individuals. Special thanks go to these following departments and agencies for their participation and contributions to the development of this publication. Contributors are listed in alphabetical order.

FBI

- WMD Directorate
  - — WMD Biological Countermeasures Unit
  - — WMD Operations Unit

CDC

- National Center for Emerging and Zoonotic Infectious Diseases (NCEZID)
  - — Division of Preparedness and Emerging Infections (DPEI)

This handbook represents a joint effort of the
Federal Bureau of Investigation, the Centers for Disease Control
and Prevention, and the Department of Justice.

CENTERS FOR DISEASE CONTROL AND PREVENTION

To obtain additional copies or with questions, please contact your local FBI FIELD OFFICE/FBI WMD Coordinator.