

STATE OF OHIO EMERGENCY OPERATIONS PLAN

TERRORISM INCIDENT ANNEX

Primary Agencies:	Ohio Homeland Security (OHS) Ohio State Highway Patrol (OSHP)
Support Agencies:	Ohio Adjutant General's Department – Ohio National Guard (ONG) Office of the Attorney General (AG) Ohio Department of Administrative Services (DAS) Ohio Department of Agriculture (ODA) Ohio Department of Commerce, Division of the State Fire Marshal (SFM) Ohio Emergency Management Agency (OEMA) Ohio Environmental Protection Agency (OEPA) Ohio Department of Health (ODH) Ohio Department of Natural Resources (ODNR) Ohio Emergency Medical Services (OEMS) Public Utilities Commission of Ohio (PUCO) Ohio Department of Rehabilitation and Correction (ODRC) Ohio Department of Transportation (ODOT)

I. INTRODUCTION

A. Purpose

1. The purpose of this Plan is to:
 - a. Present an overview of the terrorism-related hazards that potentially face the State of Ohio
 - b. Describe the State-level framework of capabilities that exist to address those hazards
 - c. Provide an outline of the concept of operations that will be employed
 - d. Provide an outline of the assignment of responsibilities of State Agencies (listed above) that are partner to this Plan that will be applied to terrorism-related incidents that occur within the State.

B. Scope

1. This Plan applies to all acts, or threats, of terrorism that could have serious effects upon the state and its population. The Federal Bureau of Investigation (FBI) defines

terrorism as, "...the unlawful use of force against persons or property to intimidate or coerce a government, civil population, or any segment thereof, in the furtherance of political or social objectives". Chapter 2909.21 of the Ohio Revised Code (ORC) further defines "Acts of Terrorism" applicable to the state of Ohio.

2. A terrorism-related incident that occurs in Ohio will require that immediate local-, State- and federal-level actions be initiated. Response to any terrorism-related incident will follow the operational priorities of a) protection of life safety, b) stabilization of incident environment(s) and c) restoration of property and the built environment.
3. Response to terrorism-related incidents will be centered on and will be geared toward enabling responding organizations to recognize the situation, rapidly and effectively exchange data, initiate and direct responses, and enable other offices to determine and prepare their roles in subsequent recovery-related actions.
4. Command and control over terrorism-related incidents will remain with the lowest-possible jurisdictional level.
5. Presidential Decision Directive 39, the U.S. Policy on Counterterrorism, 1995, designates the FBI as the lead agency for federal domestic terrorism response actions, with assistance furnished by state and local governments as required. If an event is determined to be an act of terrorism, federal resources will be brought to bear in support of operations in the state of Ohio. These may include specialists from Domestic Emergency Support Team, HAZMAT, Joint Terrorism Task Forces, or other fields as required. Their availability will be coordinated by the FBI and the state EOC.
6. Ohio Revised Code §5502.03(B)(2) designates Ohio Homeland Security as the lead agency for collecting, analyzing, maintaining, and disseminating information to support local, state, and federal law enforcement agencies, other government agencies, and private organizations in detecting, deterring, preventing, preparing for, responding to, and recovering from threatened or actual terrorist events. This information is not a public record pursuant to section §149.43 of the Revised Code. Am. Sub. S. B. No. 9 47. §5502.03(B) further states that OHS will develop and coordinate policies, protocols, and strategies that may be used to prevent, detect, prepare for, respond to, and recover from terrorist acts or threats; and that OHS will coordinate efforts of state and local governments and private organizations to enhance the security and protection of critical infrastructure and key assets in this state.
7. The State of Ohio has developed a list of Critical Facilities within the state. This list is maintained as a "Security Document" in accordance with Ch. 149.433 (ORC). Increased security measures with regard to these facilities will be taken automatically in conjunction with changes to various terrorism threat levels. These measures will be addressed in specific action plans which will also be developed and maintained as "Secure Documents". Changes or additions to such security measures will be

recommended by the State Homeland Security Advisor to the governor based on current intelligence from the State Fusion Center and its partners.

8. Specific terrorist acts/operations; include, but would not be limited to, the following general categories:
 - a. **Chemical events**, to include WMD employment (Ref: Appendix B, Tool Kit for Managing the Emergency Consequences of Terrorist Incidents, July, 2002 and State of Ohio Hazardous Materials Emergency Plan, 2001).
 - b. **Biological events**, to include WMD employment (Ref: Appendix A, Tool Kit for Managing the Emergency Consequences of Terrorist Incidents, July, 2002 and Threatened Human Biologic Incidents: Ohio Guidelines (ODH) 2002, Animal Disease Incident Plan 2008).
 - c. **Nuclear/radiological events**, to include WMD employment (Ref: Appendix C, Tool Kit for Managing the Emergency Consequences of Terrorist Incidents, July, 2002, The State of Ohio Plan for Response to Radiological Incidents at Licensed Nuclear Facilities, 2002, and The Ohio Plan for Response to Radioactive Material Transportation Accidents).
 - d. **Conventional events** (to include bombings, arson, armed assaults, etc (Ref: State of Ohio Threat Analysis and Risk Assessment, 2001, OPLAN Ready - Adjutant General's Department of Ohio, 2001, State Highway Patrol Response Plans [by Facilities], Ohio Department of Public Safety, 2002, and The Fire and Explosive Investigation Written Procedures IAW Ch. 3737. ORC, Division of the State Fire Marshal, 2002).
 - e. Infrastructure - **cyber events**, to include actions involving, or affecting, Information Technology, data processing and storage (Ref: Appendix D, Tool Kit for Managing the Emergency Consequences of Terrorist Incidents, July, 2002).
 - f. **Combined hazards**, incorporating elements of "a" to "e", with reference to applicable guidance and operational plans as cited above). (1) Preparedness for possible terrorist attacks must also consider that a variety of methods and devices may be employed. These range from sophisticated, or "high-tech" chemical, biological and radiological devices, to simple, "home-made", or "low-tech" materials obtainable in hardware and farm supply stores.
 - g. Delivery and employment of these items may entail the use of mails, aircraft, watercraft, motor vehicles, or hand delivery to an intended target.
10. Areas, facilities, complexes, or installations that may be potential targets for acts of terrorism at any level may include:
 - a. Educational institutions, including schools, colleges, and universities.

- b. Military installations, including camps, bases, stations, and armories.
- c. Research and development complexes (private and public).
- d. Commercial facilities.
- e. Transportation routes, hubs and centers, including rail yards, airfields, terminals and intermodal sites.
- f. Religious edifices, including shrines and monuments.
- g. Entertainment/recreational facilities, areas, events, & exhibitions.
- h. Governmental administrative/operating facilities and centers.
- i. Health and medical (to include pharmaceutical and laboratory) facilities.
- j. Agricultural and food production, including farms, auction markets/concentration yards, and processing, slaughter, storage and distribution sites/facilities.
- k. Monuments and symbolic structures
- l. Chemical production and storage facilities
- m. Water treatment, storage, containment dams and transmission facilities
- n. Banking and financial institutions
- o. Energy production and transmission facilities
- p. Telecommunications and information management facilities
- q. Political and special-interest facilities
- r. Manufacturing
- s. Nuclear reactors, materials and waste
- t. Postal and shipping

11. Potential demographic (population) targets include, but are not limited to:

- a. Management and staff from the above named facilities and sites.
- b. Minorities (racial, religious, cultural).

- c. Political parties and/or factions thereof.
- d. Other (fraternal and social) groups.

C. Capabilities

This plan addresses actions related to the following 11 capabilities:

1. Information Gathering and Recognition of Indicators and Warnings

Information Gathering and Recognition of Indicators and Warning Capability includes the gathering, consolidation, and retention of raw data and information from sources to include human sources, observation, technical sources and open (unclassified) materials. Unlike intelligence collection, information gathering is the continual gathering of only pure, unexamined data, instead of the collection of information that is traditionally conducted by the intelligence community or targeted investigations.

Recognition of indicators and warnings is the ability to see in this gathered data the potential trends, indications, and/or warnings of criminal and/or terrorist activities (including planning and surveillance) against U.S. citizens, government entities, critical infrastructure, and/or our allies. In these efforts, locally-generated threat and other criminal and/or terrorism-related information will be identified, gathered, entered into an appropriate data/retrieval system, and provided to appropriate analysis centers.

2. Intelligence Analysis and Production

Intelligence Analysis and Production is the merging of data and information for the purpose of analyzing, linking, and disseminating timely and actionable intelligence with an emphasis on the larger public safety and homeland security threat picture. This process focuses on the consolidation of analytical products among the intelligence analysis units at the Federal, State, local, and tribal levels for tactical, operational, and strategic use. This capability also includes the examination of raw data to identify threat pictures, recognize potentially harmful patterns, or connect suspicious links to discern potential indications or warnings.

Timely, accurate, and actionable intelligence/information products are produced in support of prevention, awareness, deterrence, response, and continuity planning operations.

3. Epidemiological Surveillance and Investigation

An Epidemiological Surveillance and Investigation capability is the capacity to rapidly conduct epidemiological investigations for humans and animals. It includes exposure and disease (both deliberate release and naturally occurring) detection, rapid

implementation of active surveillance, maintenance of ongoing surveillance activities, epidemiological investigation, analysis, and communication with the public and providers about case definitions, disease risk and mitigation, and recommendation for the implementation of control measures.

Potential exposure to disease will be identified rapidly by determining exposure and mode of transmission and agent; interrupting transmission to contain the spread of the event; and reducing number of cases. Confirmed cases are reported immediately to all relevant public health, animal health, food regulatory, environmental regulatory, and law enforcement agencies. Suspected cases are investigated promptly, reported to relevant public health or agriculture authorities, and accurately confirmed to ensure appropriate preventive or curative countermeasures are implemented. An outbreak is defined and characterized; new suspect cases are identified and characterized based on case definitions on an ongoing basis; relevant clinical specimens are obtained and transported for confirmatory laboratory testing; the source of exposure is tracked; methods of transmission identified; and effective mitigation measures are communicated to the public, providers, and relevant agencies, as appropriate.

4. Counter-Terror Investigation and Law Enforcement

Counter-Terror Investigation and Law Enforcement is a capability that includes a broad range of activities undertaken by law enforcement and related entities to detect, examine, probe, investigate, and conduct operations related to potential terrorist activities. Current and emerging investigative techniques will be used with an emphasis on training, legal frameworks, recognition of indications and warnings, source development, interdiction, and related issues specific to counter-terrorism activities. Suspects involved in criminal activities in Ohio that are related to homeland security threats will be successfully deterred, detected, disrupted, investigated, and apprehended.

5. Food and Agriculture Safety and Defense

Food and Agriculture Safety and Defense is a capability to prevent, protect against, respond to, and recover from chemical, biological and radiological contaminants, and other hazards that affect the safety of food and agricultural products. This will include the timely eradication of outbreaks of crop and animal diseases/pests, assessments of the integrity of the food producing industry, the removal and disposal of potentially compromised materials from the U.S. food supply, and decontamination of affected food manufacturing facilities or retail points of purchase or service. This will also include appropriate laboratory surveillance to detect human food-borne illness, animal disease or food product contamination.

Additionally, the public will be provided with accurate and timely notification and instructions related to a contamination event and will be given appropriate steps to follow with regard to disposal of affected food or agricultural products and/or appropriate decontamination procedures. Threats to food and agriculture safety will be prevented, mitigated, and eradicated; affected products will be disposed of;

affected facilities will be decontaminated; public, animal and plant health will be protected, and notification of the event and instructions of appropriate actions will be effectively communicated with all stakeholders.

6. Laboratory Testing

A Laboratory Testing capability includes the ongoing surveillance, rapid detection, confirmatory testing, data reporting, investigative support, and laboratory networking to address potential exposure, or exposure, to all hazards. These hazards can include chemical, radiological, and biological agents in all matrices including clinical human or animal specimens, food and environmental samples, (water, air, soil). These threats can include those deliberately released with criminal intent, as well as those that may be present as a result of unintentional or natural occurrences.

Potential exposure to disease will be identified rapidly by determining exposure and mode of transmission and agent; interrupting transmission to contain the spread of the event; and reducing number of cases. Confirmed cases will be reported immediately to all relevant public health, animal health, food regulatory, environmental regulatory, and law enforcement agencies. Suspected cases will be investigated promptly, reported to relevant public health and agriculture authorities, and accurately confirmed to ensure appropriate preventive or curative countermeasures are implemented.

Outbreaks will be defined and characterized; new suspect cases are identified and characterized based on case definitions on an ongoing basis; relevant clinical human or animal specimens will be obtained and transported for confirmatory laboratory testing; the source of exposure will be tracked; methods of transmission will be identified; and effective mitigation measures will be communicated to the public, providers, and relevant agencies, as appropriate.

7. CBRNE Detection

A preventive Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) Detection capability provides the ability to detect CBRNE materials at points of manufacture, transportation, and use. The activities and tasks associated with this capability will be carried out individually for each specific agent, rather than for all agents at the same time. Therefore, when considering critical tasks and preparedness measures, each task and measure should be applied separately to each CBRNE agent.

This capability includes the detection of CBRNE material through area monitoring, but does not include detection by their effects (i.e., signs or symptoms) on humans and animals. Population-level monitoring will be addressed within the Epidemiological Surveillance and Investigation and Animal Disease Emergency Support capabilities. A CBRNE Detection capability includes the identification and communication of CBRNE threats, but does not include actions taken to prevent an incident or respond to the consequences of a CBRNE incident.

A CBRNE detection capability includes technology, as well as the capacity to recognize potential CBRNE threats through equipment, education, and effective protocols. Training, communication, close coordination with key partners, including intelligence, law enforcement, public safety, public health, agriculture, and international partners, and public and private sector awareness of CBRNE threats will be recognized as critical enablers for this capability. Chemical, biological, radiological, nuclear, and/or explosive (CBRNE) materials are rapidly detected and characterized at borders and ports of entry, critical locations, events, and incidents.

The scope of CBRNE detection will include: 1. Manufacture – The illegal production of CBRNE material within the borders of the U.S. and its territories; 2. Transport – The movement of CBRNE material outside, across, and within the borders of the State; and 3. Use – The deployment, emplacement, or employment of CBRNE material within the State.

8. Explosive Device Response Operations

An Explosive Device Response Operations capability coordinates, directs, and conducts improvised explosive device (IED) response after initial alert and notification. This includes the coordination of intelligence fusion and analysis, information collection and threat recognition, situation assessment and the conduct of appropriate Render Safe Procedures (RSP). This capability also includes the conduct of searches for additional devices and the coordination of overall efforts to mitigate chemical, biological, radiological, nuclear, and explosive (CBRNE) threats at incident sites.

Threat assessments will be conducted, explosive and/or hazardous devices will be rendered safe, and impacted areas will be cleared of hazards. Measures will be implemented in the following priority order: ensuring public safety; safeguarding officers and responders at the scene; collection and preservation of evidence; protection and preservation of public and private property; and restoration of public services.

9. WMD and Hazardous Materials Response and Decontamination

A Weapons of Mass Destruction (WMD) and Hazardous Materials Response and Decontamination capability assesses and manages the consequences of hazardous materials releases, both accidental or as part of a terrorist attack. It includes the testing and identification of all hazardous substances onsite; and ensures that responders have protective clothing and equipment; conducts rescue operations to remove affected victims from the hazardous environment; conducts geographical survey searches of suspected sources or contamination spreads; establishes isolation perimeters; mitigates the effects of hazardous materials, decontaminates on-site victims, responders, and equipment; coordinates off-site decontamination with relevant agencies, and notifies environmental, health, agriculture, and law

enforcement agencies having jurisdiction for the incident to begin implementation of their standard evidence collection and investigation procedures.

Hazardous materials releases will be rapidly identified and mitigated; victims exposed to the hazard will be rescued, decontaminated, and treated; the impacts of release will be limited; and responders and at-risk populations will be effectively protected.

10. Intelligence and Information Sharing and Dissemination

An Intelligence and Information Sharing and Dissemination capability will provide necessary tools to enable efficient and effective prevention, protection, response, and recovery activities. Intelligence and Information Sharing and Dissemination is the multi-jurisdictional, multidisciplinary exchange and dissemination of information and intelligence among all levels of government, the private sector, and citizens within the State of Ohio. The goal of sharing and dissemination will be to facilitate the distribution of relevant, actionable, timely, and preferably declassified or unclassified information and/or intelligence that will be updated frequently to the end-users who need it, with the goal of getting the right information to the right people at the right time.

An effective intelligence/information sharing and dissemination system will provide durable, reliable, and effective information exchanges between those responsible for gathering information and the analysts and consumers of threat-related information. Effective and timely sharing of information and intelligence will occur across all jurisdictional levels within the State and private sector entities, resulting in coordinated awareness of, prevention of, protection against, and response to a threatened or actual domestic terrorist attack, major disaster, or other emergency.

11. Critical Infrastructure Protection

A Critical Infrastructure Protection capability enables public and private entities within the State to identify, assess, prioritize, and protect critical infrastructure and key resources so they can detect, prevent, deter, devalue, and mitigate deliberate efforts to destroy, incapacitate, or exploit the State's critical infrastructure and key resources. The risk to, vulnerability of, and consequence of an attack on critical infrastructure will be reduced through the identification of critical infrastructure; conduct, documentation, and standardization of risk assessments; prioritization of assets; decisions regarding protective and preventative programs; and the implementation of protective and preventative plans.

II. SITUATION

Prevention consists of those activities that serve to detect, deter, and disrupt terrorist threats or actions against the State of Ohio, its citizens and its interests. These activities decrease the perpetrators' chance of success, mitigate attack impact, minimize attack visibility, increase

the chance of apprehension or detection, and obstruct perpetrators' access to resources. Tasks addressed under these capabilities will be important regardless of the type of threat, adversary capability, or time or location of an incident. Similarly, these capabilities reflect many tasks routinely undertaken by law enforcement and related organizations as they conduct traditional all-hazards, all-crimes activities. Effective prevention depends on timely, accurate, and actionable information about the adversary, their operations, their support, potential targets, and methods of attack.

Intelligence/information fusion is an ongoing, cyclical process that incorporates three primary capabilities: Information Gathering and Recognition of Indicators and Warnings; Intelligence Analysis and Production; and Intelligence and Information Sharing and Dissemination.

The Federal Homeland Security Advisory System (HSAS) is based upon the dissemination of threat-related information to federal, state, and local offices or the public from the U.S. Attorney General's Office. HSAS advisories will cause coordinated preparedness measures to be taken based upon a specific threat level. State and local agencies are to develop their response procedures in accordance with threat level changes determined by the HSAS (Ref: Attachment A).

Credible Threats are those based upon accrued evidence that indicates an act of terrorism has occurred or is about to occur. Credible threat information may further indicate the use or presence of WMD.

The state of Ohio will change threat condition levels automatically when changes to national threat conditions are announced by the federal government (to include State EOC activation at "Orange or Red").

The State Homeland Security Advisor will consider incident and threat information related changes to threat levels and make recommendations to the governor to downgrade or upgrade as appropriate. Each State Agency will implement the appropriate threat-level security plan.

The Situations for the eleven capabilities addressed above are:

A. Information Gathering and Recognition of Indicators and Warnings

1. This capability applies to all potential terrorist incidents. Homeland security intelligence/information fusion is the overarching process of managing the development and flow of information and intelligence across all levels and sectors of government and the private sector on a continual basis. Although the primary emphasis of the State's fusion efforts are to identify, deter, and respond to emerging terrorism-related threats and risks, and efforts to provide ongoing efforts to address non-terrorism-related, all-hazards, all-crimes issues. The data collected from Information Gathering and Recognition is further analyzed and processed by Intelligence Analysis and Production.

B. Intelligence Analysis and Production

1. This capability applies to all potential terrorist incidents. This would include explosives devices, hazardous materials tank explosions, biological and toxic releases, nuclear devices, and radiological dispersals. Homeland security intelligence/information fusion is the overarching process of managing the development and flow of information and intelligence across all levels and sectors of government and the private sector on a continual basis. Although the primary emphasis of fusion is to identify, deter, and respond to emerging terrorism-related threats and risks, a collateral benefit to the State is that it will support ongoing efforts to address non-terrorism-related, all-hazards, all-crimes issues.
2. The results of the analyses in Intelligence Analysis and Production are disseminated using Intelligence and Information Sharing. Planning Products that result from Intelligence Analysis and Production are used to ensure that plans adequately address terrorist threats. Risk Management Products from Intelligence Analysis and Production provide the threat, vulnerability, and consequence data used in risk management
3. Counter-Terror Investigation and Law Enforcement is one source of data analyzed by the Intelligence Analysis and Production capability. The products of the Intelligence Analysis and Production capability may further inform Counter-Terror Investigation and Law Enforcement investigations. CBRNE Detection is one source of data analyzed by Intelligence Analysis and Production. Citizen reports of suspicious activities is another source of data analyzed by Intelligence Analysis and Production.

C. Epidemiological Surveillance and Investigation

1. Although applicable to several of the 15 National Planning Scenarios, the capability planning factors under this capability will apply to the Anthrax, Pandemic Influenza, and Foreign Animal Disease scenarios. Estimates will be made of the needs for communities to respond to epidemiological emergencies once they are identified and for baseline resources needed for timely initial detection. Epidemiological Surveillance and Investigation contributes data for analysis and is provided reports, as appropriate.

For incidents that are addressed under this capability, it will be assumed that:

2. Bacillus anthracis spores will have been added directly to a product without aerosolization
3. Patient presentations will have involved gastrointestinal, oropharyngeal, and cutaneous forms of anthrax.
4. Clinical and laboratory confirmation will have occurred between days 2 and 5 after index case presentation

5. Production facilities and distribution system mechanisms will be contaminated until formally decontaminated
6. Cases will continue sporadically following public health intervention due to consumers and retailers failing to discard/return/destroy contaminated product
7. There will be an unprecedented level of public concern, anxiety, and fear as a result of these incidents.
8. Field investigations will last 10 days at full personnel strength and then another 20 days at 50 percent personnel strength.
9. There may be a concurrent law enforcement investigation at more than one jurisdictional level.
10. Staffing in response to these incidents may include Federal or State employees at the local level, and staffing in response to these incidents may include Federal employees.
11. Nearly 100% of all cases resulting from these incidents will be interviewed during the first 10 days after the first presentation of symptoms, and 50% of non-cases will be interviewed within 30 days after the first presentation of symptoms.
12. Food contamination scenarios will involve a national response that involves local, State and Federal resources.
13. The percent of staff contributions to the investigation from the State and local levels will be dependent on the availability of resources.
14. Due to potentially unforeseen delays in the identification of non-naturally occurring epidemiological events, detection of disease outbreaks may not occur until large numbers of victims are affected, particularly when the agent has a long incubation period.
15. Animal disease incidents may involve a national response that involves local, State and Federal resources.

D. Counter-Terror Investigation and Law Enforcement

1. This capability applies to all potential terrorist incidents and is applicable to all 12 terrorism-related National Planning Scenarios, however this capability is most-closely related to bombings using improvised explosives devices, chlorine tank explosions, the use of aerosolized anthrax, improvised nuclear devices, and radiological dispersals.

2. Homeland security intelligence/information fusion is the overarching process of managing the development and flow of information and intelligence across all levels and sectors of government and the private sector on a continual basis. Although the primary emphasis of fusion is to identify, deter, and respond to emerging terrorism-related threats and risks, a collateral benefit to the state is that it will address non-terrorism-related, all-hazards, all-crimes issues.

E. Food and Agriculture Safety and Defense

1. Although applicable to several of the 15 National Planning Scenarios except for blister agents and nerve agents, this capability is most-closely related to the Food Contamination scenario. This capability applies to a wide range of incidents and emergencies including accidental or deliberate human or animal disease outbreaks, natural disasters, and nuclear and conventional events with potential for contamination of the food supply.
2. The identification of an intentional contamination incident involving a food product in the State of Ohio will have national implications. Because of the movement of food products around the United States and within the State of Ohio, it is highly probable that multiple food facilities in multiple States may have been contaminated.
3. If terrorists were to introduce a chemical or biological agent into a food product at multiple sites simultaneously within the State or around the country, the requirements for resources will increase proportionately and may exist in many States or parts of the State of Ohio simultaneously. The requirements for tactical (incident command) resources will increase proportionately with the amount of product/products contaminated.
4. It is likely that resources will be shared within the State and between states, and entities providing resources will have to balance the sharing of resources of their resources with their need to protect public and animal health within their own jurisdiction. The amount of tactical resource requirements will vary depending on the concentration of food facilities within a jurisdiction.
5. In high food facilities/people concentration areas, the spread of the effects of an incident of food and/or agricultural contamination may be rapid and many food facilities that purchased contaminated food may be affected. In areas with low concentration of food facilities/people, logistical obstacles such as driving time or distance between involved locations may present additional challenges. The time to resolve an incident will vary depending on number of site introductions and the number of different food items that have been contaminated.
6. The Food and Drug Administration regulates 80 percent of the nation's food supply – everything except meat, poultry, and egg products which are regulated by USDA. Based on vulnerability assessments conducted by the FDA and the USDA, other scenarios could have potentially more far-reaching effects.

7. For incidents that are addressed under this capability, it will be assumed that:
 - a. All response personnel in key positions will be able to respond to their respective response positions after a contaminant has been introduced and they may not respond as they are expected.
 - b. Sector partners are effectively connected to an information sharing and analysis or fusion system concept where preventative and protective measure information is proactively being shared.
 - c. Lack of infrastructure – electricity, phones, transportation, etc., will affect the ability to effectively communicate and will significantly affect the ability to plan appropriately or to respond to an incident.
 - d. If roads are non-passable due to a natural disaster, this may affect the ability to get to impacted areas.
 - e. Multi-Agency Coordination will be adequately addressed at State and local levels, and agencies will coordinate their responses as expected.
 - f. The following information will be needed to effectively detect/respond to/recover from an incident: Quantity of product affected, Distribution of product, Product type or types contaminated, Laboratory capability, Ability to determine the cause of illness, Ability to determine the food item associated with illness or to rule out certain food items, Ability to trace back product, Ability to trace forward product, Ability to effectively recall all affected product, Appropriate disposal of recalled product, Appropriate decontamination of food facility or other locations where food was available for purchase, Risk communication to consumers about appropriate food disposal instructions, and Communication with international partners.
8. The total time for recovery under this capability could last several months, depending on the complexity, severity and breadth of the incident.

F. Laboratory Testing

Plans to augment the capacity of public, animal, plant and food health laboratories should include having or having access to information systems that electronically send and receive test orders and results in compliance with PHIN Functional Area for Connecting Laboratory, Food Emergency Response Network (FERN), National Animal Health Laboratory Network (NAHLN) Systems.

1. Chemical Nerve Agents

- a. In the case of the accidental or intentional release of a chemical nerve agent, in addition to affected individuals, there will be many worried well.

- b. Up to 25% of the worried well population will require testing as well as the population of affected individuals.
- c. It will be difficult to determine exactly what proportion of the downwind population would fall in the worried-well category, but it is possible that 80 percent of the downwind population may fall into the worried-well population.
- d. Currently, chemical nerve agent analytic resources are located at the Centers for Disease Control in Atlanta, Georgia and at the state health departments of California, Florida, Michigan, Minnesota, New Mexico, New York and Virginia.

2. Laboratory Testing for Biological Agents

For laboratory testing for biological agents, it will be assumed that:

- a. Bacillus anthracis spores will have been added directly to products without aerosolization.
- b. Patient presentations will have involved gastrointestinal, oropharyngeal or cutaneous forms of anthrax.
- c. Laboratory confirmations will occur between 2-5 days after an index case presentation.
- d. Production facilities and distribution system mechanisms will be contaminated until formally decontaminated.
- e. Cases will continue sporadically following public health intervention due to consumers and retailers failing to discard/return/destroy contaminated product.
- f. Factors that could affect the number of specimens/samples calculated could include time involved to set up the assay, machine capacity, personnel shift durations, the condition that specimens/samples arrived in, physical working space, and individual pace of laboratorians. Laboratory surge capacity needs will be addressed by Laboratory Response Network (LRN), FERN, and NAHLN systems.
- g. Case definition by epidemiologists will be created within the first 10 days resulting in no further rule out testing at testing laboratories.
- h. There will be concurrent law enforcement investigations within multiple jurisdictions and at multiple governmental layers.

G. CBRNE Detection

Applicable situations for this capability include: explosive devices, hazardous materials tank explosions, biological and toxic releases, nuclear devices, and radiological dispersals.

A CBRNE Detection capability addresses biological agents outside of the body (human and animal), and does not include medical or plant samples (blood and medical tests). Medical and syndromic surveillance detection of biological agents is addressed in Epidemiological Surveillance and Investigation, as well as in Food and Agriculture Safety (see II.C and II.E, above). To be effective, close integration of these capabilities must occur with the CBRNE Detection capability.

1. Large-Scale Events

- a. The main strategy will be to use detection technologies and screening processes to interdict CBRNE materials before they are used. The alternative strategy will be to rely on existing detection technology, law enforcement investigations and alternate technologies to determine the presence of threat devices.
- b. A national capability to address large CBRNE events will be developed through the design and deployment of the Global Nuclear Detection Architecture and other similar programs.
- c. The State and its local jurisdictions will seek to develop and implement detection capabilities through use of DHS grants and guidance.
- d. Develop equipment, training and communications standards to facilitate and validate the deployment and use of detection technologies.

H. Explosive Device Response Operations

1. Coverage by Bomb Squad Teams

- a. Coverage of high-density population and critical infrastructure/key resources (CI/KR) locations by Type I level bomb squad teams is critical to the adequate protection of these assets and resources. For other locations, and when possible, Type I, II, or III level teams, based on population, population density, critical infrastructure requirements, and additional factors will be placed.
- b. All situations must be assessed by the bomb technician on the scene as to time sensitive considerations. Safety issues will take precedence over time considerations.
- c. In a catastrophic level Vehicle Borne Improvised Explosive Device (VBIED) situation where full remote capabilities are available, it is desired to have the

technological potential for diagnostics and execution of the disruption tools within one hour from time of arrival on the scene.

2. Response to Large Vehicle Bombs

- a. Radio Controlled Improvised Explosive Devices (RCIED) will require a response from a Type II team minimum, plus Electronic Countermeasures (ECM) training and equipment that meets standards set by NBSCAB

3. Response to Suicide Bomber(s)

- a. Effective response times to suicide bombers are directly related to threat identification and the communicative chain to dispatch.
- b. Response timelines to suicide bombers are dependent on location of the event relative to the placement of the capability(ies).
- c. Response to suicide bombers will be more effective if a system is in place to ensure the timely receipt of intelligence or device information to assist those responding to the threat.
- d. Bomb Squad – A bomb response organization consists of at least one bomb response team (see the definition of a “bomb response team”), accredited by the FBI Hazardous Devices School to standards set by the National Bomb Squad Commanders Advisory Board.
- e. Bomb Response Team – A sub-unit within a bomb squad, consisting of at least two certified bomb technicians and a full set of equipment meeting minimum standards for bomb squad operations. Military EOD units are not currently resource typed within NIMS but are available to respond to incidents in the community either to assist the “accredited” bomb squad, or respond to the incident in an area without State/local bomb squad presence.

I. WMD and Hazardous Materials Response and Decontamination

This capability applies to a wide range of incidents and emergencies, including those caused by explosive devices, hazardous materials tank explosions, biological and toxic releases, nuclear devices, and radiological dispersals.

For incidents that are addressed under this capability, it will be assumed that:

1. If decontamination is ongoing during the early stages of a catastrophic incident, persons undergoing decontamination will have logistical, medical, and mental health needs that will need to be addressed quickly.

2. Decontamination priorities will be set up using the following priorities, in order of importance: life safety, incident stabilization, and property conservation.
3. Efforts will be made to ensure that all fires are extinguished within a 4-day response phase.
4. Water-based oil release may extend beyond the 4-day limit. Assets will be on scene, but containment operations may not be able to begin immediately on arrival.
5. State-level resources will respond to these events within 12–24 hours. Federal resources will respond to these events within 24 hours. The United States has approximately 64 nuclear stations supported by the Radiological Emergency Preparedness Program (REPP). No less than 30 REPP response teams should be able to respond to an “improvised nuclear device” scenario within 24 hours.
6. A significant number of individuals exposed to a plume cloud or contaminant agent will flee the scene before first responders arrive. It may prove difficult to determine which of those individuals require decontamination, and to ensure such individuals present themselves for decontamination.
7. Each jurisdiction is expected to sponsor and support community emergency response teams (CERTs).
8. The projected effects of contamination resulting from a catastrophic incident are generally based on an estimated population density of 2,000 people per square mile, but may increase for major urban areas.
9. Large-gathering situations (National Security special events, sporting events, conventions, etc.) create higher localized population densities.
10. Biological agents typically have delayed symptoms. As such there will rarely be an on-site incident requiring response when a biological agent is released.
11. Health care facilities are the most likely locations for managing a human biological incident.
12. Secondary contamination will be a major concern. Hospital emergency rooms may close if patients are admitted without proper decontamination. Other secondary contamination issues include control of runoff of fluids used in decontamination, and the handling of contaminated clothing and personal effects. In addition, the secondary contamination of first responders, even those wearing personal protective equipment, can occur during the removal of patients from a hazardous area, during the performance of basic life support functions, or when initial responders are unaware that a hazardous material is involved.

13. The psychological dimensions of being exposed to a contaminant, and subsequent decontamination may present social management challenges and concerns. Of greatest concern are the short- and long-term psychological consequences resulting from actual exposure to chemical, biological, and radiological substances, and which subsequently produce negative health effects. Short-term stress symptoms may be a prelude to long-term, debilitating, post-traumatic stress disorder.

J. Intelligence and Information Sharing and Dissemination

1. The actions that are taken under this capability reflect many tasks that are routinely undertaken by law enforcement and related organizations as they conduct traditional all-hazards, all-crimes activities.
2. Although the primary emphasis of fusion center activities is to identify, deter, and respond to emerging terrorism-related threats and risks, a collateral benefit to Federal, State, local, and tribal entities is that it will support ongoing efforts to address non-terrorism-related, all-hazards, all-crimes issues.

K. Critical Infrastructure Protection

1. This capability applies to a wide range of incidents and emergencies, including those caused by any terrorism-related, accidental, or natural catastrophic event that could disrupt or destroy CI/KR in one or more sectors. Protective measures may be implemented based on the potential statewide impact if an infrastructure asset is damaged or destroyed, as a result of a terrorist attack, manmade or natural disaster or structural failure.
2. Under the CIP process as defined in the NIPP, protection of CI/KR requires an initial determination of whether the asset/system in question and the risks being posed are “critical.” Therefore, protection activities are conducted on a case-by-case basis.
3. For incidents that are addressed under this capability, it will be assumed that:
 - a. Resource needs at the State and local level will be determined through the development of a model that takes into account the presence and density of CI/KR assets in various geographic areas.
 - b. State and local law enforcement resources will be available to support CI/KR protection efforts, as required.
 - c. Critical infrastructure information will be able to be shared between Federal, State and local authorities and the private sector in a protected and secure way.

III. ASSUMPTIONS

A. A terrorist event will create such a disaster that federal assistance is needed and the president will activate the Federal Emergency Response Plan.

B. Federal Actions

1. The FBI will be available for on-site observation and advisory actions as required. If an event is expected to be or is determined to be an act of terrorism, federal support will be available. As conditions warrant, the FBI will establish a Joint Operations Center (JOC) to provide incident management support for state or local agencies as directed by the FBI On-Scene Commander (OSC).
2. The FBI employs a 4-tier threat level system (Minimal, Potential, Credible, and WMD Incidents) as a basis for initiating precautionary actions when a WMD/terrorist event is anticipated or underway. The FBI will be represented in the state EOC for liaison and to coordinate response needs. The FBI will not initiate on-site response actions without coordinating with local authorities in their initial response, rescue and recovery efforts.
3. The USEPA is responsible for the decontamination of facilities that have been targeted in, or affected by, WMD incidents.
4. Public Information Support - Primary response agencies have a responsibility to furnish the public with applicable information and educational services. A Joint Information Center (JIC) will be established to address public information issues. Ohio Homeland Security and Ohio State Highway Patrol Public Information Officers will assume lead agency responsibilities for information liaison.

C. State Actions

1. The Strategic Analysis Information Center will operate 24 hours per day, 7 days per week as necessary.

IV. CONCEPT OF OPERATIONS

A. Initiating Events

1. Situation 1 - A major act of terrorism has occurred outside the state of Ohio and its neighboring states and has the potential to affect or involve the state.
 - a. Upon the receipt of federal, or other secure, credible source, advisories or notifications regarding such events, the state of Ohio will activate the SAIC. SAIC personnel will gain situational awareness through classified and other sources and brief the State Homeland Security Advisor.

- b. If the incident necessitates activation of the EOC, Ohio EMA will, through the Ohio EOC:
 - i. Notify state agencies with relationships to local first response organizations. These may include, but are not limited to, the OSHP, the Contact Information management System (CIMS), ODH, ODA, EPA, EMS, or others as determined by the Executive Director of Ohio EMA.
 - ii. Partially activate the state EOC (assessment, executive rooms) to:
 - a) Assess the potential effect of a similar event upon the state of Ohio.
 - b) Determine EMAC-related assistance actions (or Ohio's needs).
 - c) Inform (and/or share information with) key state and local government officials regarding the situation. Compile information regarding state and local preparedness status or needs.
 - d) Conduct briefings.
 - e) Issue alerts, notifications, and advisories consistent with federal levels or formats.
- 2. Situation 2 - A major act of terrorism has occurred, or is underway, in a neighboring state which, although outside the state of Ohio, has the potential to threaten, or affect the state.
 - a. The state EOC will be activated to enable representatives from key state agencies to coordinate information with lead federal and local agencies or supporting state agencies as dictated by the situation. At a minimum, the team shall consist of:
 - i. Ohio Homeland Security
 - ii. Ohio State Highway Patrol.
 - iii. Adjutant General's Department.
 - iv. Ohio Department of Natural Resources.
 - v. Environmental Protection Agency.
 - vi. Department of Health.
 - vii. Others (ODA, PUCO, DAS, or state/private facilities and associations) as required for technical support.

- viii. In addition to those primary functions and duties cited in “Situation 1”, the state will:
 - a) Effect coordination with the FBI and/or other federal agencies and offices for technical support and advisory assistance as dictated by the situation.
 - b) Initiate coordination actions with local governments (via EOCs) in Ohio jurisdictions closest to an out-of-state affected area or areas.
 - c) Prepare appropriate action steps for potentially affected areas based on assessments of health and environmental needs for those areas (including epidemiological investigations).
 - d) Provide laboratory support when the FERN or NAHLN systems are activated.

- 3. Situation 3 – A major act of terrorism has occurred in the state of Ohio. In addition to the actions cited in “Situations 1 and 2”, above, the state of Ohio will:
 - a. Fully activate the state EOC and the SAIC.
 - b. Initiate assistance or submit support requests in accordance with EMAC or IMAC considerations (Ref: ESF 7, Resource Support, State of Ohio EOP).
 - c. Working in accordance with ICS/UCS concepts, the Lead Agencies will:
 - i. Employ EOC/Joint Dispatch Facility assets to furnish administrative, warning, and communications support for participating agencies.
 - ii. Coordinate with the lead federal agency and involved local entities to determine needs or resolve issues with regard to:
 - a) Additional threat assessments or event verification functions to include intelligence and information sharing actions applicable to the situation and follow-on support efforts (including modifications of response protocols, by agency, as necessary).
 - b) Inter-agency support actions relating to traffic control, site/perimeter security, crime scene investigations, victim ID, or others as determined by the situation.
 - c) Coordination with federal agencies in designating a Joint Operations Center location and determine required liaison staffing for the JOC as necessary and in consideration of the setting (urban, rural, etc).
 - d) Determine the need for and extent of public protective actions to include site and perimeter control, evacuations, sheltering, congregate care,

prophylaxis, decontamination, or other measures (Ref: ESF-6, Mass Care, State of Ohio EOP).

- e) Support mass care facilities as needed.
- f) Develop, or confirm, rules of engagement, or response, as required by the situation.
- d. Prior to the initiation of field support actions (including activities in privately owned facilities) by state-level support agencies, a declaration of a “State of Emergency” or similar enabling action will be made by the governor.
- e. In all events, an evaluation of the situation will be made with regard to a possible relocation to, and operation of, an alternate EOC to meet the contingencies of the situation and to provide 24 hour continuity for support functions.
 - i. Emphasis will upon communications, accommodations, staffing space, and logistical support features.

B. State-Level Operations

1. The authority for consequence management rests with the state assisted by federal agencies as necessary. It entails multiple agency participation, with the provision of technical advice and/or logistical support for both supporting and supported entities, information and educational continuity, combined asset management programs, and an extended partnership approach to both federal and state supporting efforts for affected areas.
2. The organization for consequence management in the state EOC will be based upon the structure outlined in the State of Ohio EOP.
3. The organization is based upon groupings of assigned primary functions. The specifics of an event may cause various agencies representing critical services, to shift assignments from technical support to primary or lead agency positions (eg: the Department of Agriculture may assume the lead role in an agricultural terror event).
4. The State Coordinating Officer, pre-identified by the Governor, will work with federal offices (FEMA or others as designated) to affect a combined state-federal management effort.
5. Participating agency representatives may need to provide support in locations other than the EOC (DFOs, Recovery Centers or other sites).
6. The consequences (or cascading effects) of terrorism could outlast, or surpass, an initiating event. Effects may include long-term health and medical problems, extended economic issues, or political and social concerns.

7. Military Support

- a. The Ohio National Guard, 52nd WMD-Civil Support Team (WMDCST), will provide technical assistance and advice in support of WMD incidents.
- b. The Ohio National Guard Joint Task Force 73 will provide CBRNE response in the form of search and extraction, decontamination, and limited medical triage/treatment. Additionally, the JTF will provide security forces under the National Guard Response Force (NGRF) and Quick Reactions Force (QRF). The JTF is the standing task force for initial ONG response to Terrorist and CBRNE incidents and can expand to command and control a variety of subordinate units depending on the situation.
- c. Liaison Officers from the Ohio National Guard are provided to Incident Command Posts (ICP), Unified Commands (UC), Area Commands (AC) and joint field offices as required. Due to the expected scope of most Terrorist and/or CBRNE events, the ONG may not be able to provide a LNO to each County EMA in lieu of other critical requirements for liaison.

8. Consequence management will be implemented as follows:

- a. For continuing Credible Threat Advisories/Conditions: Based upon credible threat information, state and federal agencies will advise local governmental agencies regarding additional confirmed threats of terrorism.
 - i. The SAIC will serve as the State's primary fusion center.
- b. Incident/event-related Consequence Management: If a terrorist event occurs, the governor may declare a state of emergency and applicable Consequence Management actions will be implemented:
 - i. Activation of the state EOC (IAW State of Ohio EOP and EOC SOP).
 - ii. Requesting federal assistance in accordance with Federal Response Plan procedures.
 - iii. An OHS representative will be assigned to the JOC, if established, to monitor events and relay decisions affecting Consequence Management actions to the state EOC. Other state agencies can be dispatched to assist in this function. These agencies could include OEMA, ODH, EPA, ODNR, OSHP, or ODA as required.
 - iv. State agencies will coordinate the provision of assistance to affected areas to include basic protective action support (mass care, immunizations, treatments, evacuations, relocations, or sheltering, agriculture). Ref: ESF 6, Mass Care, State of Ohio EOP; ESF-7, Resource Support; ESF 11, Agriculture; and

Threatened Human Biologic Incident: Ohio Guidelines, and State of Ohio Hazardous Materials Emergency Plan, 2001.

- v. Upon proper request, the 52nd WMD-CST will mobilize, deploy to the affected area and establish operations in conjunction with the Incident Commander.
 - c. The 52nd WMD-CST will coordinate with the established incident command to assist in assessments, hazard identification and coordination of follow - on forces as necessary.
9. Public Information Support: OSHP and the OHS PIOs will serve in a lead capacity (with Ohio EMA) for the state. Public information specialists from other lead agencies will serve in this capacity when required by the dictates of the situation.
- a. Duties include:
 - i. The determination of state agency information assistance to include development and response/dissemination methodology and mediums.
 - ii. Defining specific sharing of public information or educational duties.
 - iii. The coordination of specific event-related public information actions by lead and support agencies as required.
 - iv. Monitoring/analysis of media coverage of events and activities as they relate to the situation.
10. Disengagement or Close-Out Actions.
- a. In accordance with Unified or Incident Command System concepts, OSHP, OHS and Ohio EMA will coordinate with lead federal and other state agencies for an appropriate date/time for state Consequence Management disengagement.
 - b. Following disengagement, designated state and local organizations may continue recovery (to include long term hazard monitoring, environmental/personnel decontamination and site restoration) efforts.
 - c. Post event actions will include debriefings, general agency performance reviews and after-action documentation.

V. ASSIGNMENT of RESPONSIBILITIES

For the Capabilities outlined above and presented below, one-or-more of the Primary and Support Agencies indicated below may have a responsibility or responsibilities as indicated, and may carry out the following activities. It is not expected that all agencies that are listed as

either Lead or Support Agencies for a particular capability will have the resources or the expertise to carry out all of the responsibilities for a capability.

- A. For the **Information Gathering and Recognition of Indicators and Warnings** Capability, Lead (OHS-SAIC, OSHP) and Support (ONG, DAS, ODA, OEMA, OEPA, ODH, ODNR, PUCO, ODRC, ODOT) Agencies may:
1. Gather Information that could be used to identify terrorist operations from all sources (law enforcement, public health, agriculture, public works, transportation, firefighting, emergency medical entities and the private sector) through routine activities.
 - a. Gather homeland security information during routine day-to-day activities and pass it to appropriate authorities.
 - b. Identify items and materials used by criminal and/or terrorist organizations to carry out attacks.
 - c. Catalog information provided by all sources and retain in a database to enable timely retrieval.
 - d. Conduct information gathering operations on critical infrastructure and other potentially high-risk locations or assets.
 - e. Coordinate information-gathering activities with relevant local, tribal, State, and Federal entities on an ongoing basis, in particular with the Joint Terrorism Task Force in terrorism-related cases.
 2. Identify suspicious circumstances or indicators and warnings associated with planning, support, and operations, related to potential criminal and/or terrorist-related activities.
 - a. Recognize suspicious activities involving items and materials used by criminal and/or terrorist organizations;
 - b. Recognize and identify suspicious circumstances or indicators and warnings that may be associated with the planning, support, and operations related to potential criminal and/or terrorist-related activities.
 - c. Utilize a predefined notification process to advise law enforcement of suspicious activity.
 - d. Notify law enforcement agencies of potential terrorist activities in/around or related to private sector businesses/operations.
 3. Screen Information by receiving, authenticating, and screening information for relevance, with the appropriate level of oversight/supervision and in a timely manner.

- a. Query databases or records to check for significance of information.
 - b. Maintain and update procedures and/or systems to process the inflow of gathered information from all sources in a timely fashion.
- B. For the **Intelligence Analysis and Production** Capability, Lead (OHS-SAIC, DAS) and Support (OSHP, ONG, AG, ODA, SFM, OEMA, OEPA, ODH, ODMH, ODNR, OEMS, PUCO, ODRC, ODOT, DAS) Agencies may:
- 1. Develop and Maintain Plans, Procedures, Programs, and Systems.
 - a. Ensure that State, local and/or tribal officials with varying levels of clearance have access to useful information.
 - b. Develop means to share local-, regional- and State-level indications and warnings
 - i. Issue SAIC alerts and bulletins
 - c. Develop guidelines for tailoring information according to audience
 - d. Develop plans and procedures for establishing and staffing fusion center
 - i. Activate OHS critical incident procedure
 - 2. Establish and operate a multidisciplinary, all-source information/intelligence fusion center/process that undertakes an “all-hazards” and “all-crimes” approach using the national guidelines and standards.
 - a. Access intelligence and information repositories at all levels of classification as necessary
 - b. Ensure appropriate technological redundancy.
 - c. Establish and maintain communications, including electronic connectivity with other state and regional fusion center/processes.
 - d. When appropriate, relay and/or pass terrorist-related information to the FBI Joint Terrorism Task Force (JTTF) and FBI Field Intelligence Group (FIG).
 - 4. Access Information by obtaining access to and receiving collected information associated with the respective territory of the fusion center.
 - a. Receive, extract, or collect information from all available sources, including all relevant databases and systems available to the State fusion center, on a continuous basis and with appropriate technological redundancy.

- b. Ensure that unclassified briefings, reports and alerts are used whenever possible to provide credible information that allows public safety, private sector and non-law enforcement agencies to develop intelligence- and information-driven prevention plans without compromising source or collection methods.
 - c. Employ classified briefings and reports to brief appropriately cleared partners.
 - 5. Develop Analytic Products that support the development of risk-based prevention, protection, and response programs at all levels.
 - a. Provide briefings, reports and/or alerts tailored to recipients with detailed, specific information on actions or activities that may be indicative of an emerging threat.
 - b. Analyze information needs on a continuous basis regarding short- and long-term intelligence requirements.
 - c. Archive information and intelligence in a searchable repository to support future efforts by all fusion analysts.
- C. For the **Epidemiological Surveillance and Investigation** Capability, Lead (ODH (human), ODA (animal)) and Support (OHS, DAS, OSHP, ODA, ODH, OEMS) Agencies may:
 - 1. Develop and Maintain Plans, Procedures, Programs, and Systems.
 - a. Effectively identify and respond to potential disease outbreaks, vectors and epidemics of humans or animals.
 - b. Effectively and properly conduct coordinated outbreak investigations.
 - c. Develop and maintain efficient surveillance systems supported by information systems that comply with PHIN functional requirements for Early Event Detection, Outbreak Management and Countermeasure and Response Administration to facilitate early detection, mitigation and evaluation of expected and unexpected public health conditions.
 - d. Distinguish on the State list of notifiable conditions between select conditions that require immediate reporting to the public health agency (at a minimum, Cat A agents), and conditions for which a delay in reporting is acceptable. Dangerously Contagious or Infectious Diseases of animals are reportable to the Ohio Department of Agriculture and must be reported when a case is suspected.
 - e. Effectively and appropriately respond notifications of medical hazards.

- f. Describe time frames for notification for conditions where a delay in reporting is acceptable.
 - g. Effectively support and/or provide human and veterinary medical personnel, equipment, laboratories, and pharmaceuticals and supplies in response to disease outbreaks.
 - h. Plan and prepare for pandemic influenza, particularly for the stage when vaccine either is nonexistent or in severely short supply.
 - i. Effectively inventory medical supplies, equipment, ambulance services, hospitals, clinics and first aid units.
 - j. Maintain the network of veterinary, agricultural, and public health laboratories that will be able to effectively respond to bioterrorism incidents.
2. Develop and Maintain Training and Exercise Programs.
- a. Develop and implement training and exercises for epidemiological surveillance and investigation.
 - b. Support training on various types and models of equipment likely to be used in an emergency situation through government grants and industry sponsored workshops.
3. Direct Epidemiological Surveillance and Investigation Operations.
- a. Maintain public and animal health communication channels supported by information systems that comply with the PHIIN functional requirements for Partner Communications and Alerting, and the FERN and NAHLN systems.
 - b. Provide public health and agricultural information to the Joint Information Center for release.
 - c. Lead public health investigations to determine, in collaboration with law enforcement, disease source(s).
 - e. Report instances of disease that raise the index of suspicion of terrorist or criminal involvement to FBI Headquarters.
 - h. Make public health recommendations for prophylaxis and other interventions.
 - i. Coordinate examination of suspect deceased suspect patients with the local medical examiners and/or coroners.

4. Engage in Surveillance and Detection Operations.
 - a. Compile and analyze surveillance data.
 - b. Detect suspected outbreak(s) through pattern recognition.
 - c. Maintain chain of custody of evidentiary materials.
5. Conduct Epidemiological Investigations.
 - a. Dispatch public health or agriculture personnel to location of suspected contamination/outbreak.
 - b. Conduct epidemiological investigations to identify potential exposures and diseases.
 - c. Confirm human, animal, plant or food disease outbreaks using lab data and disease tracking data.
 - d. Create registries of ill, exposed, and potentially exposed persons.
 - e. Analyze and interpret epidemiological investigation data in coordination with data from Counter-Terror Investigation and Law Enforcement sources.
 - f. Analyze, confirm and recommend control measures for disease outbreaks.
 - g. Draft and disseminate reports on epidemiological investigations.
 - h. Have or have access to information systems to support the investigation, description and understanding of events of public health significance.
6. Monitor Containment.
 - a. Monitor the course and population characteristics of a recognized outbreak.
 - b. Have or have access to information systems that support administration of outbreak control.
 - c. Monitor effectiveness of disease outbreak mitigation steps.

D. For the **Counter-Terror Investigation and Law Enforcement** Capability, Lead (OSHP, ODNR, ODRC, SFM) and Support (OHS, ONG, AG, OEPA, ODH, ODA) Agencies may:

1. Conduct Investigations.
 - a. Recognize terrorism indications and warnings that arise during the course of investigations.

- b. Conduct targeted outreach with private businesses related to an investigation.
 - c. Engage in effective source development activities, including maintaining source confidentiality.
 - d. Maintain ability to address CBRNE hazards that may be encountered during the course of an investigation.
 - e. Gather, catalogue, and preserve evidence for prosecutorial purposes and attribution.
 - f. Coordinate with officials from critical infrastructure, key resources, and the private-sector to facilitate investigations.
 - g. Recognize indicators and warnings of potential terrorist-related activity during criminal investigations.
2. Share Information Related to Investigations.
- a. Identify and maintain liaisons with appropriate lead Federal terrorism investigation entities (JTTF).
 - b. Conduct targeted outreach with private businesses, industries, and facilities to assist an investigation.
 - c. Conduct targeted outreach with Federal, State, local, and tribal governments to assist in investigations.
 - d. Contact JTTF in a timely fashion when any nexus to terrorism is discovered.
 - e. Share investigation-related information across jurisdictions and among law enforcement and other agencies as appropriate.
 - f. Deliver investigation-related information through pre-established channels appropriate for the originating source.
 - g. Provide investigators with timely threat and intelligence information.
3. Deploy Specially-Trained Personnel.
- a. Maintain access to special operations teams.
 - b. Maintain access to personnel with specialized skills (foreign language fluency).
 - c. Translate documents and discourse and conduct interviews in languages other than English when appropriate.

E. For the **Food and Agriculture Safety and Defense** Capability, Lead (ODA, ODH, ODNR) and Support (OHS, OSHP, DAS, OEMA, OEPA) Agencies may:

1. Develop and Maintain Plans, Procedures, Programs, and Systems.
 - a. Conduct vulnerability assessments of sector-specific critical infrastructure and key resources.
 - b. Develop methods for emergency assessment of firms that manufacture, prepare, and hold U.S. Department of Agriculture and/or U.S. Food and Drug Administration-regulated commodities.
 - d. Create emergency response plans for response to all food operations for retail, food service, and food processing facilities.
 - e. Develop emergency guidelines and operation criteria for retail food, wholesale, and processing during disasters.
 - f. Develop communications plan for food safety for regulated facilities and the general public.
 - g. Develop guidelines or procedures for properly conducting coordinated outbreak investigations of food and agricultural events.
 - h. Develop plans for properly disposing of contaminated food products, diseased crops, diseased livestock or their products.
 - i. Develop plans to support incident command (IC), unified command (UC), or other agencies as needed for food and agricultural safety response.
 - j. Develop plans, procedures, and programs for responding to food safety and agricultural disease events.
 - k. Prepare food and agriculture emergency public information plans.
 - l. Develop food and agriculture incident communications plans.
 - m. Develop plans for responder safety and health.
 - n. Develop plans, procedures, and policies for coordinating, managing, and disseminating public information regarding food and agricultural safety.
 - o. Develop a communications network with State homeland security departments.
2. Develop and Maintain Training and Exercise Programs.

- a. Develop and conduct emergency food safety response training to field staff and managers of State/local food programs having responsibility for food safety response (training should include appropriate job safety training)
 - b. Provide food safety training to responders and volunteers
 - c. Develop and implement exercise programs for food and agricultural safety and defense
3. Direct Food and Agriculture Safety and Defense Operations
- a. Dispatch food and agriculture personnel to locations of suspected contamination and request food and agriculture resources needed for response to field operations.
 - b. Coordinate with Federal, State, and local agencies to ensure the safety and security of all food products in retail food establishments, food service operations and institutions.
 - c. Establish and maintain food and agricultural safety response communication systems and coordinate the provision of timely and accurate emergency public information through the Joint Information System (JIS).
 - d. Provide direction, information, and support as appropriate to Incident Commands, Unified Commands and joint field offices.
 - e. Coordinate food and agricultural safety response operations and support, and food and agriculture investigation activities.
 - f. Coordinate food and agriculture evidence preservation procedures.
 - g. Coordinate food recovery programs.
 - h. Coordinate food facility cleaning and decontamination and coordinate the disposal of contaminated food.
 - i. Coordinate agricultural recovery programs.
 - j. Ensure that the State's commercial supply of food is safe and secure following a catastrophic incident.
 - k. Develop and implement guidelines for properly conducting a coordinated outbreak investigation of food and agricultural events.
 - l. Direct agricultural processes for surveillance and testing and isolation or quarantine for threats to agricultural assets and the food supply.

- m. Provide animal, plant and food safety laboratory and diagnostic support, subject matter expertise, and technical assistance.
 - n. Establish State-level plans and protocols for food and agricultural safety response and requests for assistance.
4. Conduct Surveillance.
- a. Conduct epidemiological investigations as surveillance reports warrant, and coordinate Federal, State, and local veterinary assistance assets/services.
 - b. Search actively for possible food and agriculture contamination, plant disease or animal disease cases and use the results from sample analyses to determine the breadth of contamination.
 - c. Conduct animal, plant and food safety laboratory detection screening and confirmation.
 - d. Disseminate animal, plant and food safety laboratory testing results to appropriate stakeholders/partners.
 - e. Maintain chain-of-custody of all animal, plant and food safety evidence and integrate surveillance findings related to food and agriculture.
5. Trace Suspect Products or Animals.
- a. Collect and preserve contaminated and non-contaminated food and agriculture evidence.
 - b. Develop standard operating procedures for evidence collection in the face of highly contagious animal disease outbreak.
 - b. Inspect the safety and security of the food and agricultural infrastructure in the affected area.
 - c. Inspect and monitor all food facilities in affected areas.
 - d. Use laboratory testing and field investigations to identify products that are safe and fit for human consumption.
 - e. Conduct product tracing to determine the source, destination, and disposition of adulterated, contaminated or diseased products, plants, or animals.
 - f. Generate possible associations of transmission, exposure, and source of animal disease, plant disease, and food safety incidents, and agriculture events.

- g. Identify populations and locations at risk from animal disease, plant disease or food safety incident.
6. Develop and implement Control Measures for Contaminated Food Products, Diseased Crops or Diseased Animals.
 - a. Secure the contamination source and affected areas during food and agriculture incidents.
 - b. Provide appropriate information to the public regarding disposal of potentially contaminated food.
 - c. Determine the need for embargos, detention, condemnation, retention, seizure of food, plant or animal product embargos, animal quarantine, and food, plant or animal movement stoppage.
 - d. Control all identified food products at establishments that are suspected of being contaminated through product recall, administrative detention, and plant closures.
 - e. Stop all interstate movement of regulated plant articles and means of conveyance as needed.
 7. Conduct Product Disposal and Surface and Food Facility Decontamination.
 - a. Identify assets for food and agriculture decontamination activities.
 - b. Develop and implement food and agriculture hazardous material disposal plans.
 - c. Conduct animal, plant, and food facility decontamination.
 - e. Dispose of contaminated or diseased food, plants or animals.
- F. For the **Laboratory Testing** Capability, Lead (ODA, OEPA, ODH, ONG) and Support (OHS, OEMA, ODNR, ODOT) Agencies may:
1. Develop and Maintain Plans, Procedures, Programs, and Systems.
 - a. Establish and maintain collaborative linkages with other State laboratories, e.g., environmental, agriculture, veterinary, and university, as well as the jurisdiction's National Guard Civil Support Team (CST) and other first responders.
 - b. Establish and maintain linkages with Federal laboratory networks and member laboratories within the jurisdiction, e.g., the Food Emergency Response Network (FERN), National Animal Health Laboratory Network (NAHLN), and the EPA.

- c. Establish and utilize a State and local health alert network that complies with the PHIN Functional Area Partner Communication and Alerting for electronic connectivity with all LRN Sentinel laboratories.
 - d. Establish and maintain connectivity with the State Emergency Operations Center (SEOC) and other official components of the State and local emergency response, including the Emergency Management Assistance Compact.
 - e. Establish and maintain communication linkages with local, State, and Federal (e.g., CDC DEOC and LRN) public safety and law enforcement entities, e.g., police, fire, emergency management, and the FBI.
2. Develop and Maintain Training and Exercise Programs.
 - a. Provide information and training on the use of appropriate safety and security equipment and procedures.
 - b. Coordinate response planning, drills and exercises for laboratories with all relevant partners.
3. Direct Laboratory Testing.
 - a. Work in close partnership with local public health epidemiology, animal health and environmental health entities, and poison control to provide timely data to assure implementation of effective prevention, detection, and control measures, including treatment.
4. Sample and Specimen Management.
 - a. Establish and maintain jurisdiction-wide transport systems to assure timely receipt of samples or specimens for laboratory testing.
 - b. Perform triage screening on environmental samples.
 - c. Communicate requirements for all-hazard specimen or sample collection, packaging, and shipping to submitters (FBI, CST, first responders, HazMat Teams, and LRN Sentinel and Clinical Chemistry Laboratories).
 - d. Provide consultation to all submitters regarding appropriate collection and shipment of specimens or samples for testing.
5. Provide Surveillance Support.
 - a. Acquire and provide timely results of submitted infectious biological samples.

- b. Provide reference analysis and identification of unusual or emerging biological agents present in communities.
 - c. Perform 24/7/365 Bio-Watch analyses.
6. Detection Testing and Analysis.
- a. Evaluate clinical specimens from patients exposed to chemical or radiochemical agents (tests for blood gases, CBC analysis, and enzyme levels).
 - b. Test initial 20-40 clinical specimens to assess human exposure by measuring metabolites of chemical agents (nerve agents).
 - c. Test environmental samples for toxic industrial chemicals and materials.
 - d. Identify all human and animal origin emerging infectious agents or possible bioterrorism agents using available protocols.
7. Confirm Testing.
- a. Confirm results using LRN, NAHLN or FERN detection methods.
 - b. Use standardized protocols to detect emerging infectious agents or possible bioterrorism agents in human clinical specimens (LRN), food (FERN), animal (NAHLN) or environmental samples.
 - c. Verify reactive Bio-Watch samples.
8. Support Epidemiological Investigations.
- a. Work in close partnership with public health epidemiology, animal health, environmental health, and poison control to provide timely data to assure implementation of effective prevention, detection, and control measures, including treatment.
 - b. Collaborate with law enforcement and perform testing of evidentiary samples.
 - c. Coordinate testing of environmental samples for assessment and remediation.
 - d. Determine whether an emerging infectious disease agent or a biological threat agent consists of single or multiple strains.
9. Report Results.
- a. Report surveillance results suggestive of an outbreak immediately to public health or agriculture officials. .

- b. Report confirmed laboratory results to all submitters in a timely manner.
 - c. Contact the nearest Federal Reference laboratory when unable to identify or rule-out emerging infectious agents or possible bioterrorism agents.
 - d. Notify appropriate public health, agriculture, public safety, and law enforcement officials immediately (24/7) of presumptive and confirmed laboratory results of a chemical and biological threat agent.
- G. For the **CBRNE Detection** Capability, Lead (OHS, OSHP, ONG, ODA, SFM, OEPA, ODH) and Support (AG, DAS, OEMA, ODNR, PUCO, ODRC) Agencies may:
- 1. Develop and Maintain Plans, Procedures, Programs, and Systems.
 - a. Maintain plans and processes for CBRNE detection and communication operations.
 - b. Maintain policies and protocols for determining appropriate locations for detection operations (“interdiction points”) for each CBRNE agent.
 - c. Maintain processes to identify, acquire, and integrate appropriate detection technology in operational environments for each CBRNE agent.
 - d. Implement equipment acquisition and certification standards for each CBRNE agent.
 - e. Maintain policies and agreements to enhance and maintain adequate resources and technologies for detection operations for each CBRNE agent.
 - f. Maintain coordination and/or mutual aid agreements with external CBRNE detection and alarm resolution capabilities.
 - g. Maintain protocols to ensure that technical support is available during detection operations for each CBRNE agent.
 - h. Acquire and allocate resources to address identified financial gaps in detection for each CBRNE agent.
 - i. Maintain processes for obtaining data regarding evolving CBRNE threats in coordination with the Information Sharing and Dissemination Capability.
 - j. Maintain an interoperable information network for detection of each CBRNE agent.
 - k. Maintain a program to conduct detection of each CBRNE agent at critical infrastructure/key resources (CI/KR) in coordination with the Critical Infrastructure Protection Capability.

1. Prioritize and allocate CBRNE detection resources to CI/KR in coordination with Critical Infrastructure Protection capability.
 - m. Deploy fixed and mobile detection resources to CI/KR for each CBRNE agent.
2. Develop and Maintain Training and Exercise Programs.
 - a. Develop and maintain training programs to support CBRNE detection and communication operations and identify personnel for CBRNE detection training.
 - b. Develop and implement training to enable personnel (first responders, law enforcement, intelligence, and medical community) to recognize the presence of CBRNE material.
 - c. Establish key personnel training standards for CBRNE detection.
3. Detect CBRNE.
 - a. Conduct CBRNE detection operations in communities for illegal manufacture and/or use.
 - b. Detect the use of CBRNE material in a community and/or venue.
 - c. Detect illegal manufacturing of CBRNE material at potential manufacturing sites.
 - d. Conduct CBRNE detection operations at key transportation points and detect CBRNE material on people or items entering/boarding events, aircraft, mass transit, or other high impact targets.
 - e. Inspect and monitor cargo at key interdiction points for potential CBRNE material.
 - f. Identify potential CBRNE material at key interdiction points requiring further inspection.
 - g. Use intelligence information to focus CBRNE material searches and surveillance activities and to target suspect containers or shipments.
 - h. Detect the theft or diversion of CBRNE materials.
 - i. Coordinate with Animal Health and Epidemiological Surveillance to focus CBRNE detection on public health and medical information (syndromic surveillance and medical diagnostic tests).
4. Identify and/or Characterize CBRNE material.
 - a. Conduct screenings to confirm the presence of CBRNE materials.

- b. Provide CBRNE samples to relevant entities (public health or animal health laboratories, law enforcement, forensic laboratories, etc.) for additional assessments, as necessary.
- c. Conduct appropriate tests and assessments to characterize and identify detected CBRNE material.
- d. Determine whether detected CBRNE material is a threat.
- e. Gather CBRNE material detection information that can be used in attribution efforts to appropriate personnel, including law enforcement and intelligence community personnel.

5. Communicate CBRNE Detection Incidents.

- a. Coordinate CBRNE material threat and discovery information with intelligence, public safety, public health and other appropriate agencies.
- b. Notify appropriate personnel (intelligence community, law enforcement personnel, first responders, and the general public) of CBRNE detection data and results.
- c. Communicate data and observations using appropriate formats and standards.

H. For the **Explosive Device Response Operations** Capability, Lead (OHS, OSHP, ONG, SFM, ODRC) and Support (AG, DAS, OEPA, ODH) Agencies may:

1. Respond to explosive device incidents by:

- a. Implementing National Guidelines for Bomb Technicians.
- b. Implementing procedures and programs including standardized training and exercises to counter terrorist events, employing weapons of mass destruction (WMD), suicide bombers, Vehicle Borne Improvised Explosive Devices (VBIED), and Radio Controlled Improvised Explosive Devices (RCIED).
- c. Implementing plans that coordinate explosive device response in multi-jurisdictional areas which protect critical infrastructure and key resources from terrorist threats.
- d. Implementing programs to share explosive device response information, effective practices, and lessons learned.
- e. Assisting public safety bomb squads and teams in achieving increased capability to counter terrorist events.

- I. For the **WMD and Hazardous Materials Response and Decontamination** Capability, Lead (OSHP, ONG, ODA, SFM, OEPA, ODH, ODRC) and Support (OHS, AG, OEPA, OEMS) Agencies may:
 1. Direct WMD and Hazardous Material Response and Decontamination Tactical Operations.
 - a. Establish and implement on-scene management for hazmat material responses.
 - b. Coordinate with and provide technical guidance to entities performing decontamination operations.
 - c. Coordinate with hospitals to develop plans for managing/decontaminating self-presenting contaminated victims.
 - d. Coordinate resource management of hazmat equipment, supplies, and personnel.
 - e. Issue guidance for self-decontamination, where appropriate, expedient and possible.
 2. Assess Hazard and Evaluate Risk.
 - a. Collect, prioritize and manage data and information from all sources.
 - b. Use plume dispersion models and other analytical tools to generate ongoing WMD/hazmat dispersion assessments.
 - c. Develop and implement an Incident Action Plan (IAP) specific to WMD/hazmat issues based upon the risk evaluation process.
 3. Conduct Mitigation Activities.
 - a. Identify appropriate PPE based on suspected hazardous material.
 - b. Coordinate with safety officer to monitor responders for exposure to hazmat.
 4. Conduct Decontamination and Clean-up /Recovery Operations.
 - a. Identify assets required for decontamination activities.
 - b. Identify the type of contaminants, nature of response operations, and the required type/level of decontamination operations.
 - c. Develop and implement plans, procedures, and protocols to ensure on-site individual gross decontamination of persons and household pets affected by the incident.

- d. Provide a means to allow medical treatment facilities and shelter managers to readily identify people who have received gross decontamination.
5. Demobilize WMD and Hazmat Response and Decontamination.
- a. Work with Incident Command(s) and Unified Command(s) to ensure that incident-specific evidence collection and investigation protocols are clearly understood and communicated to all responders.
- J. For the **Intelligence and Information Sharing and Dissemination** Capability, Lead (OHS, OEMA) and Support (OSHP, ONG, AG, ODA, OEPA, ODH, DAS-OIT, PUCO) Agencies may:
- 1. Implement Plans, Procedures, Programs, and Systems.
 - a. Identify appropriate law enforcement and other enforcement governmental personnel for receipt of security clearances at an appropriate level to ensure effective dissemination of critical information.
 - b. Implement processes for preventing, reporting, and addressing the inappropriate disclosure of information and/or intelligence.
 - c. Implement mechanisms/processes for sharing information/intelligence between Federal and State sources.
 - d. Implement alternative, supplemental, and back-up mechanisms for routing information and/or intelligence to appropriate agencies as necessary.
 - 2. Incorporate All Stakeholders in Information Flow.
 - a. Share information and/or intelligence between Federal, State and local levels.
 - b. Prevent, report, and/or address inappropriate disclosures of information and/or intelligence.
 - 3. Information Flow.
 - a. Activate computers in the Secure room and start gathering additional information that would assist with the production and release of information and intelligence for use in the decision making process in the EOC and to all our federal and state and local partners through bulletins and postings to insure the timely and accurate sharing of information
 - b. Share intelligence and information systematically between Federal, State, local, and regional entities.

- c. Disseminate relevant intelligence and/or information from Federal or State entities to local authorities.
 - c. Disseminate relevant information and/or intelligence products to street-level law enforcement personnel.
 - d. Provide relevant intelligence and/or information from local authorities to Federal or State entities in a usable format and in a timely manner.
 - e. Infrastructure Protection staff will maintain a presence at the SAIC with access to the Automated Critical Asset Management System (ACAMS), to provide a comprehensive and consistent integrated inventory of a targeted asset and an assessment of assets located within a specified radius of the damaged or destroyed affected asset.
4. Horizontal Information Flow.
- a. Coordinate information flow across jurisdictions among law enforcement and other appropriate agencies at all levels through effective and timely information sharing.
 - c. Structure dissemination and information sharing mechanisms so that private-sector entities receive accurate, timely, and unclassified information.
- K. For the **Critical Infrastructure Protection** Capability, Lead (OHS, OSHP, ONG, DAS, ODA, SFM, ODNR, ODRC) and Support (AG, OEMA, OEPA, ODH, ODOT) Agencies may:
1. Implement Plans, Procedures, Programs, and Systems.
 - a. Implement risk assessment tools.
 - b. Implement strategies and guidelines for cyber infrastructure protection.
 - c. Implement strategies and guidelines for protection of infrastructure personnel.
 - d. Implement databases of infrastructure assets, systems, networks, and functions.
 - e. Implement sector-specific metrics to measure progress and to assess effectiveness of the sector-specific CI/KR protection programs.
 2. Identify CI/KR.
 - a. Implement selection criteria to identify CI/KR.
 - b. Identify CI/KR within the State.

3. Assess Risks.

- a. Conduct consequence analyses to determine which assets, systems, networks, and functions are high consequence and therefore require risk assessment.
- b. Conduct vulnerability assessments on high-consequence assets, systems, networks, and functions.
- c. Conduct detailed threat assessments on high-consequence assets, systems, networks, and functions.
- d. Determine risk profiles of high-consequence assets, systems, networks, and functions.
- e. Share the assessment of sector-specific infrastructure risk with interdependent entities within appropriate sectors.
- f. Prioritize high-risk CI/KR for consideration of protective measures

6. Protect Assets

- a. Implement surge capacity measures to increase CIP during a terrorism incident.
- b. Implement protective programs and plans to reduce the general level of risk for the highest risk CI/KR.
- c. Implement protective programs and plans to respond to and recover from specific threat-initiated actions.
- d. Implement programs to defend critical cyber assets, systems, networks, and functions.
- e. Implement detection measures such as inspection surveillance, employee monitoring, and security counterintelligence.