

Domestic Preparedness Checklist

Review State Plans, Laws, and Capabilities

- √ Review the state's emergency plan and make needed changes to correct any procedural problems encountered on September 11.
- √ Identify what intelligence information is needed at the state level, who can receive it, and assess security clearances with the Department of Defense and the FBI. Ensure Governor has viable statutory mechanisms in place to share intelligence information between state and local agencies and consider mandating a formal communication network between the intelligence community and medical community.
- √ Examine state laws and authorities that relate to search and seizure, invasion of privacy, quarantine, evacuation, relocation or restricting access and consider enacting new health emergency powers act if necessary. (See Model State Emergency Health Powers Act.)
- √ Understand what the authorities and prohibitions are to using military assets in the state.
- √ Review current state laws dealing with record checks, background checks, and access to public records to ensure they do not interfere with security. Consider whether legislation changes in the state's open records law are necessary to ensure the protection of sensitive documents; review information posted on websites concerning sensitive information and critical infrastructure protection.
- √ Review, update, and strengthen security procedures at potential terrorist targets in state including state capitol and state buildings.
- √ Review and update plan for continuity of government operations during emergencies.
- √ Review and update state evacuation plans.
- √ Develop an effective strategy for communicating the potential terrorism threat to the public and the media.
- √ Create a counterterrorism task force to identify shortfalls in legal authorities, programmatic authorities, and funding issues. Counterterrorism task forces should include Chief Information Officers and local capabilities, especially the EMTs, fire and rescue, public health and medical, public utilities, and disaster preparedness personnel whose responsibility it would be to respond to terrorist events.
- √ Take advantage of the Emergency Management Assistance Compact (EMAC). EMAC is an interstate mutual aid agreement that allows states to assist one another in responding to all kinds of natural and man-made disasters. EMAC offers a quick and easy way for states to send personnel and equipment to help disaster relief efforts in other states. A system like this enables experts to be used across jurisdictions and regions based on the nature of a particular event. There are 42 states and two territories that are members of EMAC and other states and territories are considering joining.

- √ Submit State Needs Assessments to Department of Justice. Over the last several years the Department of Justice has provided state and local jurisdictions with funds to assist in purchasing the specialized equipment required to respond to terrorist incidents effectively and safely. Currently, under congressional direction, the states, in order to receive these funds, are required to complete a state-wide threat and needs assessment and to provide the department a three-year comprehensive strategy addressing how these funds, and other department assistance, would be allocated within the state. To date only nine states have submitted plans. Attorney General Ashcroft has asked that all state needs assessments and state-wide strategic plans be submitted as soon as possible, and no later than December 15, 2001.

Bioterrorism Preparedness

Review the attached Model Public Health Act and consider implementing the following:

- √ Assess and strengthen hospitals surge capability. The emergency management, medical, and public health professions should work on all levels to ensure that each region in the country has a certain minimum surge capacity to deal with mass casualty events.
- √ Consider developing mutual aid agreements across multiple jurisdictions and consider developing a regional bioterrorism response capability.
- √ Ensure procedures are in place to access National Pharmaceutical Stockpile including how to formally request resources and how local governments will receive it.
- √ Ensure that the appropriate local first responders are up to date on nerve agents and bioweapons programs, including the delivery systems used for bioweapons.
- √ Identify existing assets and needs concerning stockpiling of drugs, equipment and supplies, and training.
- √ Public health laboratories must have the capacity to rapidly and accurately analyze and identify samples submitted for analysis. This capacity is key to identifying and responding to biological and chemical threats.
- √ Create secure and accessible information systems. Effective, secure, rapid communication among federal, state, and local health agencies, including high-speed Internet access, satellite distance-learning capability, and videoconferencing, is critical to coordinated response to emergencies, including the handling of vital records.

Agroterrorism

Farms and the food supply remain among the nation's most exposed targets. Fertilizers can be used to produce powerful bombs, pesticides can become chemical weapons, and small amounts of deadly bacteria can taint the food supply for thousands of people. Agricultural terrorism awareness needs to be heightened by states and the federal government.

- √ Farmers should take precautions to prevent against possible contamination of plants, livestock, or tampering with farm products and also should secure chemicals such as ammonium nitrate and urea that could be used to make bombs.
- √ Pesticide dealers should tighten security.

- √ Farmers and commercial pesticide dealers should be required to report all thefts of chemicals and pesticides to law enforcement.

Cyberterrorism

- √ Ensure that by December 2001 your state has applied for a license to use the 2.4 megahertz of public safety 700 MHz that the Federal Communications Commission (FCC) has designated for state use. Under this state license approach, states will have the ability to communicate across jurisdictions and with each other during an emergency or disaster. It will allow states to apply their unique expertise and knowledge to best use the radio spectrum to meet the public safety needs of their citizens. The state license application, FCC form 601 is available on the FCC website (www.fcc.gov) or by calling the FCC's distribution center at 1-800-418-3676.
- √ Ensure the development and maintenance of an information technology enterprise (inter-agency) security oversight plan. This plan should include:
 1. emphasis on awareness of vulnerabilities and threats to information technology systems;
 2. development of teams (consider using Y2K teams) to deal with cyber terrorism;
 3. a security assessment of all hardware, software, and networks including state-owned and operated, leased, or contracted;
 4. review of Y2K preparations and revamp to protect the states' critical infrastructures;
 5. contingency plans for government continuity and essential services when systems are down;
 6. the ability to aggregate security threats from all information systems, and nationwide data sharing on security threats that will allow for trend analysis; and
 7. a statewide interoperable communications system and emergency response call center.
- √ Rely on and include state and local chief information officers on the state's counterterrorism task force to help identify threats and solutions for preventing attacks and improving security.