

## States' Homeland Security Priorities

### Summary

The September 11 terrorist attacks against the World Trade Center and the Pentagon quickly propelled terrorism to the top of the nation's agenda. Even before the events of September 11, governors had identified terrorism as a real domestic security concern and, since 1996, the issue has been part of the National Governors Association efforts in emergency preparedness. However, the magnitude and nature of the September 11 terrorist attacks, anthrax crisis, and national alerts have led Governors to initiate unprecedented efforts to implement a comprehensive state-based strategy to prepare for, prevent, respond to, and recover from terrorist attacks within their borders.

Homeland Security is a complex challenge that demands significant investment and collaboration among local, state, and federal governments and integration with the private sector. Over the last several months, the NGA Center has worked with state homeland security directors and analyzed the states and territories' written responses to the Office of Homeland Security's request for state input into the national strategy. The major priorities and issues identified by the state and territorial officials are:

- coordination must involve all levels of government;
- the federal government must disseminate timely intelligence information to the states;
- states must work with local governments to develop interoperable communications between first responders and adequate wireless spectrum must be set aside to do the job;
- state and local governments need help and technical assistance to identify and protect critical infrastructure;
- both the states and federal government must focus on enhancing bioterrorism preparedness and re-building the nation's public health system to address 21<sup>st</sup> century threats;
- the federal government should provide adequate federal funding and support to ensure that homeland security needs are met.
- the federal government should work with states to protect sensitive security information, including restricting access to information available through "freedom of information" requests;
- an effective system must be developed that secures points of entry at borders, airports, and seaports without placing an undue burden on commerce;
- the National Guard has proven itself to be an effective force during emergencies and crises. The mission of the National Guard should remain flexible, and Guard units should primarily remain under the control of the governor during times of crises; and
- federal agencies should integrate their command systems into existing state and local incident command systems (ICS) rather than requiring state and local agencies to adapt to federal command systems.

### Coordinating Efforts by All Levels of Government

As we move forward to develop a national strategy for homeland security and to implement new emergency preparedness plans at the federal, state, and local levels, coordination among levels of government will be essential. Coordination ensures that all entities within a state are working toward the same goals. To accomplish this, all federal resources, programs, and activities involving state and local governments must be coordinated through the nation's governors and their appropriate state

agencies. This will ensure a comprehensive statewide domestic preparedness strategy that reflects the unique characteristics and needs of each state. Programs and funding that bypass the states ensure gaps in coverage, incompatible local systems, and wasteful duplication of effort. A comprehensive state terrorism strategy, or plan, is the best and most appropriate framework for the delivery of federal programs and funding.

### **Receiving and Disseminating Timely Intelligence Information**

A state's homeland security advisory system can only be as effective as the intelligence it receives. The federal government collects, creates, manages, and protects information necessary for national security purposes. As such, the states rely on the federal government to share actionable information and intelligence it receives to prepare for terrorist attacks. States believe that the Office of Homeland Security should be a central repository and clearinghouse to provide state and local agencies with counterterrorism-related information and intelligence and to assist states in their efforts to distribute information tailored to communities.

Governors and other high-ranking state officials must receive timely and critical intelligence information related to terrorist threats. Granting security clearances to certain state and local personnel using a compartmented, need-to-know system would facilitate secure sharing of critical intelligence. Security clearances should be standardized and reciprocal among agencies and levels of government.

### **Developing Interoperable Communications between First Responders**

In the response stages of consequence management, as was tragically evidenced by the World Trade Center attacks of September 11, the ability to save lives is directly proportional to the capability to communicate.

Interoperable equipment standards for emergency responders, including definition and terms, is critical so in any use of mutual aid the responding party has equipment compatible with all other responders.

Many states are developing state-of-the-art radio communications networks for emergency first responders, including law enforcement and fire personnel, emergency medical services (EMS) workers, and other public health professionals. These systems must be designed to be interoperable both intrastate and among contiguous states. An adequate wireless spectrum to accommodate tens of thousands of federal, state, and local users is essential.

- Action must be taken at the federal level to ensure that there are adequate radio frequencies, known as spectrum, dedicated to public safety needs. Under the existing allocations, governed by the Federal Communications Commission (FCC), there is inadequate available dedicated public safety spectrum at the 700 MHz frequency band.
- There are two related issues regarding spectrum availability. First, there is a timing issue as to when commercial television broadcasters will vacate analog spectrum in the 60–69 channel range. Second, there is the interference issue, posed by Canadian broadcasters, associated with broadcast spectrum in the northern-border region.

As mandated by a 1996 act of Congress, commercial broadcasters are directed to relinquish the 700 MHz spectrum band by December 31, 2006, which includes 24 MHz of spectrum allocated for public safety. However, a provision in the 1996 agreement stipulated that broadcaster vacancy of the 700 MHz spectrum would be contingent on nationwide transition of analog to digital services by 85 percent of market share, so enforcement of this agreement is in doubt. The situation will rapidly worsen as states develop more comprehensive communications systems to transmit voice and data targeted at incident prevention and emergency response. Dedicated spectrum for state and local

government public safety use is a vital part of the nation's homeland security strategy, and the federal government must make immediate plans for its accommodation.

A land mobile radio system (LMRS) will provide full and comprehensive interagency communications. However, federal funding is necessary to implement LMRS in each state. To take maximum advantage of the interoperability features of this system, U.S. Department of Defense (DOD), federal non-DOD, state government and local government must all be included. Although DOD has the funding to implement migration to this system, other federal agencies, state governments, and local governments do not. Congress could assist in improving emergency communications by funding LMRS in all states and territories at the state and local level.

### **Identifying and Protecting Critical Infrastructure**

In the aftermath of the September 11 attack, governors have responded to the call for increased homeland security. They are providing sustained security for public buildings, dams, borders, water supplies, nuclear plants, airports, education centers, and other critical infrastructure.

State homeland security directors understand the interdependencies and volatility of shared assets, such as pipelines, communications, and power grids, and they have made protection of key assets and critical infrastructures a top priority. Because it is a practical impossibility to protect every vulnerable site, public gathering place, or bridge and tunnel in the nation, states require federal assistance to focus protection efforts and set funding priorities to conduct risk and vulnerability assessments. Protection of critical infrastructure and effective information sharing are directly related.

An equitable distribution of investment and inventorying responsibility needs to be developed. The federal government should underwrite the cost of protecting assets with national security implications, states should receive federal funding to distribute to cities and counties in the vicinity of critical infrastructure, and the private sector should be given guidance and regulatory oversight to make necessary security-related upgrades to both physical and cyber-infrastructure.

### **Enhancing Bioterrorism Preparedness**

The public health and medical care arenas present the greatest national shortages in capabilities and resources to respond and react to weapons of mass destruction (WMD) events. To deal with mass casualty events (or potential mass casualty events), our nation and our states must make the increase in public health and medical capabilities—and the ability to deploy these resources—very high priorities.

The U.S. Department of Health and Human Services (HHS) has dedicated \$1.1 billion to help states strengthen their capacity to respond to acts of bioterrorism and other public health emergencies for both the human and animal populations. However, state and local governments face substantial challenges in preparing the nation's public health system to deal with a chemical, biological or nuclear/radiological attack. Challenges include securing investment in the nation's hospitals and testing labs, creating laws that provide for emergency health powers, deploying personal protective equipment (PPE), and conducting joint-forces training among first responders and the military. The anthrax mailings of last October proved that even a relatively minor scale of attacks could severely test the public health infrastructure.

State homeland security directors recognize that the build-out of public health needs to be integrated into all of the other state preparedness and emergency response agencies efforts. They believe the federal definition of "first responder" should be expanded to include public health, hospitals, and other non-traditional response agencies.

State and local governments need help in upgrading their public health infrastructure in the following key areas:

- Coordinated planning with public health personnel, including hospitals and labs.
- Enhanced analytical capacity at state and local laboratories.
- Improved response and capacity to deal with mass casualties' response and capacity.
- Enhanced medical surge capacity—because of inadequate surge capacity, appropriate medical care for victims of mass casualty incidents is far from guaranteed. The nation must consider nontraditional ways to buttress medical surge capacity, including non-hospital alternatives such as Veterans Hospitals; and utilizing gymnasiums, armories, and other facilities, such as mobile hospitals, for mass casualty incidents.
- Build-out of communications systems that improve surveillance, detection, and communication capabilities based on symptomology and disease reporting at both local and regional levels (including alerts and notifications).
- Training to improve state and local capacity in epidemiology and disease surveillance.
- Bioterrorism-relevant training for all responders, especially covering the range of harmful agents and eradicated diseases, such as smallpox.
- Rapid distribution of vaccines and medical supplies.

### **Funding**

Despite indications of a national economic recovery, state budgets are expected to remain depressed through fiscal 2003 due to anemic revenue growth, an unanticipated jump in income tax refunds, and a meteoric rise in health care costs. The national recession and the economic fallout of September 11, combined with the explosion in Medicaid spending, contributed to a \$40 billion to \$50 billion budget shortfall. As a result, 39 states were forced to reduce their enacted budgets by about \$15 billion, tap “rainy day” funds, and/or make transfers from other reserves. Governors are facing unprecedented fiscal pressure. Even as the economy turns around, the state budget forecast will remain stormy since revenue growth lags the recovery by at least 12 months to 18 months.

The federal government should provide adequate federal funding and support to ensure that homeland security needs are met. The Office of Homeland Security should have the ultimate authority to coordinate policy and set funding levels from which grants to states could be provided for sustained state capacity. Every state should be assured a minimum allocation.

In addition to significant initial federal investment, ensuring homeland security requires yearly maintenance-of-effort and a long-term commitment by the federal government.

### **Protecting Sensitive Security Information**

In the interest of homeland security, the nation's governors are concerned about the disclosure of sensitive security information compiled by both state and federal governments. Governors ask that consideration be given to amending the federal Freedom of Information Act (FOIA), Title 5, U.S.C., Section 552, to protect this information from general disclosure. FOIA includes specific provisions protecting classified information, trade secrets, and confidential commercial and financial information from disclosure. Although these provisions may apply to homeland security information, FOIA provisions do not specifically address the protection of sensitive security information. Information that may need protection from disclosure includes:

- federal agency requests from states to assess state security vulnerabilities, response capacities, and government infrastructures;

- details concerning the location, storage, and transportation of hazardous material;
- Federal Emergency Management Agency assessments;
- grant proposals and receipts describing security vulnerabilities; and
- private-sector information gathered to assess security vulnerabilities.

Many states have already begun to consider measures to protect this information at the state level. To further enhance our nation's security, a dialogue should begin on possible changes to FOIA to provide federal protection of critical infrastructure and vulnerability information.

In addition, some states are considering revising existing FOIA laws to exempt critical information by statute, as a means of "piggybacking" on the proposed Sections 203 and 204 of the President's proposed homeland security legislation and to further safeguard against the disclosure of vulnerability-related information.

### **Securing Borders, Airports, and Seaports**

Following the attacks of September 11, enhanced security measures at border crossings and ports of entry delayed private and commercial vehicle crossings and the passage of materials needed by manufacturers, wholesalers, and retailers of commercial goods and services. While the security measures are reasonable and necessary, the impact on interstate and international commerce has been significant—especially in states that share a border with Canada. Governors showed their willingness to help lead federal agencies by activating the National Guard to assist at border crossings in the same manner as the Guard was then being used, under state control, at our nation's 422 international airports. Utilization of the National Guard under Title 32 U.S.C. for a federal purpose and at federal expense, albeit under continuing state control, is an operationally and fiscally efficient way to provide interim state assistance to the federal government.

More appropriate staffing must be provided for the federal agencies responsible for border and port security and a better system must be developed to deal with the tens of millions of containers that cross U.S. borders. The contents—or even the senders—of thousands of these multi-ton containers moving via trucks, trains, or barges are unknown until the cargo is cleared at its final destination within the country, generally more than 10 days after the containers have gone through our borders and moved on to major industrial cities.

The right level of protection will require thousands of state and local government officials, along with the federal government, and literally millions of people will have to be trained to a higher level of alertness.

### **Defining the Role of the National Guard in Homeland Security**

Throughout its history, the National Guard has participated in domestic disaster response and recovery operations. In recent years this mission has been referred to as Military Support to Civil Authorities (MSCA). Because of its preparation for the full spectrum of federal missions and its organization, the National Guard, while performing in either state or federal status, is prepared to accomplish any and all homeland security roles. Many states' Guard forces include infantry, aviation, engineer and a variety of service support units.

The National Guard can be effectively used in many ways. However, as recent experience in federalizing the National Guard for border security missions under Title 10 U.S.C. so aptly illustrated, optimal use of the National Guard occurs under the control of the governor.

Using National Guard forces under Title 32 U.S.C. has significant fiscal and operational advantages. Under Title 32, Guardsmen receive their pay and allowances from the federal government but remain in their assigned units and under their governor's command. They continue to train for other missions and are available to deploy with their units. Federalized Guardsmen, however, are no longer available

to their states or units. Moreover, Guardsmen serving under Title 32 do not fall under the Posse Comitatus Act, the 1878 law that prohibits the use of federal troops in law enforcement.

As homeland security evolves and matures, there will undoubtedly be new and unanticipated homeland security roles for the National Guard in addition to its vitally important OCONUS combat role. For example, in some states, the National Guard is responsible for receiving, breaking down, and distributing the Centers for Disease Control and Prevention (CDC) Pharmaceutical Push Package, as well as securing and deploying other critical pre-positioned emergency response equipment. For homeland security purposes, the National Guard is America's forward-deployed military force. It uniquely connects every fire and police station to the Pentagon and every statehouse to the White House. The National Guard should therefore be a lead domestic military component in executing our national homeland security strategy.

Thirty-two states have a federally resourced National Guard Civil Support Team (CST) capable of operating in a dead zone and conducting an immediate onsite assessment of hundreds of chemical, biological, radiological, and nuclear threat agents. CSTs provide life-saving situational awareness and technical assistance to first responders who might otherwise be among the legions of casualties when responding to the site of a terrorist attack. Every state, territory, and the District of Columbia need a National Guard CST to safeguard its citizens and emergency responders. Congress should therefore authorize and fund a team in each jurisdiction.

### **Integrating Incident Command Systems**

State homeland security directors believe that federal agencies should integrate their command systems into existing state and local incident command systems (ICS) rather than requiring state and local agencies to adapt to federal command systems. State and local governments have systems already in place that are tailored to local conditions (population distribution, geography, weather, economy, political factors, etc.). In most events—especially a biological event—it may be a long time before the event is detected and even longer before possible terrorist involvement is suspected. During that time, local officials will be in charge.

Therefore, the federal agencies (FBI and DOD) should adapt to the local system. State and local agencies/jurisdictions know that in the crisis management phase of a terrorist attack, the FBI is in charge and that, in the consequence management phase, FEMA is in charge of coordinating federal support of response and recovery. The consensus among many states is that the Unified Command process is the best way to integrate command in both crisis and consequence management, especially as the two phases may be conducted concurrently. The National Interagency Incident Management System-based ICS widely recognized and used among emergency management and first-responder organizations throughout the country, incorporates the Unified Command process.

### **Conclusion**

Governors have a critical interest in domestic terrorism because responding to the consequences of terrorist events is clearly within their authorized roles and responsibilities. State and local officials—often in partnership with the private sector—are working to defend the security of America's critical infrastructure (including transportation systems, dams, water supplies, and energy facilities), communication networks, and the food supply. In addition, the public health system is working overtime to respond to current public health threats and to prepare for future emergency situations. Governors recognize that the transformation of state emergency preparedness systems to address the threat of terrorism will take time, money, and strategic planning.