

The Strategic Plan for Safeguarding
the **COMMONWEALTH** *of*
MASSACHUSETTS
Against Terrorist & Related Threats



Commonwealth of Massachusetts

Mitt Romney, Governor

The Office of Commonwealth Security

Richard S. Swensen, Director

January 2003

Prepared for the Commonwealth of Massachusetts by

The Institute For Foreign Policy Analysis

Cambridge, MA Washington, DC

The Strategic Plan for Safeguarding
the **COMMONWEALTH** *of*
MASSACHUSETTS
Against Terrorist & Related Threats



Commonwealth of Massachusetts
Mitt Romney, Governor

The Office of Commonwealth Security
Richard S. Swensen, Director

January 2003

Prepared for the Commonwealth of Massachusetts by



The Institute For Foreign Policy Analysis

in Association with The Fletcher School, Tufts University

Executive Summary	iii
I. Introduction	1
Key Definitions	3
The New Security Environment and Threats	4
Combating the Emerging Threats	5
The Means of Attack	6
Division of Responsibilities within Homeland Security	8
Steps Taken by the Commonwealth to Increase Post-9/11 Security	8
II. Preventing Terrorist Attacks	13
Organizing for Commonwealth Security	13
III. Critical Mission Areas: Reducing the Commonwealth's Vulnerabilities	17
Intelligence and Warning	17
Transportation Security	19
Domestic Counterterrorism	20
Protecting Critical Infrastructure and Key Assets in the Commonwealth	21
Defending Against Catastrophic Threats	26
Emergency Preparedness and Response	27
IV. Foundations	33
The Law	33
Science and Technology	34
Information Sharing and Systems	35
Regional Cooperation	36
V. Conclusions: The Commonwealth's Homeland Security Priorities	38

Executive Summary

This *Strategic Plan for Safeguarding the Commonwealth of Massachusetts against Terrorist and Related Threats* outlines threats that confront the Commonwealth and the nature of our vulnerabilities; describes the concrete steps taken by Massachusetts since the events of September 11, 2001 to enhance security and to protect the Commonwealth from terrorism; addresses measures that still need to be taken or continued; and, finally, sets forth a series of specific recommendations designed to guide and improve Commonwealth security in the years ahead.

As the first state-wide blueprint to address the threat of terrorism to the Commonwealth of Massachusetts, this *Strategic Plan* builds upon the *National Strategy for Homeland Security* issued by the Office of Homeland Security in July 2002. It takes as its point of departure the recommendation that state governments, as well as local authorities and concerned citizens, should “go through a similar process of priority-setting and long-term planning.” It provides a strategic framework upon which the Commonwealth can structure its activities and create priorities as it organizes to combat terrorism. This document is based on extensive interviews and discussions with officials in each of the major agencies and offices having responsibility for Commonwealth security. It is not a static document, however; instead, it represents a strategy that will be modified and updated over time as required and the security situation warrants. The *Strategic Plan* is the beginning of what will be a prolonged effort to defend the Commonwealth from terrorism and its destructive consequences and to do so within a dynamic and rapidly changing setting at home and abroad.

Strategic Objectives

In keeping with the *National Strategy for Homeland Security*, this *Strategic Plan* for Massachusetts is based on three key strategic objectives:

- Prevent terrorist attacks within the Commonwealth
- Reduce the Commonwealth's vulnerability to terrorism
- Minimize the damage and recover from attacks that do occur

Preventing Terrorist Attacks

The first priority for both the Nation and the Commonwealth is to prevent and deter terrorist attacks. Deterrence against terrorist actions is created by the commitment to defeat terrorism wherever it appears by detecting terrorists before they have the chance to strike, to prevent terrorists from entering the country, and to take action to eliminate the threat that terrorists pose to the Nation. Because Massachusetts is a key point of entry as a result of its port and airport facilities, the Commonwealth bears a special responsibility to the region and the Nation.

An effective domestic counterterrorism effort requires preventive action. We have numerous law enforcement capabilities available to thwart terrorist acts that can only be fully used if an efficient intelligence and warning system is capable of detecting and monitoring terrorist activity before an attack occurs. This requires that we maintain an effective intelligence and warning system. For the Commonwealth, this means not only a threat alert system such as has been put into place since 9/11, but also the ability to disseminate, communicate, and integrate timely information and intelligence to the user community.

Terrorism itself is a means of attack that utilizes many types of capabilities as well as strategies and tactics. It may employ suicide bombers as in 9/11 or remotely launched surface-to-air missiles as in the failed attack on an Israeli airliner in December 2002. It is possible to envisage suicide bombers carrying explosives or entering the Commonwealth with an infec-

tious disease. Ships carrying containers with a nuclear weapon entering our ports or ships capable of launching a nuclear or conventionally armed short-range missile off our shores provide only several examples of the types of capabilities that could be available to terrorists against targets in Massachusetts. Terrorists today have the ability to strike at any place, at any time, and with a wide variety of weapons. Terrorist attacks are generally both premeditated and meticulously planned. The tactics and targets of various terrorist movements, as well as the weapons they favor, are shaped by a group's ideology and its internal organization. With this in mind, the Commonwealth of Massachusetts must defend against a wide range of potential attacks. Terrorists can employ traditional means such as conventional explosives and guns. However, terrorists are seeking to obtain weapons of mass destruction in order to produce mass casualties of innocent U.S. citizens. In addition, as demonstrated so vividly on September 11, terrorists utilize asymmetric strategies and capabilities to strike our infrastructure and inflict casualties on our population.

Organizing for Commonwealth Security

If terrorist attacks are to be prevented, our strategy must be focused at each of the levels of government and, to the extent possible, between the public and private sectors. The United States Constitution confers on the states all authority not specifically granted to the federal government. Within the U.S. structure there are overlapping federal, state, and local authorities and jurisdictions. How to focus, coordinate, and, where necessary, integrate the efforts of these elements of governance is a formidable challenge but nevertheless an essential task if we are to prevent future acts of terror.

Although the responsibility for preparing for and responding to a terrorist attack is shared by the federal, state, and local governments, the state and local authorities will be the first responders to a terrorist incident. As we organize against the threat of terrorism, relevant federal, state, and local government agencies should develop complementary systems that minimize

duplication and ensure that essential requirements are met. Specifically, this includes cooperation in the areas of law enforcement and prevention, emergency response and recovery, policy development and implementation.

Because it supplies the bulk of our goods and services, the private sector is a valuable source of ideas, concepts, and technologies that should be tapped to fight the war on terrorism. Moreover, since the greater part of our infrastructure is owned and operated by the private sector, the Commonwealth must work in close conjunction with the private sector to identify vulnerabilities to critical infrastructure nodes that are spread across the state. A cooperative partnership with the Commonwealth is both an example of the private sector's good citizenship as well as a reflection of sound corporate business practice designed to protect a company's assets and thus to contribute a sustained effort to prevent terrorist attack against the Commonwealth and its citizens.

Although the Commonwealth has an obligation to work with the public and private sectors to provide for security, the role of its citizens is of crucial importance. The events of 9/11, the anthrax attacks, and the fear of future incidents have made the people of Massachusetts more vigilant, informed, and eager to help defend against attack and to win the war on terrorism.

Steps Taken by the Commonwealth to Increase Post-9/11 Security

Since 9/11, the Commonwealth has taken numerous and wide-ranging measures to strengthen security against terrorism. The state has created the Office of Commonwealth Security, established a Bioterrorism Coordinating Council, implemented a state-wide Threat Alert System, established, with the U.S. Coast Guard, the port of Boston steering committee "Operation Safe Commerce-Boston," and developed various legal initiatives to enhance security. In addition, the state has increased coordination among federal, commonwealth, and local organizations, augmented security measures for all critical infrastructure nodes of the state, established the Statewide Anti Terrorism Unified Re-

sponse Network (SATURN), implemented more training among the various emergency management agencies, and strengthened the state's infectious disease surveillance program.

Critical Mission Areas: Reducing the Commonwealth's Vulnerabilities

The Strategic Plan for Safeguarding the Commonwealth of Massachusetts against Terrorist and Related Threats aligns and focuses Commonwealth security functions into six critical mission areas: intelligence and warning; transportation security; domestic counterterrorism; protecting critical infrastructure and key assets in the Commonwealth; defending against catastrophic threats; and, emergency preparedness and response. The *Strategic Plan* provides a framework to enhance these valuable security functions of the Commonwealth.

Intelligence and Warning

Terrorists have the ability to strike at any place, at any time, and with a wide variety of weapons. They depend on surprise to carry out their missions. Just as the attack on Pearl Harbor demonstrated shortfalls in U.S. intelligence and warning, the September 11 attacks on the Pentagon and World Trade Center once again pointed out deficiencies that must be addressed if we are to deter, preempt, prevent, and protect the Nation from another surprise terrorist attack.

Since 9/11, how to strengthen the capabilities of the various federal, state, and local agencies to gather and communicate actionable intelligence has been widely discussed. Good intelligence is the cornerstone of a strategy for Commonwealth security. The federal, state, and local emergency management, and law enforcement agencies together with the private sector must efficiently collect, share, and use intelligence in order to win the war against terrorism.

The Strategic Plan for Safeguarding the Commonwealth of Massachusetts against Terrorist and Related Threats identifies five major initiatives in this area:

- Enhance intelligence cooperation
- Facilitate the sharing of threat information

- Augment the Commonwealth Threat Alert System
- Utilize vulnerability assessments
- Increase tracking of dual-use equipment

Transportation Security

Transportation presents one of the largest potential vulnerabilities and challenges to the Commonwealth. The state's transportation network encompasses seaports, airports, highways, pipelines, railroads, and waterways that move people and goods. Such infrastructure must be protected to ensure the reliable flow of goods and services and to prevent terrorists from using our transportation assets to enter the United States or to perpetrate a terrorist action such as that committed by the hijackers of the two aircraft that took off from Logan International Airport on 9/11 and were crashed into the World Trade Center.

The federal government is currently working with both the Commonwealth and the private sector to upgrade security in all modes of transportation. The areas of emphasis have included: commercial aviation and road/highway/interstate systems; transportation of hazardous and explosive materials; protection of national airspace; shipping container security; traffic-management systems; transportation operators and workers; linkages with international transportation systems; and information sharing. The federal government is also utilizing existing model relationships (Operation Safe Commerce Boston) and systems to implement unified national standards for transportation security.

The *Strategic Plan for Safeguarding the Commonwealth of Massachusetts against Terrorist and Related Threats* identifies four major initiatives in this area:

- Create "Smart Borders"
- Promote "Operation Safe Commerce-Boston"
- Develop and deploy non-intrusive inspection devices
- Protect the Commonwealth's airports

Domestic Counterterrorism

The terrorist attacks of 9/11 redefined the missions, roles, and responsibilities of federal, state, and local law enforcement authorities to focus more extensively on counterterrorism issues. While it has been necessary to assign priority to preventing terrorism, pre-9/11 responsibilities remain important as well. Law enforcement agencies have been called upon to fight terrorism while they continue to work in their traditional areas of responsibility – and often to do so without major additional resources.

Enabling law enforcement agencies to focus on older and newer priorities requires numerous changes in approach, organization, training and capabilities as set forth throughout this report. Many improvements have already been made throughout the Commonwealth, but much more needs to be done to strengthen domestic counterterrorism capabilities. The improvement of post-9/11 communication among these agencies has produced greater coordination of domestic counterterrorism efforts.

The *Strategic Plan for Safeguarding the Commonwealth of Massachusetts against Terrorist and Related Threats* identifies four major initiatives in this area:

- Improve intergovernmental law enforcement intelligence sharing and cooperation
- Continue to emphasize agency cooperation through both the Joint Terrorism Task Force and Anti-Terrorism Task Force
- Target terrorist financing
- Employ "red team" techniques

Protecting Critical Infrastructure and Key Assets in the Commonwealth

Crucially important to reducing the Commonwealth's vulnerabilities is the protection of its infrastructure. This was immediately recognized after 9/11. The Massachusetts State Police prepared a directory of critical public and private infrastructure. The federal government defines critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, nation-

al economic security, national public health or safety, or any combination of those matters.” It defines key assets as “individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage morale or confidence.” Key assets include symbols or historical sites and monuments, and high profile concentrations of people such as concerts or sporting events. Criteria are being developed at the federal level that will provide a clearer basis for prioritizing critical infrastructure assets in Massachusetts.

Fighting terrorism is an exceedingly complex task. Our strategic approach will require agility and flexibility because terrorists will be agile and flexible in adapting their tactics to exploit our vulnerabilities. Intelligence that is now publicly available indicates that the organizers of the terrorist acts of 9/11 have chosen to target civilians and the infrastructure that supports our society – what have been termed soft targets. These include essentially three categories. The first category is targets of *symbolic* value such as the USS *Constitution* or the State House; the second is *infrastructure* targets such as skyscrapers, ports, train stations, and nuclear power plants; the third is *human targets* – large numbers of people who would be congregated in a sports stadium or other public setting. Influential public figures have also been singled out in terrorist documents as a category for attack.

To accomplish their goals, terrorists can employ diverse capabilities encompassing conventional weapons as well as other approaches such as strikes against the U.S. cyber/information technology infrastructure. Terrorists may soon possess weapons of mass destruction (WMD), including chemical, biological, nuclear, and radiological devices, which could produce unprecedented levels of devastation against our population and infrastructure. The Commonwealth will seek to deny terrorists the opportunity to inflict damage upon our critical infrastructure nodes and key assets by improving their protection.

The *Strategic Plan for Safeguarding the Commonwealth of Massachusetts against Terrorist and Re-*

lated Threats identifies nine major initiatives in this area:

- Maintain a complete and accurate assessment of the Commonwealth’s critical infrastructure and key assets
- Protect, to the extent possible, the Commonwealth’s critical infrastructure and key assets
- Harness the five-step risk management model to protect critical assets
- Work with the federal government to develop a National Infrastructure Protection Plan and utilize appropriate criteria being developed
- Enhance Port Security through “Operation Safe Commerce-Boston”
- Increase security of international shipping containers
- Devote continued attention to the security of Logan International Airport
- Secure cyberspace
- Enable effective partnership and cooperation with state and local governments and the private sector

Defending Against Catastrophic Threats

Defending the Commonwealth against catastrophic threats, including WMD, requires unprecedented coordination, communication, and interoperability among all relevant agencies, authorities, organizations, and individuals, especially first responders. Such cooperation will allow for better detection and response to a WMD attack.

The *Strategic Plan for Safeguarding the Commonwealth of Massachusetts against Terrorist and Related Threats* identifies three major initiatives in this area:

- Prevent terrorist use of nuclear weapons through better sensors and procedures
- Increase the training of local health providers to recognize attacks utilizing weapons of mass destruction
- Facilitate advanced research into medical sciences to develop broad spectrum vaccines, antimicrobials, and antidotes

Emergency Preparedness and Response

Preparing for response and recovery in the event of a terrorist attack is vitally important in mitigating the effects of any such incident. The response to an emergency must be coordinated, comprehensive, and to the extent feasible, standardized among responders. The state, along with its municipalities, will bear much of the initial burden and responsibility for providing an effective public health response to a biological or chemical terrorist attack on the state's population. The first line of defense will be the state and local public health personnel, who will likely be the first to recognize that the Commonwealth has been attacked with biological or chemical agents.

The Commonwealth must continue to ensure that all response personnel and organizations are properly equipped, trained, and exercised to respond to all terrorist threats and attacks within the Commonwealth. It is also necessary for the Commonwealth to engage the private sector and to work with the federal government.

The *Strategic Plan for Safeguarding the Commonwealth of Massachusetts against Terrorist and Related Threats* identifies seventeen major initiatives in this area:

- Enhance preparations for detecting and responding to a bioterrorist/chemical attack
- Maintain efforts to secure federal grants to continue planning, training, and purchasing of equipment
- Utilize the Massachusetts Bioterrorism Coordinating Council
- Make use of the Statewide Bioterrorism Preparedness and Response Program Advisory Committee and the Hospital Preparedness Planning Committee
- Augment the Commonwealth's access to vaccine
- Enhance cooperation with the Centers for Disease Control and Prevention
- Address the issue of surge capacity, especially in hospitals
- Aid in the creation of a national incident management system

- Continue to implement the use of the Incident Command System
- Enable seamless communication via interoperability among all responders
- Continue the development of tabletop exercises to provide training
- Strengthen ties with neighboring states through the use of the Emergency Management Assistance Compact
- Improve state relations with the National Disaster Medical System
- Create guidelines for vaccination
- Enhance first responder training
- Augment the victim support system
- Plan for military support to civil authorities

Foundations

The *National Strategy for Homeland Security* cites four fundamental tenets or foundations – law, science and technology, information sharing and systems, and international cooperation – that infuse each homeland security mission area, cut across federal, state, and local levels of government, and permeate all sectors of U.S. society. Three of these tenets, law, science and technology, and information sharing and systems, provide a useful starting point to assess needed homeland security investments within the Commonwealth. Since a principal state-level focus will be regional, cross-state cooperation, this *Strategic Plan* includes this important area as one of the foundations for Commonwealth security.

The Law

Throughout its history, the United States has utilized the law to advance and preserve our security and liberty. The law supplies the means for the government to act and to define the proper limits of those actions. The law also provides the basis for civil relationships that affect each of our citizens. Since September 11, the federal government has enacted major legislation designed to combat terrorism while simultaneously attempting to ensure that they do not unduly preempt state law or adversely impact our basic civil liberties.

The Commonwealth has also focused closely on legislative requirements following the events of 9/11. It has conducted an extensive review of the state's existing statutes to determine what laws are applicable to the current counterterrorism effort and what additional legislation is necessary to protect the public welfare and provide for security against terrorism. As a consequence of this review, Massachusetts quickly drafted and passed a series of first round legal measures addressing issues related to the use of hoax substances, the possession of weapons at airports, limitations on public access to sensitive infrastructure data, criminalizing unauthorized possession of explosives and the use/possession of either bio- or chemical weapons, and criminalizing the communication of terrorist threats in various media. A major goal underpinning development of its anti-terrorism laws is to make certain that basic civil liberties in the Commonwealth are not undermined.

The *Strategic Plan for Safeguarding the Commonwealth of Massachusetts against Terrorist and Related Threats* identifies the following legislative initiatives in this area that are currently pending:

- Maritime security
- Money laundering
- Computer hacking
- Statewide grand jury
- Defining the crime of terrorism
- Bioterrorism and emergency powers
- Wire tapping
- The tagging of explosives
- A forfeiture statute to include anti-terrorism

Science and Technology

Our Nation's historic strength in science and technology is critical to protecting America from terrorism. Just as science and technology have helped the United States defeat enemies overseas, they will contribute to our efforts against terrorists who attack our Nation. The Commonwealth possesses unique and robust capabilities particularly in the vital science and technology areas cited above. Indeed, our state is the location of many of the world's most innovative

high-technology firms and organizations, defense corporations, renowned educational centers, and medical institutions, responsible for ground-breaking research ranging from software development and information technology, biomedicine and vaccines against bioterrorism, to advanced surveillance/detection techniques and systems. As a result, the Commonwealth has the potential to play a leading role in the national effort and to make significant contributions to the homeland security mission both to the Nation as whole, and directly here in Massachusetts.

The *Strategic Plan for Safeguarding the Commonwealth of Massachusetts against Terrorist and Related Threats* identifies the following two initiatives in this area:

- Develop chemical, biological, radiological, and nuclear detection mechanisms
- Utilize the innovative high-technology firms and organizations, defense corporations, renowned educational centers, and medical institutions found within the Commonwealth to make significant contributions to Homeland Security

Information Sharing and Systems

Information systems contribute to every facet of the homeland security mission. However, even though American information technology is the most advanced in the world, at present our Nation's information systems do not adequately support that mission. Databases used for federal law enforcement, immigration, intelligence, public health surveillance, and emergency management have not been interconnected in a manner that eliminates information gaps or redundancies.

The *Strategic Plan for Safeguarding the Commonwealth of Massachusetts against Terrorist and Related Threats* identifies two major initiatives in this area:

- Further develop the Information Technology Commission to address the state's information technology systems and to enhance interconnectedness
- Improve the communication capabilities of the state

Regional Cooperation

The Commonwealth needs to place greater emphasis on regional cooperation for the homeland security mission. This requirement became obvious following September 11 for several reasons. The impact of terrorist incidents can easily transcend state borders. For example, an outbreak of smallpox in the Commonwealth could quickly spread to neighboring states and to the Nation as a whole.

The Commonwealth should seize the initiative to conclude additional mutual aid agreements with neighboring states and to institute advance planning to cope with the regional/national implications of terrorism. This will require greater planning, cooperation, and joint exercises across state boundaries in and beyond New England.

The *Strategic Plan for Safeguarding the Commonwealth of Massachusetts against Terrorist and Related Threats* identifies three major initiatives in this area:

- Strengthen ties with neighboring states through the use of Emergency Management Assistance Compacts
- Utilize the New England Regional Coalition of Governors to harmonize, coordinate, and implement homeland security strategies
- Conclude mutual aid agreements with neighboring states to request out-of-state aid during an emergency situation.

Conclusions

The *Strategic Plan for Safeguarding the Commonwealth of Massachusetts against Terrorist and Related Threats* identifies important tasks that have already been initiated together with priorities and issues that must be addressed:

- *A new mindset is needed.* The post-9/11 strategic environment requires a new strategy that incorporates innovative, original concepts that cut across federal, state, and local jurisdictions as well as transcend outmoded, ineffective approaches to security. We must think about issues, resources, and relationships in ways that “connect the dots” in unprecedented and unac-

customed ways. It is no longer possible to compartmentalize security, including intelligence, between what takes place outside the United States and what could occur as a result in the Commonwealth.

- *Organize for homeland security:* How we organize for Commonwealth security highlights the critical importance that we attach to the protection of our citizens and infrastructure against terrorism. Essentially, there are four leading organizational options for homeland security. They include: 1) moving the Office of Commonwealth Security (OCS) into an existing cabinet department, e.g., the Executive Office of Public Safety; 2) creation of a Commonwealth Department of Homeland Security patterned after the recently established federal Department of Homeland Security; 3) retention of the OCS with additional areas of responsibility and jurisdiction; and, 4) keeping the same OCS organizational structure as now exists. In option one, the responsibilities of Commonwealth homeland security would be folded into an existing cabinet department such as the Executive Office of Public Safety allowing the new Commonwealth security entity to tap into the range of funding and staffing resources available to a cabinet-level secretariat. Option two would mirror the design of the new Department of Homeland Security which will amalgamate at least twenty-two diverse federal agencies including the U.S. Coast Guard, the Customs Service, the Immigration and Naturalization Service, the Secret Service, and the Transportation Security Administration. Option three, an expanded OCS, would be given significantly greater staff personnel, a separate budget, and augmented resources. Finally, option four is the continuation of the status quo. If OCS is to implement its broad charter successfully, however, maintaining the status quo is not a viable long-term organizational option. Whatever organizational option is chosen, the Office of Commonwealth Security, at least during emergencies, should have a direct line

of communication and responsibility to the Governor. Such an organizational approach would communicate to the citizens of the Commonwealth that Massachusetts attaches as great a priority as the federal government to homeland security.

- *Review and update the Governor's emergency powers.* The Governor's emergency powers need to be reviewed and modified as deemed necessary in order to address the exigencies of the terrorist threat. Where required, new legislation must be drafted and passed to ensure that the Governor and the Commonwealth can cope with a range of possibly unprecedented emergencies that were not deemed likely – or even considered – prior to September 11. At a minimum, the Commonwealth needs to review and modify emergency powers related to continuity of government and lines of succession issues in case of the injury or death of the Governor and Lieutenant Governor; quarantines and evacuation procedures; appropriation/use of private property; imposition of rationing and related restrictions; and legal liability and indemnification issues.
- *Augment the Commonwealth's biomedical health service capabilities.* The core capacity for public health and medical care needs to be greatly enhanced with respect to detection and treatment of infectious disease resulting from bioterrorism. The biomedical, public health, and human services communities should be working in greater partnership with one another, coordinating more effectively with the larger national security community.
- *Expand surge capabilities.* The Commonwealth must develop a comprehensive strategy for assuring surge capacity for health care in the event of a large scale terrorist incident. The Commonwealth needs to identify all existing assets, including the number of current medical/health staff as well as retired physicians and health personnel who could be called upon for help in an emergency, and how they would be mobilized to address mass casualty care. In addition, procedures for increasing the number of hospital beds and related health care assets need to be developed and implemented.
- *First responder training.* Updated and continuing courses/training for first responders to incidents involving chemical, biological, radiological, and nuclear weapons must be an integral part of the instruction received by the firefighters, police, HAZMAT workers, public health personnel, doctors, and nurses, and other appropriate groups throughout the Commonwealth.
- *Promote greater regional cooperation.* The Commonwealth needs to place greater emphasis on regional cooperation for the homeland security mission. Advance planning to cope with the regional/national implications of bioterrorism is an urgent priority. This will require greater planning, cooperation, and joint exercises across state boundaries in and beyond New England.
- *Identify the Commonwealth's critical infrastructure and vulnerabilities.* Continue to identify, update, and prioritize the inventory of the Commonwealth's critical infrastructure. This encompasses: airports, seaports and harbors, nuclear facilities, dams, water and sewer plants, electric power plants, gas pipelines, bridges, biological and chemical facilities, and our cyber infrastructure. Utilize the criteria being developed at the federal level that will furnish a clearer basis for prioritizing the Commonwealth's critical infrastructure.
- *Protect our seaports, harbors, and airports.* Commonwealth agencies responsible for the protection of the state's harbors and airports, working closely with the U.S. Coast Guard and other relevant federal agencies, need to detect, intercept, and interdict potential threats as far away as possible to thwart criminal or catastrophic events.
- *Foster closer relations with the private sector.* Develop a partnership with the private sector. Preparing for homeland security must include the private sector as a vi-

tal partner in the war against terrorism considering that most of the Commonwealth's critical infrastructure is owned or operated by the private sector.

- *Ensure the compatibility of equipment:* The Commonwealth needs to take the necessary steps to ensure the compatibility/ interoperability of equipment related to emergency preparedness and response such as communication devices, respirators, and other emergency gear.
- *Increase utilization of simulations and related techniques.* The use of simulations, tabletop activities, and “red teaming” that includes participation of the appropriate federal, state, and local officials to help improve the Commonwealth's security against terrorist attacks should be expanded. These tools are indispensable for training, measuring readiness, and identifying shortcomings in plans, operations and tactics, and equipment (e.g., non-interoperable communication devices).
- *Develop a comprehensive media/public relations strategy:* The Commonwealth must develop a comprehensive media and public relations plan to ensure that adequate procedures are in place to disseminate a consistent, accurate message designed to allay public fears.
- *The Strategic Plan for Safeguarding the Commonwealth of Massachusetts Against Terrorist and Related Threats* should be periodically reviewed, updated, and revised to take the fullest account possible of changing requirements for Commonwealth security.

Introduction

Americans discovered an alarming reality on September 11, 2001: that the United States is not exempt from ruthless foreign enemies capable of inflicting massive innocent civilian casualties on U.S. soil. The appalling attacks on the World Trade Center and the Pentagon on September 11, followed by the anthrax outbreak in several parts of the country, including Washington, D.C., dramatically reshaped the outlook of Americans regarding the threats confronting our Nation and created an imperative to prepare against future terrorist acts. Although the United States continues to face a range of security challenges, the events of 9/11 brought homeland security and counterterrorism into unprecedented focus. Indeed, today America is at war, in the second year of its global campaign to defeat Al Qaeda, the international terrorist network responsible for September 11, and to counter other terrorist threats that jeopardize our security. Homeland security is now our Nation's number one national security priority.

To quote President Bush, terrorism "is a challenge as formidable as any ever faced by our Nation." The United States confronts serious terrorist threats that encompass not only landmark buildings and government installations such as those attacked on 9/11, but also a wide array of other public and private infrastructure such as seaports, financial institutions, railroad, highway and airport transportation centers, water supplies, treatment plants, power grids, telecommunication and information technology nodes, and agricultural products and related facilities. The potential targets include the hospitals that would be critical elements in post-attack recovery. Although Al Qaeda represents the most urgent and immediate threat to the United

States, a number of additional terrorist groups – including domestic terrorist actors – have the capability to attack America. Given the openness of our society, terrorist assaults can come at any time and at any location, without warning, resulting in devastating physical, economic, and psychological impacts. These daunting challenges directly affect the security of the Commonwealth of Massachusetts and accordingly require sustained and concerted action. This includes the federal, state, and local levels as well as the public and private sectors. It requires cooperation between Massachusetts and other states in and beyond New England.

Fighting terrorism is an exceedingly complex task. Our strategic approach will require agility and flexibility because terrorists will be agile and flexible in adapting their tactics to exploit our vulnerabilities. Our response must be as sustained as the threat of terrorism, which is likely to last far into the future. Regrettably, the United States affords terrorists countless targets for possible attack. Intelligence that is now publicly available indicates that the organizers of the terrorist acts of 9/11 have chosen to target civilians and the infrastructure that supports our society – what have been termed soft targets. These include essentially three categories. The first is targets of *symbolic* value. In this case the goal is to produce a devastating psychological impact by destroying a national treasure such as the *USS Constitution* or an important building such as the State House. The second category is *infrastructure* targets such as skyscrapers, ports, train stations, and nuclear power plants. Such targets have great economic and symbolic value, but they also provide a basis for killing large numbers of people as in the World Trade Center. The final category is *human targets* – large numbers of people who would be congregated in a sports stadium or other public setting. Influential public figures have also been singled out in terrorist documents as a category for attack. To accomplish their goals, terrorists can employ diverse capabilities encompassing conventional weapons as well as other approaches such as strikes against the U.S. cyber/information technology infrastructure. Terrorists may soon possess

weapons of mass destruction (WMD), including chemical, biological, nuclear, and radiological devices, which could produce unprecedented levels of devastation against our population and infrastructure.

To deal with the terrorist threat effectively, the Commonwealth is crafting an innovative strategy that cuts across federal, state, and local jurisdictions as well as traditional approaches to security. Countering the terrorist threat requires a new mindset that not only brings together departments, agencies, expertise, and capabilities that have usually been viewed as separate, but also leads us to think differently about security than we may have been accustomed to in the past. Since 9/11 we have had to consider issues, resources, and relationships in ways that “connect the dots” in unprecedented and unaccustomed ways. Countering the terrorist threat also requires the acquisition of new capabilities coupled with more effective utilization of existing resources. In this regard, a key challenge is to ensure that new capabilities and existing resources are complementary and reinforcing, not duplicative; interlocking and not interblocking. Commonwealth security must also encompass efforts to anticipate, deter, and defend against terrorist acts on our citizens and critical infrastructure and to prepare for the management of the immediate and longer-term consequences of possible terrorist incidents. In addition, the strategy should serve as the foundation of sustained action in the coming years, for we face a challenge that may only begin to abate as we manifest continued resolve and dedication. Moreover, while implementing a strategy for enhanced security in Massachusetts, we must ensure that the civil liberties that define our way of life are not undermined. At the same time we must protect our ports and borders while ensuring that the commercial activity on which our prosperity depends is not jeopardized.

Since September 11, as this document enumerates, the Commonwealth has made significant progress in improving the security of Massachusetts against terrorist threats. However, considerable work remains as we prepare for a future that contains a broad spectrum of threats and dangers. To quote President Bush

again, the fight against terrorism demands a “coordinated and focused effort from our entire society – the federal government, state and local governments, the private sector, and the American people.”

This *Strategic Plan for Safeguarding the Commonwealth of Massachusetts against Terrorist and Related Threats* outlines threats that confront the Commonwealth and the nature of our vulnerabilities; describes the concrete steps taken by Massachusetts since the events of September 11, 2001 to enhance security and to protect the Commonwealth from terrorism; addresses measures that still need to be taken or continued; and, finally, sets forth a series of specific recommendations designed to guide and improve Commonwealth security in the years ahead.

This *Strategic Plan* represents the first state-wide blueprint to address the threat of terrorism to the Commonwealth of Massachusetts. It builds upon the *National Strategy for Homeland Security* issued by the Office of Homeland Security in July 2002. It takes as its point of departure the recommendation that state governments, as well as local authorities and concerned citizens, should “go through a similar process of priority-setting and long-term planning.” Its goal is to establish a strategic framework upon which the Commonwealth can structure its activities and create priorities as it organizes to combat terrorism. This document is based on extensive interviews and discussions with officials in each of the major agencies and offices having responsibility for Commonwealth security. It is not a static document, however; instead, it represents a strategy that will be modified and updated over time as required and the security situation warrants. The *Strategic Plan* is the beginning of what will be a prolonged effort to defend the Commonwealth from terrorism and its destructive consequences and to do so within a dynamic and rapidly changing setting at home and abroad.

In keeping with the *National Strategy for Homeland Security*, this *Strategic Plan* for Massachusetts is based on three key strategic objectives:

- Prevent terrorist attacks within the Commonwealth
- Reduce the Commonwealth’s vulnerability to terrorism
- Minimize the damage and recover from attacks that do occur

For Commonwealth homeland security, we must align and focus the critical mission areas identified in the *National Strategy for Homeland Security*. These include intelligence and warning; border and transportation security; domestic counterterrorism; protecting critical infrastructure and key assets; defending against catastrophic terrorism; and, emergency preparedness and response. Providing adequate intelligence and early warning, border and transportation security, and undertaking domestic counterterrorism are designed primarily to prevent terrorist attacks. Protecting critical infrastructure and defending against catastrophic terrorism focus on reducing our vulnerabilities. Emergency response and preparedness emphasize the need to minimize damage and to recover as rapidly as possible from an attack. Although the Commonwealth must address each of these mission areas, the focus of our effort is the most serious threats to Massachusetts:

- Port security
- Bioterrorism
- Attacks on critical infrastructure
- Information warfare

Each of these threats and the strategic response requirements for the Commonwealth are addressed in this document.

Key Definitions

This document utilizes the federal government’s definition of both homeland security and terrorism found in the *National Strategy for Homeland Security*. Homeland security is defined as “a concerted national effort to prevent terrorist attacks within the United States, reduce America’s vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.” Terrorism is defined as “any premeditated, unlawful act dangerous to human life or public welfare that is intended to intim-

idate or coerce civilian populations or governments.” This particular characterization of terrorism includes kidnappings; shootings; hijackings; conventional bombings; attacks involving chemical, biological, radiological, or nuclear weapons; cyber attacks; and any other forms of malevolent violence. U.S. citizens or foreigners, acting in connection with others, on their own, or on behalf of a hostile state who commit such acts are defined as terrorists.

The New Security Environment and Threats

Despite heightened awareness and numerous security efforts undertaken since September 11, 2001, and described below, Massachusetts, along with every other state, remains vulnerable to a wide variety of terrorist attacks. Nonetheless, the Commonwealth is actively engaged in preparedness activities designed to deter, prevent, and manage the consequences of a range of potential terrorist acts. This effort encompasses numerous federal, state, and local agencies and a variety of programs throughout the Commonwealth.

The new security environment contains threats that may have their origins in the mountains of South Asia, where terrorist training camps are located, and their consequences in the form of terrorist acts in our towns and cities, as we witnessed on 9/11. No longer is it possible to compartmentalize security between what takes place beyond our shores and what may occur as a result in Boston, Springfield, Amherst, or elsewhere in the Commonwealth. What is foreign and what is domestic are inextricably intertwined in ways that could hardly be imagined before 9/11. To think in such terms of interconnectedness is the essential precondition for the mindset that will be required at the state and local levels for post-9/11 Commonwealth security. We must be prepared to think in a novel fashion about phenomena that were once viewed as separate and unconnected as in the case of 9/11 itself – attacks of a type and magnitude that were widely thought to be inconceivable or impossible. Terrorists have demonstrated the capacity to turn our commercial aircraft into weapons to be used against oth-

er civilian targets. They have shown that it is possible to receive training in locations as remote as Afghanistan or as close as pilot-training facilities here in the United States.

It is the nature of our society that Massachusetts poses for the terrorist a target-rich environment so vast that complete protection is impossible. To make this assertion is simply to acknowledge the magnitude of the problem and to underscore the need for strategic planning that sets forth priorities and brings together resources that can be utilized to deter, prevent, and preempt terrorism, and if necessary cope with the consequences.

Within the Commonwealth we have an extensive array of capabilities to employ against terrorism. That is the good news. Unfortunately, Massachusetts, no less than the United States as a whole, contains countless targets for possible attack that are unprotected or inadequately safeguarded. Terrorists are likely to favor strikes against targets such as those that took place in New York City and Washington, D.C., on September 11. While the vulnerability of these targets can be reduced through more adequate intelligence collection, analysis and timely dissemination, together with improved physical security and other target-hardening measures, prevention across the board can never be fully guaranteed. The use of simple box cutters and commercial airliners filled with jet fuel as weapons demonstrates that terrorists are limited only by their imagination and their ability to gain access to the specific targeted groups and facilities required to carry out their acts.

Therefore, we must be prepared, through careful planning and the creation of rapid incident response capabilities, to minimize the consequences of terrorist attacks, while at the same time we develop unprecedented means to collect, analyze, and make available in timely fashion information that would minimize the likelihood of attack and provide protection to our most vulnerable and important targets, as discussed in greater detail in this document. Despite the fact that we have experienced successes in the war on terrorism, such as the toppling of the Taliban regime in Afghanistan and apprehending terrorists, the threat remains

a clear, present, and long-term danger to the Commonwealth. Our enemies are actively engaged in planning future attacks that could include targets in Massachusetts. The state's large, diverse, and mobile population allows terrorists to hide within our midst and to select from a long list of lucrative targets. People come together at schools, sporting events, malls, concerts, office buildings, high-rise residences, places of worship, and vacation resorts. These circumstances and venues present numerous potential targets where large numbers of casualties may be inflicted. The majority of the Commonwealth's citizens reside in urban areas that are themselves rich in potential terrorist targets.

Democracy and Liberty

Terrorism on the scale of 9/11 requires responses that minimize the threat to democratic institutions and constitutional freedoms of the Commonwealth. Because terrorist acts are intended to disrupt fundamental liberties, our responses must take full account of the need to safeguard that which terrorists would destroy. Consequently, as it enacts a strategy to protect its population and infrastructure, the Commonwealth will in parallel take the requisite steps to ensure that basic civil liberties are not sacrificed. As the Commonwealth takes the necessary measures to protect the physical security of its population, it is axiomatic that steps must be taken simultaneously to ensure that long-held and cherished democratic values and liberties are not undermined.

The Economy of the Commonwealth

Terrorism on the scale of 9/11 poses a direct threat to our economy. The massive property damage that occurred at the World Trade Center and Pentagon is part of the bitter legacy of those tragic events. Not as apparent, however, are the enormous economic/monetary losses, estimated in the hundreds of billions of dollars, resulting from the disruption of capital markets and other important economic sectors in New York City, together with the loss of irreplaceable human talent and productive labor represented by those killed or disabled. The

economy of Massachusetts is vital to the immediate New England region as well as to the Nation as a whole. Massachusetts is home to leading financial institutions as well as some of the world's foremost educational centers, high-technology firms, and innovative organizations producing pioneering research extending from software to biomedicine and vaccines against bioterrorism. The Commonwealth contains an entrepreneurial population with extensive education and training as well as a major concentration of the Nation's scientific and intellectual leadership. The importance of Massachusetts is underscored by its potential contributions to the core missions of homeland security. Therefore, Massachusetts represents a lucrative target for those who would seek to disrupt the economic life of the region and the Nation.

Combating the Emerging Threats

The first priority for both the Nation and the Commonwealth is to prevent and deter terrorist attacks. Deterrence against terrorist actions is created by the commitment to defeat terrorism wherever it appears by detecting terrorists before they have the chance to strike, to prevent terrorists from entering the country, and to take action to eliminate the threat that terrorists pose to the Nation. Because Massachusetts is a key point of entry as a result of its port and airport facilities, the Commonwealth bears a special responsibility to the region and the Nation.

An effective domestic counterterrorism effort requires preventive action. We have numerous law enforcement capabilities available to thwart terrorist acts that can only be fully used if an efficient intelligence and warning system is capable of detecting and monitoring terrorist activity before an attack occurs. This requires that we maintain an effective intelligence and warning system. For the Commonwealth, this means not only a threat alert system such as has been put into place since 9/11, but also the ability to disseminate, communicate, and integrate timely information and intelligence to the user community. Efforts to strengthen

such capabilities in the Commonwealth since 9/11 are described in this document.

In order to enhance capabilities for responding to a terrorist attack, the President of the United States has proposed that federal, state, and local public safety organizations work together to develop a comprehensive Federal Incident Management Plan. This all-discipline, all-hazard Federal Incident Management Plan would serve to clarify and streamline federal incident management procedures thus eliminating the distinction between the law enforcement/intelligence function of crisis management and the consequence management emergency mitigation and relief function. As a result, the Federal Incident Management Plan would make clear the specific roles and contributions of each emergency response and law enforcement agency to mitigate the incident after the terrorist attack has occurred.

The Means of Attack

Terrorism itself is a means of attack that utilizes many types of capabilities as well as strategies and tactics. It may employ suicide bombers as in 9/11 or remotely launched surface-to-air missiles as in the failed attack on an Israeli airliner in December 2002. It is possible to envisage suicide bombers carrying explosives or entering the Commonwealth with an infectious disease. Ships carrying containers with a nuclear weapon entering our ports or ships capable of launching a nuclear or conventionally armed short-range missile off our shores provide only several examples of the types of capabilities that could be available to terrorists against targets in Massachusetts. Terrorists today have the ability to strike at any place, at any time, and with a wide variety of weapons. Terrorist attacks are generally both premeditated and meticulously planned. The tactics and targets of various terrorist movements, as well as the weapons they favor, are shaped by a group's ideology and its internal organization. With this in mind, the Commonwealth must defend against a wide range of potential attacks. Terrorists can employ traditional means such as conventional explosives and guns. However, terrorists are seeking to obtain weapons of

mass destruction in order to produce mass casualties of innocent U.S. citizens. In addition, as demonstrated so vividly on September 11, terrorists utilize asymmetric strategies and capabilities to strike our infrastructure and inflict casualties on our population.

Weapons of Mass Destruction

Weapons of mass destruction (WMD) comprising chemical, biological, radiological, and nuclear devices (CBRN) are becoming more available to a variety of countries, as well as to terrorist organizations. Documents found by U.S. forces in Afghanistan showed that Al Qaeda possessed detailed diagrams of chemical and nuclear weapons. Many U.S. intelligence experts believe that the appropriate question is not *will* terrorists gain possession of WMDs, but rather *when*. Several estimates indicate that terrorist organizations may already have them. Indeed, the letters containing anthrax which killed five people in the months following 9/11 and the 1995 sarin gas attack in a Tokyo subway by the Japanese cult *Aum Shinriyko* plainly demonstrate this fact. CBRN weapons can be targeted against humans, animals, crops, the environment, and physical structures in a variety of ways.

Chemical weapons are extremely dangerous and have the potential of causing mass-casualties. A wide spectrum of chemical attack employment options exist. Chemical agents may be dispersed as a gas, vapor, liquid, or aerosol. A chemical agent could be disseminated by explosive or mechanical delivery systems. Chemical weapons are relatively easy to produce by using basic equipment, trained personnel, and other precursor materials and equipment that also frequently have non-lethal, legitimate uses. Each chemical agent has its own rate of dispersal where its longevity is varied. Some chemicals remain toxic for days or weeks and require decontamination and clean up while others disperse rapidly. Common industrial and agricultural chemicals can also be as highly toxic as bona fide chemical weapons and, as the 1984 Bhopal, India catastrophe demonstrated, just as deadly when unleashed.

Biological weapons consist of large numbers of disease-causing live microorganisms possessing a high lethality rate. Biological weapons can be manufactured if the required skills and equipment are obtained to produce microorganisms. The deliberate release of anthrax spores – primarily via letters delivered by the U.S. Postal Service – during the autumn of 2001, resulted in the deaths of five innocent people and seriously harmed 17 others. As these terrorist incidents showed, the delivery systems for biological weapons need not be sophisticated or high tech. Lastly, biological agents utilized against livestock and crops would not only cause casualties but possibly also result in greater disruption by generating fear about the purity and integrity of our food sources.

The anthrax outbreak of 2001 did not include actual cases in Massachusetts. Nevertheless, the Commonwealth faced the need to provide for the contingency that anthrax spores could be found in Massachusetts. An outbreak of biological terrorism in any part of the Nation is likely to pose a danger to all parts of the United States. Therefore, the Commonwealth must be prepared to work closely with the federal authorities and with other states. With respect to smallpox, this means that we must have in place the personnel and facilities to vaccinate people in accordance with established priorities. Given the nature of infectious disease such as smallpox, this requires that Massachusetts be prepared to implement the national plan at the state level. Smallpox used as a biological weapon would not be restricted to the time and place of the attack. Because of its insidious characteristics and highly infectious nature, over time the smallpox virus could, unless quarantine and restrictive measures were enacted rapidly, infect individuals unknowingly who may travel and in turn infect other unsuspecting victims, thereby expanding the geographic footprint of the disease exponentially. Biological weapons also present grave difficulties because local law and health officials may not know immediately that an attack has taken place, thus giving the infectious agent even greater opportunity to spread.

Radiological weapons, often referred to as “dirty bombs,” are a combination of radioactive mate-

rial with conventional explosives. These weapons have the capability of broadly spreading radioactive material causing disruption and public hysteria, most notably within densely populated metropolitan areas.

Depending on their size, nuclear weapons are the most lethal of all CBRN weapons because of their capability to kill large numbers of people and to destroy infrastructure. Acquisition of nuclear weapons by a terrorist organization is becoming increasingly possible in the porous global technology-transfer setting of the early twenty-first century. If the components for a nuclear device, or even the assembled weapon itself, could be obtained on the world market, a terrorist organization would have at its disposal a capability with vast destructive potential with which either to threaten devastation, for example, by blackmail or actually use against high-value targets.

Conventional Means of Attack

While planning to counter and respond to WMD attacks must be given high priority, the Commonwealth must at the same time prepare for attacks by conventional means. These might include explosives such as those used in the Oklahoma City Federal Building bombing or in the car bombings against U.S. embassies in Tanzania and Kenya. To date, the overwhelming majority of terrorist incidents were carried out with easily obtained conventional weapons including high explosives, guns, and knives. Due to their ready availability and minimal costs, it is highly likely that terrorists will continue to employ such weapons even as they seek to acquire more lethal capabilities, including WMD.

The Cyberspace Infrastructure

The threat of cyber attacks is of great concern to the Commonwealth and its economy. Cyberspace connects a “network of networks” that directly support all major sectors of our economy. This includes rail, air, and seaports, as well as finance and banking, information and telecommunications, public health, emergency services, water, energy, food, and the defense-industrial base. Since our economy depends on

interconnected networks that are responsible for the daily transfer of billions of dollars in transactions and messages sent electronically, the threat of cyber attacks has become a serious concern. A terrorist organization seeking to cause widespread disruption of infrastructure services and generate public fear will increasingly attempt to do so by learning the vulnerabilities of key cyberspace nodes and then attacking them. Because of its position at the forefront of the information age, Massachusetts represents a cyber-terrorist target of potentially great importance.

Attacks on Critical Infrastructure

Protecting the Commonwealth's critical infrastructure from cyber attack or from terrorist attacks by other means is a daunting challenge. Our critical infrastructure comprises a diverse set of assets encompassing airports, sea and water ports, nuclear facilities, dams, water and sewer plants, electric power plants, gas pipelines, bridges, and other key facilities such as hospitals that offer an almost endless list of potential targets. Deterring terrorist attacks or reducing the likelihood of such attacks on Massachusetts will require the combined efforts of federal, state and local authorities. States must develop an inventory of the most vulnerable critical infrastructure nodes in tandem with the implementation of specific security procedures designed to protect them. The Commonwealth has completed such an effort as part of its response to 9/11. Because resources to protect such critical infrastructure are finite, the Commonwealth will need to assess on a continuing basis the levels and types of protection to be given to specific infrastructure. This document addresses issues of prioritization as we take necessary steps to protect critical Commonwealth infrastructure from the threat of terrorism.

Division of Responsibilities within Homeland Security

Because federal, state, and local governments have a shared responsibility in homeland security, a key challenge is to develop an efficient structure where duplication of resources is min-

imized and essential security requirements are met. Given that the threat of terrorism is diverse and complex, national, state, and local policymakers must formulate strategies with an understanding of the various interests, capacity, and challenges they confront. A greater understanding of these issues will help promote the streamlining and coordination of federal, state, and local efforts.

Since terrorist acts are local events, the initial responsibility for action rests with first-responders organizations such as the police, fire departments, emergency medical personnel, and public health agencies. State and local governments have the responsibility of maintaining first-responder capabilities, including providing adequate funding levels. This is becoming increasingly onerous at a time of budget cuts and deficits. At the same time, the extraordinary circumstances resulting from 9/11 create requirements for new capabilities that may only be adequately met with greater federal assistance.

Steps Taken by the Commonwealth to Increase Post-9/11 Security

Since 9/11, the Commonwealth has taken numerous and wide-ranging measures to strengthen security against terrorism. The list set forth below summarizes some of these measures. It provides a basis for assessing what has been done as a necessary step in identifying other strategic initiatives that will be required.

Creation of the Office of Commonwealth Security

The Office of Commonwealth Security (OCS) was created in the aftermath of 9/11 to coordinate efforts and to increase security within the Commonwealth against terrorist and associated threats. OCS interacts and coordinates its activities with a variety of state agencies that play a key role in the Commonwealth's efforts to combat terrorism. These agencies include the Executive Office of Public Safety (EOPS), the State Police, Massachusetts Emergency Management Agency (MEMA), Fire Services, and the National Guard. OCS has also formed close

working relations with the Secretary of Transportation and Construction, the Department of Public Health, the Secretary of Environmental Affairs, and various other state and local authorities. OCS is also an active member of the Anti-Terrorism Task Force (ATTF) established by the United States Attorney's office in Boston. In addition, OCS is the state's official liaison with the newly created federal Department of Homeland Security as well as with a number of other federal agencies.

OCS has established a Bioterrorism Coordinating Council comprised of a six-member panel of leading medical doctors and scientists charged with developing a comprehensive strategy to protect the Commonwealth in the event of a bioterrorism attack. In addition, OCS has created and implemented a Threat Alert System, which is a set of guidelines that have been developed for the private sector and for all agencies and departments in the Commonwealth in the event of an emergency or terrorist related incident.

Moreover, OCS has worked with the U.S. Coast Guard in securing the Port of Boston through the creation of the steering committee "Operation Safe Commerce-Boston." This steering committee, represented by a coalition of federal, state, and local agencies along with the private sector, has worked to enhance port and transportation security while facilitating commerce. It is focusing on key issues such as enhanced dissemination of intelligence and information sharing, cargo container security, flammable/dangerous cargo such as liquefied natural gas (LNG), cruise ship security, and emergency management. The two key issues that are the present object of attention are enhanced dissemination of intelligence and information sharing and emergency management.

OCS also helped to develop several post-9/11 legal initiatives regarding terrorism and enhanced Commonwealth security for consideration by the State Legislature. The first round of legislation won strong bipartisan support and was enacted. A second round is currently pending. These legal initiatives are described in greater detail below. Moreover, OCS developed this *Strategic Plan for Safeguarding the Com-*

monwealth of Massachusetts Against Terrorist and Related Threats.

Finally, OCS, together with the United States Attorney's Office, the FBI, and the Massachusetts Attorney General's office, has initiated an Outreach Program with the state's Islamic and Muslim community. The purpose of the Outreach Program is to establish a forum for communication. A major goal of the program is to reassure the Islamic/Muslim community that their basic civil liberties will be safeguarded, not sacrificed as our Nation wages the war on terrorism and seeks to bring Al Qaeda, the Islamic terrorist group responsible for September 11, to justice.

Coordination among Federal, Commonwealth, and Local Organizations

In the aftermath of September 11, the law enforcement communities, together with emergency management agencies and other local organizations, have worked together in unprecedented fashion in the fight against terrorism. These groups have been required to play a more significant role in safeguarding both the Commonwealth and the Nation as a whole. Therefore, it has been necessary for these agencies and committees to assume new and expanded responsibilities, coordinate across jurisdictional boundaries and collaborate with each other in order to prevent, disrupt, and prepare for the possibility of future terrorist attacks. Overall, greater cooperation and lines of communication have been formed despite diverse organizational cultures and organizational priorities.

In addition, the 9/11 attacks have led to new thinking about how federal, state, and local law enforcement agencies go about their business. In order for the federal government to utilize the capabilities of state and local law enforcement agencies to prevent further terrorist attacks, increased intelligence sharing is vital. The creation of the Anti-Terrorism Task Force (ATTF) by the U.S. Attorney in Boston following 9/11, as well as increased communication by the members of the existing FBI-led Joint Terrorism Task Force (JTTF), has led to greater coordination among federal, state, and local

law enforcement agencies. Finally, the Commonwealth's Executive Office of Public Safety has developed the Statewide Anti-Terrorism Unified Response Network or SATURN (more below) to provide information sharing and terrorist training for first responders throughout the state.

Increased Security Measures

The Commonwealth has greatly increased security at Logan International Airport, the ports, the Massachusetts Bay Transit Authority, public and federal buildings, nuclear power plants, electric power plants, water supplies, and other important critical infrastructure nodes. The United States Coast Guard, working with the Office of Commonwealth Security and other state and private entities, has enhanced security and helped to make the port of Boston a model for the Nation. The Massachusetts State Police have provided additional on-site protection to many of the critical infrastructure nodes across the Commonwealth. Officers are being trained in both WMD scenarios and in combating terrorism. In addition, the State Police has created and staffed its own Anti-Terrorism Unit (ATU). The ATU is a ten-member element within the Criminal Information Section of the State Police. The creation of the ATU has doubled State Police resources dedicated to collecting and disseminating intelligence.

The Massachusetts Emergency Management Agency (MEMA) has been responsible for increasing the number of training courses and the planning and organization of seminars, workshops, and conferences available to state, local, and volunteer agencies, as well as to official and public safety personnel throughout the Commonwealth. Since 9/11, MEMA has conducted a rigorous training program in the area of hazardous materials (HAZMAT), terrorism awareness, radiological incidents, chemical stockpile emergency preparedness, HAZMAT/WMD awareness for hospitals, and debris management.

Aviation Security and Logan International Airport have been studied and analyzed by the Massachusetts Port Authority (MASSPORT) and the Executive Office of Transportation and Con-

struction which have bolstered security at all airports throughout the state. The increased inspection of baggage, passengers, and airline and airport personnel along with greater protection for the various airport facilities has greatly increased security within the aviation industry found in the Commonwealth. In keeping with federal requirements, all checked baggage placed on commercial flights must be screened for explosives by December 31, 2002. MASSPORT, responsible for Boston's Logan International Airport, not only accomplished this task but completed it well before the official deadline.

The Statewide Anti-Terrorism Unified Response Network (SATURN) was created by the Executive Office of Public Safety. It is designed for information sharing and training first responders for terrorist incidents. The training provided through SATURN is cross-disciplinary, which enhances the ability of all public safety and public health services in Massachusetts to work together as would be required during a time of crisis. By including fire, police, and emergency management departments throughout all 351 cities and towns in the Commonwealth, SATURN is designed to foster compatible and complementary approaches to the myriad of first responder, preparedness, and terrorist-related issues confronting the state's safety, emergency response, and law enforcement officials.

The Massachusetts Department of Public Health (MDPH) has strengthened the state's infectious disease surveillance program by establishing a functional reporting mechanism called the Boston Emergency Department Volume Surveillance System where eleven hospitals in the greater Boston metropolitan area report at the end of the day to the Department of Public Health on its patient volume. This reporting allows for electronic and human surveillance of potential infectious disease outbreaks. MDPH hopes to expand this system eventually to include all of Massachusetts. Additionally the MDPH is developing readiness assessments and hospital preparedness plans, and enhancing its laboratory and communication capacities.

The Massachusetts Threat Alert System was placed in operation by the Commonwealth after 9/11. This is a set of guidelines that have been developed for all agencies and departments in the Commonwealth in the event of an emergency or terrorist related incident. While providing a common basis for alerting departments and agencies, in addition to cities and towns as well as private-sector entities, this system leaves to these groups sufficient latitude to formulate specific responses as alert levels change.

The Executive Office of Transportation and Construction (EOTC) is responsible for the planning, management, supervision, design, construction, and maintenance of public transit services, general aviation programs, and the highway network operated in the Commonwealth by the agencies and authorities under and within its jurisdiction. It is comprised of the Massachusetts Bay Transit Authority (MBTA), the Massachusetts Highway Department, and the Massachusetts Aeronautics Commission.

Since September 11, EOTC has increased the number of inspectors who regularly check the bridges throughout the Commonwealth. It has also prepositioned equipment throughout the state for speedier restoration of services after a possible terrorist attack. The Highway Department has also constructed an operations and command control center that is staffed around the clock. The MBTA has beefed-up security throughout its subway and transportation system, adding additional security personnel and MBTA police.

The Aeronautics Commission is responsible for all general aviation Commonwealth airports with exception of Logan International and Hanscom airports which are under the direction of MASSPORT. The Commission has completed a statewide badge identification program for airport workers, staff, and aircraft owners. It is the first identification program in the nation for private airports. A number of these airports have also erected security fences to prevent unauthorized access to facilities and aircraft.

The Massachusetts Environmental Police, part of the Department of Fisheries, Wildlife and Environmental Law Enforcement, has worked with fed-

eral, state, and local entities to augment Commonwealth security against terrorism. For example, the Water Patrol unit of the Environmental Police, working with the U.S. Coast Guard, provided additional security to protect Boston Harbor in the immediate aftermath of September 11. Moreover, the Environmental Police provide personnel to buttress security at such locations as reservoirs, hunting and fishing areas, as well as at rivers and ports throughout the state.

The Boston Police Department, utilizing technology provided by the Defense Threat Reduction Agency, part of the U.S. Department of Defense, is developing a computer software modeling and analysis program that will enhance the city's emergency preparedness and response to a major terrorist incident including the possible use of WMDs. The models will provide information on the area and population affected as well as identify key emergency management assets located in the immediate vicinity of the incident.

The Massachusetts Water Resources Agency (MWRA) has made many improvements to the security of the water supply of Central and Eastern Massachusetts. The MWRA has begun the process of building new covered storage tanks to replace all open water reservoirs and has greatly impeded access to underground aqueducts feeding water into the greater Boston metropolitan area. Water-monitoring facilities and mobile decontamination units increase the preparedness for a quick response to combat any hazardous situation.

The New England Gas Association (NEGA) is a regional trade association representing natural gas distribution companies, transmission companies, and liquefied natural gas suppliers. Since 9/11, officials from the Commonwealth have met regularly with NEGA and with many of its more than 260 associate member companies to coordinate security activities and procedures. To date, security overall has improved dramatically at all facilities and productive working relationships between agencies such as MEMA, the State Police, the Department of Fire Services, and the U.S. Coast Guard have been fostered and expanded with

NEGA and its member firms. Two key goals of these efforts are to ensure the safety of gas supply and transport and to make certain that gas/fuel supplies can be restored rapidly in the event of a terrorist incident.

National Grid USA. Commonwealth officials have also met on a regular basis to coordinate security efforts with officials at National Grid USA which transmits and distributes electricity throughout Massachusetts. As a result, National Grid officials have instituted several measures specifically designed to protect the electric power infrastructure and to restore service quickly if interrupted.

Legislative Initiatives

The threat of terrorism has focused attention on the need to develop and enact legislation to protect the Commonwealth. The following is a summary of priority legislation related to homeland security and terrorism that has been passed by the State Legislature and enacted into law in Massachusetts:

- *An Act Relative to the Possession, Transport, Use or Placement of a Hoax Substance.* This law makes it a felony to threaten to use a fake or hoax substance to cause anxiety and fear. It builds on previous legislation making it a crime actually to use a “hoax device.”
- *An Act Relative to Possession of Dangerous Weapons and other Devices at Airport Security Checkpoints and Within Secure Areas.* This law makes it a felony to enter or attempt to enter through an airport security checkpoint or a secure area within an airport with a firearm, dangerous weapon, or knife.
- *An Act Limiting Access to Public Records pertaining to Commonwealth Security and Infrastructure.* This law exempts certain records from being classified as public records, including information pertaining to threat assessments, security plans, and structural documents depicting critical infrastructure of buildings, for example, whose detailed blueprints and other information could assist terrorists in planning and carrying out devastating attacks.

- *An Act Establishing the Crime of Selling Explosives to Unauthorized Persons.* This law expands the authority of the State Fire Marshal by requiring permits from the Fire Marshal for all buildings or structures used to manufacture or store explosives. In addition, the legislation makes it a crime for a person to sell or transfer explosive materials to unauthorized individuals or to individuals who do not have permitted facilities to store such materials.
- *An Act Criminalizing the Use or Possession of a Biological or Chemical Weapon.* This law makes it a state law crime to possess, transport, use or place any biological, chemical, radioactive or other substance that is capable of causing death, serious bodily injury, or significant property damage with the intent to injure or kill any person or to destroy or damage property, punishable by up to 20 years in state prison.
- *An Act Relative to Communicating a Terrorist Threat.* This law increases penalties under current law for communicating threats in various media involving certain types of structures.

Currently, there is a second round of legislation that has yet to be enacted. These bills include such issues as maritime security, money laundering, computer hacking, statewide grand jury, defining the crime of terrorism, bioterrorism and emergency powers, wire tapping, the tagging of explosives, and a forfeiture statute to include anti-terrorism.

II

Preventing Terrorist Attacks

The previous section of this document assessed the threat to the Commonwealth, together with our major points of vulnerability. As discussed, we confront the potential for terrorist action that includes biological, chemical, nuclear, or radiological weapons or conventional explosives. The potential delivery systems encompass trucks, automobiles, commercial aircraft, ships, missiles, or even suicide bombers. As a means of attack, terrorism must be viewed as a flexible political instrument that requires agility of thought and flexibility on the part of those who would prevent such attacks.

Organizing for Commonwealth Security

If terrorist attacks are to be prevented, our strategy must be focused at each of the levels of government and, to the extent possible, between the public and private sectors. The United States Constitution confers on the states all authority not specifically granted to the federal government. Within the U.S. structure there are overlapping federal, state, and local authorities and jurisdictions. How to focus, coordinate, and, where necessary, integrate the efforts of these elements of governance is a formidable challenge but nevertheless an essential task if we are to prevent future acts of terror.

Although the responsibility for preparing for and responding to a terrorist attack is shared

by the federal, state, and local governments, the state and local authorities will be the first responders to a terrorist incident. As we organize against the threat of terrorism, relevant federal, state, and local government agencies should develop complementary systems that minimize duplication and ensure that essential requirements are met. Specifically, this includes cooperation in the areas of law enforcement and prevention, emergency response and recovery, policy development and implementation.

Law Enforcement and Prevention

Federal, state, and local law enforcement agencies must build strong working relationships with one another to enhance collaboration and cooperation. The lack of a working relationship and the absence of trust that an established re-

lationship represents impedes the steady flow of intelligence that will be indispensable to prevent future terrorist attacks. Past domestic counterterrorism law enforcement activities have been sometimes hampered by the failure of timely intelligence to reach the appropriate users when it was needed. “Stove piping” and deficiencies in information sharing have restricted intra-governmental law enforcement cooperation, planning, and response capabilities. The new mindset required for the new post-9/11 era includes a greater commitment to share information and intelligence data if we are to deter and prevent terrorism and apprehend the perpetrators of terrorist acts.

While it will take some time to understand and benefit fully from the lessons of 9/11, important steps have already been taken to create additional information-sharing capabilities, such as the aforementioned SATURN network. The Commonwealth must build upon these efforts to provide timely and relevant information. Key to success will be the extent to which barriers that have impeded the flow of intelligence can be removed.

Although much remains to be done, there have been significant areas of progress since 9/11. The White House Office of Homeland Security is establishing a “network of networks” that will allow information to be shared across government agencies and between the various levels of government. This information architecture is being developed with the goal of balancing security with privacy, building databases that can be updated, and creating an unclassified network that will be available to the first responder community. Information technology systems that support the requirements for Commonwealth homeland security will have to draw from a variety of disparate and sometimes antiquated databases. Contributors to, and users of, such databases include the law enforcement, immigration, customs, intelligence, and biomedical communities.

Recognizing that much of the information likely to be available will come from the federal level, the Commonwealth must assure that information is rapidly disseminated and shared at the state and local levels. This requires an ad-

vance understanding of who needs to receive such information and how to think about information that is received. For example, the new post-9/11 mindset requires thought patterns that can help identify trend lines and patterns. An incident in another jurisdiction, inside or outside the Commonwealth, that would not have been of concern pre-9/11 may be part of a broader pattern. The admission of patients having particular symptoms to an emergency room in one part of the Commonwealth or outside the state may signal a similar outbreak elsewhere. Local and state officials, as well as those in the private sector dealing with Commonwealth security, must be alert to possible trends and patterns that can serve as alarm signals of impending danger. It is axiomatic that good intelligence is the prerequisite for effective strategies at all phases of terrorist activity. Equally important, however, is an ability to discern as early as possible how seemingly discrete events may be related to each other as indicators of broader patterns of activity.

Emergency Response and Recovery

However broad their implications and ramifications, terrorist incidents are also events for which the initial response is local, just as local responders will be the last to leave the scene. Like other states, the Commonwealth, and in particular the Massachusetts Emergency Management Agency (MEMA), has long had in place capabilities for response to natural disasters such as hurricanes and blizzards, as well as floods and fires. The effect of 9/11 is to heighten awareness of needs for emergency response capabilities in new areas such as the use of a weapon of mass destruction. While our hospitals have always been available to accommodate the needs of victims of natural disaster, we must think anew about our requirements in the event of a 9/11-type terrorist attack or another type of catastrophic event such as the use of a biological or nuclear weapon that would place unprecedented demands on our emergency response and recovery capabilities.

Such resources include responder personnel as well as infrastructure. They encompass detection capabilities and protective equipment, as

well as decontamination and the ability to communicate among responders who have previously had little or no occasion to work together. Emergency response and recovery – what is termed consequence management – places a premium on cooperation that can best be facilitated by advance planning and training, of which there have been extensive efforts at the state and local levels since 9/11, although this will be a continuing and evolving requirement. For example, planning is under way by MEMA and the Department of Fire Services (DFS) to place a decontamination trailer with necessary equipment in every community that has a hospital. A memorandum of understanding has been signed between the State National Guard Civilian Support Team and DFS on general principles and procedures for working together.

Emergency response and recovery inevitably draw on local resources. Among the lessons of 9/11, however, is the possibility that the scale of devastation will be far greater than previously envisaged. This means that the local authorities will need outside help from other parts of the Commonwealth or from outside the state. This may include firefighting equipment or medical personnel made available by a neighboring jurisdiction in time of need, or resources that can best be provided according to a federal plan such as vaccines or antidotes to be drawn from a national stockpile in times of emergency.

Policy Development and Implementation

The events of 9/11 have resulted in a host of new policy requirements that call forth a need for new organizational arrangements and relationships. Commonwealth security presents numerous requirements that, as this document points out, can best be met as a result of concerted federal, state, and local action. Numerous governmental departments and agencies that have not previously had to work closely together have new roles to play in supporting Commonwealth security. At the highest level the need exists for integrated policy development and implementation based on the leadership provided by the Governor and other officials.

Simulations, Tabletop Exercises, and Other Practice Drills

The use of tabletop simulations, drills, and interagency exercises has become vitally important in preparing to deal with a terrorist attack. These tools allow first responders and their agencies to become familiar with emergency plans, the equipment to be used, and the needed skills to get the job done. Such exercises can help identify gaps in planning and resources. They can also provide valuable lessons in how to work together most effectively on the part of those who have primary responsibilities in the event of a terrorist attack.

Several of these exercises have been conducted in the Commonwealth since 9/11. They include the November 2002 tabletop exercise “Operation Prometheus,” held within the greater Boston metropolitan area. This exercise enabled the National Guard, the Executive Office of Public Safety, the Massachusetts Emergency Management Agency, the Emergency Medical Service, Fire Services, State Police, and many other emergency management and law enforcement agencies to participate in a bioterrorist-related exercise to help strengthen the Commonwealth’s capabilities. Other such exercises will need to be organized as we continue to develop, test, and evaluate the Commonwealth’s ability to cope with a terrorist attack.

The Citizens of the Commonwealth

Although the Commonwealth has an obligation to work with the public and private sectors to provide for security, the role of its citizens is of crucial importance. The events of 9/11, the anthrax attacks, and the fear of future incidents have made the people of Massachusetts more vigilant, informed, and eager to help defend against attack and to win the war on terrorism. This increased vigilance may be illustrated by the following examples: commercial fishermen working alongside the Coast Guard in watching for suspicious maritime activities, or hunters, snowmobilers, birdwatchers, and hikers alerting the Massachusetts Environmental Police on suspect or out-of-the ordinary behavior. This contribution to the Commonwealth’s security is often forgotten or easily

overlooked. Nevertheless, many state and local law enforcement and emergency management agencies are working hard at creating efficient public outreach programs to expand their information-gathering sources.

The Private Sector

The private sector supplies the bulk of our goods and services. It is also a valuable source of ideas, concepts, and technologies that should be tapped to fight the war on terrorism. Moreover, since most of the infrastructure in Massachusetts is privately owned and operated, the Commonwealth must work in close conjunction with the private sector to identify vulnerabilities to critical infrastructure nodes that are spread across the state. Such a cooperative partnership with the Commonwealth is both an example of the private sector's good citizenship as well as a reflection of sound corporate business practice designed to protect a company's assets and thus to contribute a sustained effort to prevent terrorist attack against the Commonwealth and its citizens.

Critical Mission Areas

Reducing the Commonwealth's Vulnerabilities

Intelligence and Warning

Terrorists have the ability to strike at any place, at any time, and with a wide variety of weapons. They depend on surprise to carry out their missions. Just as the attack on Pearl Harbor demonstrated shortfalls in U.S. intelligence and warning, the September 11 attacks on the Pentagon and World Trade Center once again pointed up deficiencies that must be addressed if we are to deter, preempt, prevent, and protect the Nation from another surprise terrorist attack.

Since 9/11, how to strengthen the capabilities of the various federal, state, and local agencies to gather and communicate actionable intelligence has been widely discussed. Protecting the Commonwealth is a daunting challenge if terrorists can choose the time, place, and method of attack as they assess our vulnerabilities. Therefore, timely and relevant information is one of our most valuable resources. Good intelligence is the cornerstone of a strategy for Commonwealth security. The federal,

state, and local law enforcement and private sector agencies must efficiently collect, use, and share intelligence in order to win in the war against terrorism.

Enhance Intelligence Cooperation

Cooperation between the federal, state, and local governments must occur both horizontally (within each level of government) and vertically (among various levels of government). “Stove piping” and deficiencies in information sharing severely complicate interagency cooperation, planning, and response capabilities. Credible threat information needs to reach local authorities in time to be utilized to deter, prevent, or respond to a terrorist action.

There are many government departments and agencies on the federal level that support homeland security as part of their overall mission. Such entities must be able to work in close cooperation with state and local authorities in ways that were not envisaged before 9/11. For

instance, the U.S. Attorney General, as the chief law enforcement officer, currently leads the effort to detect, prevent, and investigate terrorist activity within our Nation. The U.S. Attorney General's September 17, 2001 directive to create the Anti-Terrorism Task Force (ATTF), allowed for streamlining the collection, analysis, and timely distribution of threat information to improve response capabilities within each state. The Anti-Terrorism Task Force has begun to foster a close working relationship between local, state, and federal law enforcement agencies.

Since 9/11, the Centers for Disease Control and Prevention and the National Institutes of Health, both part of the Department of Health and Human Services, have provided essential expertise and resources related to bioterrorism to each of the fifty states. In particular, the Centers for Disease Control has worked with the Massachusetts Department of Public Health in bolstering the effectiveness of the state's laboratory facilities and has provided funding to help the Commonwealth create an infectious disease surveillance system. The expertise and information shared with the Commonwealth allows for a greatly improved warning system.

Other federal entities have significant counterterrorism intelligence responsibilities, including the CIA's Counterterrorist Center and the FBI's Counterterrorism Division and Criminal Intelligence Section. The nature of the terrorist threat facing the Commonwealth requires new working relationships at all intelligence levels.

The Sharing of Threat Information

The Nation's intelligence agencies have begun to make necessary adjustments to help facilitate increased needs for homeland security by working with state and local authorities. In the past, law enforcement and intelligence agencies have not always shared information due to legal and cultural barriers between the agencies. A steady flow of intelligence is needed to prevent future terrorist attacks. Compartmentalization and deficiencies in information sharing severely complicate intergovernmental law enforce-

ment cooperation, planning, and response capabilities. Since 9/11, however, the flow of information and intelligence between the federal government and the state and local agencies of the Commonwealth has greatly improved.

In particular, the Office of Commonwealth Security has developed cooperative relationships with the various federal law enforcement and emergency management agencies. Moreover, throughout the various agencies within the Commonwealth, new cooperative relationships have developed since 9/11. There has been an increased flow of information and intelligence within the Commonwealth and with the federal government. The development of new professional relationships has enabled federal, state, and local law enforcement agencies to share timely and relevant information in unprecedented ways even though continuing efforts toward further improvement and streamlining will undoubtedly be needed.

Federal Threat Alert System

The creation of the Homeland Security Advisory System in March 2002 provides a comprehensive and effective means to disseminate information regarding the risk of terrorist attacks to federal, state, and local authorities and most importantly, to the American people. This five-stage, color-coded, terrorism-warning system creates a common framework for characterizing the nature and level of threat and appropriate measures that should be taken in response. It is a national framework that is flexible enough to apply to threats made against a state, city, town, industry, or company. The common vocabulary used to describe each threat allows for easier communication within and outside government. Currently, the U.S. Attorney General, in conjunction with the Department of Homeland Security, is responsible for developing, implementing and managing the system.

The Advisory System also provides a national framework for public announcements of threat advisories and alerts to notify law enforcement and state and local government officials of threats. Prior to the creation of the Advisory System, all threats were treated as equal. All alerts have a different response. The Advi-

sory System provides a basis for establishing a threat level that can be translated into alert requirements. This allows for federal, state, and local governments to know more fully what to communicate to their citizens and what are the appropriate actions to be taken. The System also informs the public about government preparations against terrorism, and provides the public with the information necessary to go about their daily lives with knowledge of the threat at hand. Moreover, the Advisory System characterizes appropriate levels of vigilance, preparedness, and readiness within its five-stage, color-coded graduated threat conditions. Each threat condition has corresponding suggested measures to be taken in response. Such responses include increasing surveillance of critical locations, preparing to execute contingency procedures, and closing public and government facilities.

The Massachusetts Threat Alert System provides state-level guidelines for use in the event of an emergency or terrorist related incident. While establishing a common alert basis, this system leaves sufficient latitude to formulate specific responses as alert levels change. Threat information is disseminated from the federal to the state and then to local public safety agencies and to private sector owners of key targets within the Commonwealth. The Office of Commonwealth Security coordinates the Massachusetts Threat Alert System with the Homeland Security Advisory System in order to provide the necessary threat warnings. Massachusetts law enforcement, emergency management, and private agencies follow the same alert framework to diminish confusion.

Vulnerability Assessments

Vulnerability assessments are a necessary part of intelligence in combating terrorism. The Commonwealth has begun the process of comprehensive vulnerability assessments of all the state's critical infrastructure nodes and key assets to complement the federal government's efforts. Such vulnerability assessments can provide federal, state, and local authorities a working knowledge of potential targets and their vulnerabilities. This knowledge

could enhance the prospects for allocating resources needed both to protect the infrastructure and for restoring a facility that was the object of terrorist attack. To begin developing these assessments, the Commonwealth should employ "red team" techniques in order to view state and local level critical infrastructure and key assets from a terrorist's perspective in order to understand more fully the methods, means, and targets of terrorists and help anticipate, prevent and prepare for emerging threats and vulnerabilities.

Transportation Security

Transportation presents one of the largest potential vulnerabilities and challenges to the Commonwealth. The state's transportation network encompasses seaports, airports, highways, pipelines, railroads, and waterways that move people and goods. Such infrastructure must be protected to ensure the reliable flow of goods and services and prevent terrorists from using our transportation assets to enter the United States or to perpetrate a terrorist action.

The federal government is currently working with both the Commonwealth and the private sector to upgrade security in all modes of transportation. The areas of emphasis have included: commercial aviation and road/highway/interstate systems; transportation of hazardous and explosive materials; protection of national airspace; shipping container security; traffic-management systems; transportation operators and workers; linkages with international transportation systems; and information sharing. The federal government is also utilizing existing relationships (the aforementioned Operation Safe Commerce Boston) and systems to implement unified national standards for transportation security.

As we increase transportation security, the risk that the flow of commerce will be inhibited arises. For example, the increased security due to 9/11 resulted in a 15-20 mile traffic backup on the Canadian border. After four days of such delays, automakers complained that security was having adverse economic effects on production that takes place both in Canada and the United States, with large numbers

of people moving across the border on a daily basis. Given the sheer volume of trans-border trade and movement of people, the process of verifying and processing entry into the United States in order to stop terrorists or smuggled goods is a complex task that requires time, patience, and innovative approaches, including “smart borders” and other steps to facilitate entry based on the willingness of frequent users and travelers to undergo special background and other investigations. Therefore it is necessary for the state to balance competing security and economic requirements. This could be achieved by increasing the amount of information available on inbound goods and passengers entering the Commonwealth from overseas and by creating “smart borders.”

Private industry faces competing requirements to invest in security enhancements to hedge against the risk of a disruptive attack without jeopardizing competitiveness or hampering the flow of commerce and people. Together, government and industry should work to develop and deploy non-intrusive inspection technologies to ensure rapid and more thorough screening. The Commonwealth has employed additional mobile x-ray trucks to help screen international shipping containers. The Commonwealth has worked with the United States Coast Guard, U.S. Customs Service, and Border Patrol to secure port facilities within the state and protect the docking of liquefied natural gas (LNG) tankers that supply the Commonwealth with energy. Moreover, the new office of Transportation Security Administration (TSA) has assumed the responsibility from the Federal Aviation Agency for aviation security as well as the security of all transportation modes under the jurisdiction of the Department of Transportation. The TSA took on the ambitious program of federalizing and giving new training to all screening workers and requiring that all checked baggage placed on commercial flights must be screened for explosives. The Massachusetts Port Authority has worked with the TSA in overseeing security at Logan International Airport.

Domestic Counterterrorism

The terrorist attacks of 9/11 redefined the missions, roles, and responsibilities of federal, state, and local law enforcement authorities to focus more extensively on counterterrorism issues. While it has been necessary to assign priority to preventing terrorism, pre-9/11 responsibilities remain important as well. Law enforcement agencies have been called upon to fight terrorism while they continue to work in their traditional areas of responsibility – and often to do so without major additional resources.

Enabling law enforcement agencies to focus on older *and* newer priorities requires numerous changes in approach, organization, training and capabilities as set forth throughout this document. Many improvements have already been made in the Commonwealth, but much more needs to be done to strengthen domestic counterterrorism capabilities. Cooperation among federal, state, and local law enforcement agencies, together with the increased flow of intelligence among them, is essential. The improvement of post-9/11 communication among these agencies has produced greater coordination of domestic counterterrorism efforts.

Despite the progress being made within the areas of intelligence sharing and cooperation, there remain weaknesses in domestic counterterrorism efforts. The ability to identify and monitor terrorist funding is still inadequate. Therefore, the Commonwealth should continue to strengthen its efforts in information sharing and coordination while assisting the federal government, when possible, to identify sources of terrorist funding by providing information to the FBI’s Financial Review Group, which investigates suspicious financial transactions, and to the Custom Service’s Operation Green Quest, which freezes terrorists’ accounts and seizes assets of individuals and organizations involved in terrorism.

The Commonwealth should also work with the federal government to help increase information sharing with the state and local levels through the FBI-led Joint Terrorism Task Force (JTTF), which is the investigative arm of the ATTF, in order to build and continual-

ly update a fully integrated, accessible terrorist watch list. To facilitate two-way information sharing (federal to state as well as state to federal), the Commonwealth should help the Department of Justice, when possible, expand and maintain the FBI's National Crime Information Center (NCIC) database that is accessible to approximately 650,000 state and local law enforcement officers, enhance the FBI's consolidated Terrorism Watch List, expand the FBI's Integrated Automated Fingerprint Identification System, and lastly, help uncover and report unusual behavior and security anomalies to federal law enforcement authorities.

To date, the Commonwealth has begun to provide information to these federal programs by working through the Anti-Terrorism Task Force in Boston. The ATTF has begun to establish a long-term, sustained, multi-agency, and multi-jurisdictional law enforcement collaboration at the federal, state, and local level to maximize the Commonwealth's counterterrorism efforts of detecting, tracking, and apprehending potential terrorists.

Finally, the use of "red team" exercises to anticipate terrorist actions will provide useful knowledge for both the federal, state, and local law enforcement and emergency management agencies in preparing for a terrorist attack. Employing various law enforcement personnel to act and think like terrorists to carry out "mock" terrorist attacks against critical infrastructure nodes tests response capabilities of governmental and private-sector agencies. The use of comprehensive intelligence and information about a known terrorist group also allows "red teaming" to help predict the methods, means, and targets of terrorists. This knowledge contributes to efforts to anticipate, prevent, and prepare for emerging threats and vulnerabilities. The Commonwealth has begun to employ "red team" exercises to assess the vulnerabilities and protection needs of various critical infrastructure nodes and key assets, such as the port of Boston or Logan International Airport. This effort will need not only to be continued but also augmented in light of the strategies, tactics, and capabilities likely to be available to terrorists.

Protecting Critical Infrastructure and Key Assets in the Commonwealth

Crucially important to reducing the Commonwealth's vulnerabilities is the protection of its infrastructure. This was immediately recognized after 9/11. The Massachusetts State Police prepared a directory of critical public and private infrastructure. The USA PATRIOT Act, signed into law by President Bush in October 2001, defines critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The *National Strategy for Homeland Security* defines key assets as "individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage morale or confidence." Key assets include symbols or historical sites and monuments, and high profile events such as concerts or sporting events. As noted elsewhere in this document, the Nation's critical infrastructure includes the public and private sectors. Agriculture, food, and water, along with the public health and emergency services, are essential to our survival and well being. Other critical infrastructure, such as sea-ports, airports, and communications systems, are vital to our economy. Governmental infrastructure protects our national security and freedom.

Because resources for the protection of critical infrastructure and key assets are limited, it is essential for strategic planning that criteria and procedures for identifying priorities be developed. As already noted, based on publicly available intelligence, the organizers of terrorist acts such as those of 9/11 have identified essentially three categories of targets. The first consists of targets of largely *symbolic* value. These could include monuments and public buildings. The second category comprises *infrastructure*, such as transportation systems or skyscrapers, having great economic *and* symbolic value, but also having the potential to kill

large numbers of our population. Such congregations of people who come together for a sporting event or meet in other public settings constitute *human targets* from the terrorist's perspective. As in 9/11, terrorists often attempt to kill or injure as large a number of people as possible. The human category also includes influential public figures who could be attacked in terrorist operations.

Based on intelligence about potential targets drawn from terrorist sources such as those that have become available since September 11, the Commonwealth should develop an approach to protecting critical assets that utilizes a risk-management model. Such an approach has been outlined by the National Infrastructure Protection Center in a document entitled *Risk Management: An Essential Guide to Protecting Critical Assets*, issued in 2002. Its essential elements should be part of the Commonwealth's approach to protecting critical infrastructure. Specifically, this approach provides for an effort that:

- Identifies weaknesses in an organization or system, such as a water system, electric power grid, or buildings
- Offers a rational method for making decisions about the expenditure of scarce resources and the selection of cost-effective countermeasures to protect valuable assets
- Improves the success rate of an organization's security efforts by emphasizing the communication of risks and recommendations to the final decision-making authority
- Helps security professionals and key decision-makers answer the question: "How much security is enough?"

The National Infrastructure Protection Center sets forth a five-step risk model that not only assesses assets, threats, and vulnerabilities, but also incorporates a basis for continuous assessment. Its goal is to allow organizations to fashion their management of risk to the changing situation and to take account of new risks as they arise. Strategic planning for the Commonwealth to protect critical infrastructure should include the following steps:

1. *Asset assessment* focused on identifying those resources or assets that are most important. These would include human assets, such as first responders and public health officials, as well as physical assets, such as hospitals and information. The focus is an understanding of the consequences of loss of the asset for the Commonwealth and its citizens.
2. *Threat assessment* is the second step. Here it is essential to take into account the priority attached to the asset by the enemy. Is there a past pattern that can be discerned as we think about likely targets of terrorist action? Are there sources of intelligence that can be utilized to provide insights into the types of targets likely to be chosen in the future based on previous terrorist activity? Threat assessment includes both intent and capability based if possible (but not necessarily) on history or proven track record.
3. *Vulnerability assessment* as the third step resembles the security survey that would be undertaken to identify where security is lacking in the asset. Typical vulnerabilities include poor access controls, unscreened visitors in secure areas, or the lack of appropriate software to prevent information tampering or theft. A necessary part of the assessment is an identification of those vulnerabilities most likely to be exploited by a terrorist group.
4. *Risk assessment* represents an effort to combine the asset, threat, and vulnerability assessments for purposes of evaluation as a basis for assessing the level of risk. Specifically, the following three questions would be addressed:
 - What is the likely effect if an identified asset is lost or harmed by one of the identified unwanted events?
 - How likely is it that an adversary or adversaries can and will attack those identified assets?
 - What are the most likely vulnerabilities that the adversary or adversaries will exploit to target the identified assets?

In systematically analyzing each of these questions, individual category numerical values would be used. A simple equation provides the basis for a numerical system for rating risks:

$$\text{risk} = \text{consequence} \times (\text{threat} \times \text{vulnerability})$$

In this formula the segment multiplying “threat by vulnerability” represents the probability of the unwanted event, while the consequence is the effect of the loss of the asset. The outcome of such an approach would be a more informed judgment of how much at risk a particular asset is likely to be. To repeat, the utilization of this type of approach can contribute to rational decision-making about how, when, and where to allocate limited resources. Nevertheless, the analyses must be constantly recalibrated to take account of updated intelligence about likely terrorist targets. The analysis must always be based on the assumption that terrorists will be seeking to attack where we are most vulnerable.

5. *Identification of Countermeasure Options* is the final step in the model. Its purpose is to provide countermeasures designed to lower the overall risk to the asset to an acceptable level. Countermeasures can be set forth as options in which the expected costs and benefits in integrating risk could be identified.

This model is designed to be utilized as a continuous process, rather than a one-time effort. Given the characteristics of the terrorist threat and its evolving, long-term nature, it is essential to monitor constantly changes in assets, the threat, and vulnerabilities based on up-to-date information. As changes become evident, they must be entered into the model in order to produce a revised risk assessment and to make new recommendations for countermeasures.

To assist Massachusetts and the other forty-nine states with this effort, the federal government is developing criteria based on the type of risk management model described above that will provide a clearer basis for prioritizing their critical infrastructure assets. This criteria will help determine how much emphasis should be given to protecting historic landmarks such as

the *USS Constitution* or to safeguarding vital economic assets such as skyscrapers.

The Commonwealth’s critical infrastructure includes several key sectors: seaports/harbors/airports; cyber assets encompassing information networks and telecommunications; energy; transportation; banking and finance; defense industrial base; chemical industry; agriculture; food; water; public health; emergency services; and postal and shipping. The following descriptions are illustrative of two key infrastructure sectors in the Massachusetts and the steps that have been taken to safeguard them.

Seaports, Harbors, and Logan International Airport

Seaports are vital to the economic prosperity of the state of Massachusetts and the Nation as a whole. In the wake of the terrorist attacks, port security has attracted urgent attention because seaports are a target-rich environment. Designed primarily with efficiency of operation, not security against terrorists in mind, seaports are vulnerable because they are located on open waterfronts often in downtown areas. They are used by a wide variety of traffic, and are governed by overlapping jurisdictions of federal, state, and local authorities rather than a centralized agency. In ways that distinguish them from airports, which can be more easily separated, seaports overlap and intersect with the cities of which they are a vital part.

The ports of Massachusetts are the conduit for large volumes of goods and services shipped to destinations throughout the United States and from our ports to all parts of the world. Through the port of Boston flows approximately 70 percent of New England’s energy. The port of Boston supports a growing import and export trade, and hosts approximately 200,000 cruise-ship passengers a year. Overall the port contributes three billion dollars and 9,000 jobs to the local economy. Because the port of Boston is in close proximity to local neighborhoods, securing it with total perimeter control will be difficult and probably impossible to accomplish.

It is recognized that a comprehensive strategy for expanded maritime domain awareness

is required to protect the maritime industry and the Commonwealth's economy from terrorist attack. Such a strategy incorporates an approach in which threats will be identified and neutralized as far as possible from their intended targets, even before containers are loaded aboard ships abroad. Such a strategy could include operational procedures such as standards on inspections, container seals, interagency information sharing, databases, credentialing of transport workers, and chain of command. "Operation Safe Commerce-Boston" has begun to focus on these problems.

A key aspect of port security involves shipping containers. Every day, more than 15 million cargo containers are in transit to destinations around the world. Containers account for about 90 percent of the world's traded cargo. Approximately 1.3 million tons of general cargo arrive in containers in the ports of Massachusetts each year. These containers were designed with transport costs and improved speed and efficiency, rather than security, primarily in mind. Failure to address the security component of containers adequately increases their attractiveness for use in a possible terrorist attack. Such an attack could produce major disruption to the U.S. economy. As a result, the Commonwealth has made substantial efforts to address this problem since 9/11. About seventy percent of all cargo containers entering the port of Boston are now being examined. This compares with a national average of only two percent. Clearly much remains to be done to close this gap in homeland security.

In order to address port security, several steps are essential. They include:

- Adoption of the Automated Manifest System (AMS) where high-risk containers are identified and information is collected and distributed efficiently to those that require the necessary intelligence. For this purpose it will be essential to work with the various maritime transportation lines to obtain necessary information.
- Creation of an effective and efficient sensor and anti-tamper device. The current anti-tamper devices can be easily opened without any sign of such tampering.

- Development of a working tracking device to assure accountability of container transit.
- Improvements in accuracy, duration, and format for transmitting and sharing data about the contents, location, and ownership of container shipments.
- Construction of a safe and secure seaport facility to inspect containers. Currently, suspicious containers are transported through the streets of Boston to a facility within the city. This is a potentially hazardous situation that should be remedied as soon as possible.
- Acquisition of a second x-ray truck to enhance both the flow of cargo and security at the port and to assure that no container is left uninspected.

Since two of the four planes hijacked on September 11 originated from Logan International Airport, the Commonwealth has given much attention to its aviation infrastructure. Although priority is understandably focused on Logan International Airport, the Commonwealth contains a large number of smaller airports. Such facilities contain private aircraft as well as training facilities such as those that could be utilized by terrorists. Small aircraft can be commandeered to carry explosives or biological-chemical weapons. Terrorists can be trained in the essential flying skills that were required by the 9/11 hijackers. Therefore, the Commonwealth's airports must be made as secure as necessary while retaining the ability to perform their necessary and legitimate functions.

Logan International Airport is the eighteenth largest airport in the country in terms of passenger volume and is classified as a Category X airport by the FAA, the category reserved for the largest international airports. On November 19, 2001, President Bush signed into law the Aviation and Transportation Security Act of 2001. This act was established to achieve a secure air travel system and created a new federal agency within the Department of Transportation named the Transportation Security Administration (TSA). The TSA assumed responsibility from the Federal Aviation Agency

for aviation security as well as the security of all transportation modes under the jurisdiction of the Department of Transportation. It was the TSA that took on the ambitious program of requiring all airport screening checkpoints throughout the nation to have a fully federalized screening work force. While airport security has been reviewed and upgraded as a matter of priority, much remains to be done to take account of evolving terrorist threats. These may include the entry into the United States of passengers bearing infectious diseases or efforts to launch rockets against aircraft taking off from or landing at Massachusetts airports. Given its size and contribution to the Commonwealth and regional economy, as well as the large number of passengers using it, Logan International Airport itself represents a potential terrorist target and as such, must be the focus of continuing attention.

Cyber Security

As a matter of Commonwealth strategic planning, it is essential to consider cyberspace as another arena for potential terrorist action. Cyberterrorism represents the convergence of virtual space and terrorism. Terrorist acts in the form of a cyber attack could be mounted against the information systems that are indispensable to the operation of all or parts of our critical infrastructure. Such an attack could be launched either as a stand-alone event or in conjunction with a wider terrorist incident. For example, cyber war could be used to take down the ability of first responders to communicate in a situation in which a terrorist attack on the scale of 9/11 had been launched. Cyber attacks could be launched against private-sector infrastructure or against the information systems of the state, local, or federal government. Certain types of WMD use could have important ramifications for our information systems. For example, this could include the electromagnetic pulse (EMP) effects of a nuclear weapon that could destroy or disrupt communications and other information systems throughout and beyond Massachusetts. More must be done to strengthen security to protect our critical infrastructure from cyber-

terrorism. Protection of the internet cannot be done with government regulation alone. Cyber security requires government and private-sector cooperation. The threat of cyber attacks is of great concern. Our economy is heavily dependent on cyberspace, information technology, and the information infrastructure. The U.S. government itself is heavily dependent on the private-sector information infrastructure. Cyberspace connects a network of networks that directly support all sectors of our economy ranging from energy, transportation, including rail, air, and merchant marine, finance and banking, information and telecommunications, public health, emergency services, water, food, the defense-industrial base, and postal services and shipping. Since our economy depends on these interconnected networks responsible for the daily transfer of billions of dollars in transactions and messages electronically, the threat of cyber attacks presents a clear and present danger.

After 9/11, the United States acted quickly to secure the information and telecommunications structure that supports cyberspace by creating the Critical Infrastructure Protection Board which brought together a public and private partnership to create a National Strategy to Secure Cyberspace. This National Strategy will eventually provide a detailed outline on how both public and private organizations can secure their part of cyberspace that they control. It will need to be assessed for specific applicability to the needs of the Commonwealth. The Commonwealth has already begun to focus efforts on securing cyberspace by increasing redundancy, encryption, electronic firewalls, and the compartmentalization of computer systems.

Working with the Private Sector to Protect Critical Infrastructure

Because most of the infrastructure in our Nation and the Commonwealth is privately owned or operated, it is necessary to work closely with the private sector in securing the various critical infrastructure nodes. The private sector has primary responsibility for protecting such privately owned infrastructure as power lines

or water reservoirs. Substantial efforts have been made since 9/11 to give added protection to such infrastructure. Such protection often includes private security firms as well as representatives of the official law enforcement community.

Since 9/11, the most vulnerable targets and critical infrastructure nodes within the state have been identified. Greater cooperation with the private sector to enhance cooperation with information systems is needed to promote better security. Since the federal, state, and local governments rely on the private sector for critical infrastructure nodes, the private sector's ability to protect critical infrastructure needs to be strengthened and complemented by official resources. There are several cases of such cooperation. For example, as noted earlier the Massachusetts Water Resources Agency has worked hand in hand with various state and local agencies to ensure protection of its facilities. The New England Gas Association has coordinated efforts with the state in facilitating security needs for liquefied natural gas (LNG) tankers entering the port of Boston. Finally, the Commonwealth and National Grid USA – responsible for supplying electricity to Massachusetts – have also expanded security collaboration and related endeavors in the aftermath of 9/11.

Reducing the Commonwealth's vulnerability to a potential terrorist attack requires the coordinated effort of many federal, state and local departments and agencies that have long-standing relationships with the private sector. As noted earlier, since the private sector owns the majority of the critical nodes within the state, the Commonwealth must collaborate with the private sector to ensure that essential services are not interrupted or that they can be restored quickly following an attack. To accomplish this task the Commonwealth and the private sector must work together to establish an accurate inventory and assessment of the private sector's critical infrastructure and key assets along with their vulnerabilities.

However, concerns that the particulars about their infrastructure and business practices may become public knowledge via the Freedom of

Information Act (FOIA) has inhibited private companies from sharing detailed information with the state about its critical infrastructure, especially regarding specific vulnerabilities. The private sector fears that the release of such competition-sensitive, proprietary data could result in legal liabilities and a loss of competitive advantage. Cognizant of this problem, the Commonwealth, as described earlier in this document, enacted legislation that excludes sensitive infrastructure information from FOIA requirements.

The promise of tax and insurance reductions as incentives for security enhancements should also be considered as part of a strategy to engage the private sector in addressing security needs. Another option would be for the Commonwealth to use a regulation-based approach requiring private industry to supply certain kinds of information deemed vital to homeland security. An appropriate combination of such approaches should be considered.

Defending against Catastrophic Threats

Defending the Commonwealth against catastrophic threats, including WMD, requires unprecedented coordination, communication, and interoperability among all relevant agencies, authorities, organizations, and individuals, especially first responders. Such cooperation will allow for better detection and response to a WMD attack. Since 9/11, communication and cooperation have increased throughout the state and with the Centers for Disease Control and Prevention that has the federal role of detecting, diagnosing, and addressing biological and chemical threats. In Massachusetts, the Bio-terrorism Coordinating Council, comprised of a six-member panel of leading physicians and scientists, has been given the task of serving the Governor as a think tank and advising the Department of Public Health in the development of a comprehensive strategy to protect the Commonwealth in the event of a bioterrorism attack. The Department of Fire Services, responsible for the state's six Hazardous Material teams, has worked in collaboration with the

state's National Guard Civil Support Team in preparing to respond to a WMD event.

The development and deployment of advanced detection technologies and enhanced laboratory surveillance, which would be able to identify a chemical, biological, radiological, or nuclear attack at the early stages, would greatly aid response and recovery efforts across the entire Commonwealth. The ability to recognize and report as quickly as possible a chemical or biological attack will minimize casualties and allow for proper treatment of those injured. As described in an earlier section, the Massachusetts Department of Public Health employs an infectious disease surveillance mechanism within the greater Boston metropolitan area to monitor patient volume and types of illness in area hospitals in order to identify potential outbreaks. Moreover, the Commonwealth has also deployed chemical, biological, radiological, and nuclear detection mechanisms throughout the Boston area with the help of the Massachusetts National Guard. However, the Commonwealth must work with the federal government to introduce even more affordable, accurate, compact, and dependable sensors to detect and identify nuclear, chemical, and biological agents within the state. Such equipment could be utilized at key points of entry to deter the smuggling of WMDs.

The development and deployment of advanced detection technologies and enhanced laboratory surveillance equipment throughout the Commonwealth to improve the ability to identify a chemical or biological attack still remains to be undertaken. In addition, local health providers and emergency personnel must be able to diagnose symptoms and detect an epidemic in its early stages. This could be done with the increased training of local health providers through the Centers for Disease Control Epidemic Intelligence Service to help recognize biological attacks. Moreover, it would be beneficial to the Commonwealth to help facilitate federal efforts to link public health databases such as the Epidemic Information Exchange System, the National Electronic Disease Surveillance System, and the Laboratory Response Network in order to increase the speed and precision of diagnoses and confir-

mation of attack. This information could then be utilized by state officials to take the appropriate responses.

In improving treatment and response programs, the Commonwealth should facilitate advanced research into medical sciences such as infectious disease prevention and treatment, forensic epidemiology, or microbial forensics. Moreover, Massachusetts should work with the proposed National Biological Weapons Analysis Center to identify highest priority threat agents and to conduct risk assessments within the Commonwealth.

First responders consisting of law enforcement and emergency management agencies need training and hazardous materials gear to protect themselves and the public during an emergency. The absence of adequate training and protective gear will result in unnecessary delays and increased casualties in mitigating the impact of a bio/chemical incident.

Emergency Preparedness and Response

Preparing for response and recovery in the event of a terrorist attack is vitally important in mitigating the effects of any such incident. Essential to ensuring homeland security is the creation of effective plans and appropriate procedures for responding to a catastrophic terrorist incident such as a biological or radiological attack. The response to an emergency must be coordinated, comprehensive, and to the extent feasible, standardized among responders.

The Commonwealth must continue to improve the communications capabilities among first responders, especially police and firefighters. Such communication systems in the Commonwealth are still inadequate. For example, security efforts to provide protection to liquefied natural gas (LNG) tankers entering the port of Boston are hampered by the use of multiple radio systems that must be "patched" together. The Commonwealth has begun to address these issues by applying for federal grants and testing new equipment. One improvement made with the use of federal grants has been MEMA's effort to supply common communica-

tions equipment by distributing 800-megahertz handheld radios to towns and cities across the state. Nevertheless, the Commonwealth should work as closely as possible with the federal, state, and local authorities to ensure that interoperable communication is improved.

Preparations for a Bioterrorist/Chemical Attack

The state, along with its municipalities, will bear much of the initial burden and responsibility for providing an effective public health response to a biological or chemical terrorist attack on the state's population. The first line of defense will be the state and local public health personnel who will likely be the first to recognize that the Commonwealth has been attacked with biological agents. Therefore, it is imperative that these healthcare providers have the appropriate equipment, training, funding, and immunization to carry out their critical mission of detecting and responding to such an attack. Improved infectious disease surveillance mechanisms, as stated in the previous chapter, will increase the capacity of the Commonwealth's public health systems to respond to outbreaks or contagious diseases. The state should continue to expand its research and investment in developing more affordable and portable detection mechanisms to increase warning of an attack.

Handling Outbreaks

To handle the outbreak of an infectious disease, the Commonwealth must continue its efforts in securing federal grants for training and equipping its state, local, and private health care personnel to deal with the growing threat of WMD terrorism. Massachusetts has received federal funds to enhance public health preparedness efforts against biological threats. These funds are intended to upgrade infectious disease surveillance and investigation, enhance the readiness of hospital systems to deal with large numbers of casualties, and expand public health laboratory and communication system capacity. In addition, the Massachusetts Department of Public Health, in conjunction with the Bioterrorism Council, has established two advisory committees, the State-

wide Bioterrorism Preparedness and Response Program Advisory Committee and the Hospital Preparedness Planning Committee. These committees are being used to strengthen preparedness by making improvements in the state's capabilities to respond to a chemical or biological incident.

Augmenting the Commonwealth's Access to Vaccine

It is necessary for the Commonwealth to work with the federal government in ensuring that adequate pharmaceutical and vaccine supplies are quickly available for a rapid response to a bioterrorist attack. This is especially important given the threat that may be presented by smallpox. Although a worldwide immunization program eradicated smallpox disease in the 1970s, the use of smallpox as a bioterrorist weapon has led the U.S. government to develop plans for vaccinating military personnel, healthcare, and emergency workers as a matter of urgency and to make smallpox vaccine available to the public by 2004. It is suspected that countries such as Iraq have kept quantities of smallpox for possible use. It is also feared that certain terrorist groups may gain access to the smallpox virus.

The Commonwealth must be prepared for mass vaccination against smallpox. Although the federal government presently maintains the stockpile of the smallpox vaccine, it is left to the state and local governments to set up the vaccination clinics and the procedures to do so. The Centers for Disease Control and Prevention (CDC), based in Atlanta, Georgia, has the ability to ship the vaccine anywhere in the country in a matter of hours. The state has already submitted its vaccination plans to the federal government. Although the CDC will advise and assist state and local health departments throughout the state in the event of a bioterrorist outbreak, the Commonwealth and its localities will have the primary response responsibility.

The federal government has taken steps designed to provide help to the states to cope with bioterrorism. The National Pharmaceutical Stockpile presently contains sufficient antibiotics to treat twenty million people against

diseases such as anthrax, plague, and smallpox. The National Pharmaceutical Stockpile Program maintains a repository of pharmaceuticals, antidotes, and medical supplies, known as twelve-hour Push Packages, that can be used in an emergency. There are twelve strategically positioned Push Packages around the Nation. Each Push Package has the ability to be transported to the emergency site within twelve hours for distribution by the state. The first emergency use occurred on September 11 when one Push Package was delivered to New York City in the immediate aftermath of the World Trade Center attacks. It is imperative that a comprehensive and efficient plan be put in place in Massachusetts to ensure the distribution of the Push Package once received from the federal government. A detailed plan concerning protection and distribution must be carefully developed to ensure that adequate medical supplies are made available throughout the state. Even though the Centers for Disease Control has the ability to ship vaccines or antibiotics anywhere in the country in a matter of hours, it is left to the state and local levels to set up clinics to vaccinate people and take other necessary medical measures if a bioterrorist attack occurs.

The Commonwealth must work with the federal government in assuring access to vaccine stocks, developing new vaccines and treatments, and obtaining equipment to detect any infectious disease or chemical weapons use. For this purpose laboratories, universities, and pharmaceutical companies located within the Commonwealth should be identified and called upon as necessary as part of the response capabilities that would be required in the event of a terrorist attack using WMD.

Cooperation with the Center for Disease Control and Prevention

The Centers for Disease Control and Prevention (CDC) will aid the Commonwealth in detecting, diagnosing, and mitigating bioterrorist threats. The CDC's Epidemic Intelligence Service is currently being expanded and augmented to assist local and state officials in recognizing biological attacks through better training.

The newly created Epidemic Information Exchange System allows for disease information sharing through a secure information system. This will eventually allow all public health databases to be linked nationwide through the National Electronic Disease Surveillance System in order to recognize disease patterns. Moreover, the Laboratory Response Network will draw upon existing laboratory technology to increase the speed of diagnosing and confirming a potential biological attack. The Commonwealth has established a working relationship with the CDC's Laboratory Response Network for Bioterrorism. This relationship allows state public health laboratories to serve as a link between local and clinical laboratory levels and the CDC. This network augments the state's capability to identify and investigate disease outbreaks and provides testing and reference services.

Surge Capacity

Surge capacity is the ability of the healthcare community to handle a large influx of patients. The Commonwealth presently lacks adequate capabilities for dealing with a prolonged mass casualty event. Hospitals will be able to find some necessary beds during a time of emergency by postponing nonessential surgery and other procedures. However, due to shortages of nurses and other healthcare professionals within the Commonwealth, the problem of personnel will become an issue if mass casualties result from a terrorist attack.

The creation of a reserve cadre of retired personnel should be considered. Such a reserve could be created on a volunteer basis, tapping into a substantial source of expertise that would be required as part of a public health surge capacity. Issues of training, immunization, and legal protection of such a reserve cadre would need to be addressed before a plan could come into action.

Available medical personnel from other states could also be utilized to strengthen existing capacity within the Commonwealth. However, indemnification and licensing issues may need to be addressed through state legislation.

Moreover, the issue of personnel compensation must also be reviewed.

The Commonwealth must also identify other potential solutions to address the problem of mass casualties. The use of hotels, schools, gymnasiums, or sporting arenas should be considered. However, if such facilities are used, the issues of liability and worker compensation must be addressed. Nevertheless, it will be essential to understand the potential limits of such interstate cooperation. Fearing that they themselves will face outbreaks of bioterrorism or of infectious disease across their borders, states or even local authorities within states may be reluctant either to provide healthcare workers or to receive patients with infectious diseases.

Cooperation with the Federal Government

The Commonwealth needs to coordinate and work closely with the Department of Homeland Security as the federal government develops the Federal Incident Management Plan. This effort is an all-discipline, all-hazard plan that eliminates the distinction between ‘crisis management’ and ‘consequence management,’ recognizing that consequence management is crisis response. The Federal Incident Management Plan would provide common terminology and a unified command structure to support all incidents of disaster whether it be bioterrorism or a blizzard. The plan would include the capability to clarify the roles and contributions of the emergency response agency at the federal, state, and local level.

The Federal Incident Management Plan calls for a federal coordinator to manage the site of emergency. The federal coordinator would then be responsible to the President for coordinating the entire federal response. Lead agencies would maintain operational control over their functions. For example, the FBI would remain the lead agency for federal law enforcement while working with the federal coordinator.

To supplement the Federal Incident Management Plan, a national incident management system must also be created at the state and local level. This would allow state and local governments to integrate their response assets with the federal government in an emergency.

Finally, the Commonwealth needs to strengthen ties with neighboring states in case of an emergency. The Emergency Management Assistance Compact (EMAC), ratified by the Commonwealth, administered by the National Emergency Management Association (NEMA), and endorsed by the Federal Emergency Management Agency (FEMA), is a legal mechanism that represents a mutual aid agreement between states. This agreement allows states to request out-of-state aid in an emergency. States requesting aid are obligated to repay costs to states that provide it. Massachusetts should take a lead in strengthening cooperation with governors of the New England region. Both the New England Regional Coalition of Governors and the National Governor’s Association provide a useful setting for such cooperation.

National Disaster Medical System

The Commonwealth must look to the federal government to receive several forms of support. For example, any bioterrorist event will most likely overwhelm an existing state, local, and privately owned health care facility. To prepare against this contingency, the Commonwealth and its local and privately owned health care facilities need to continue working with the federal National Disaster Medical System. This federal/private partnership that includes the Departments of Health and Human Services, Defense, Veterans Affairs, and FEMA, provides rapid response and critical surge capabilities to support localities in disaster medical treatment. This system would provide essential resources in a time of need within the Commonwealth.

Guidelines for Vaccination

Guidelines for vaccinating civilian response personnel against biological agents are being developed. At present, the federal government has decided to recommend smallpox vaccination to all emergency workers and response teams that have the role of investigating suspected cases. Currently, the Commonwealth is preparing to offer the smallpox vaccine to the frontline emergency personnel and has submitted plans that have been approved by the

federal government for first-stage smallpox vaccinations. Immunizations will soon begin. The Department of Health and Human Services (HHS) has been ordered by the President to work with state and local governments to form volunteer Smallpox Response Teams who can provide critical services in the event of a smallpox attack. To ensure that Smallpox Response Teams can mobilize immediately in an emergency, health care workers and other critical personnel will be immunized.

First Responder Training

The Commonwealth must work with the federal government in building a national first responder training and evaluation system. The past anthrax attacks and the continued threat of a WMD attack have forced emergency personnel to undergo retraining. To ensure that personnel are efficiently prepared, the Commonwealth should work with the Department of Homeland Security to create a consolidated and expanded training and evaluation system. This system would be based on a four-phased approach: requirements, plans, training (and exercises), and assessments (comprising evaluations and corrective action plans). The Department of Homeland Security would serve as the central coordinating body responsible for overseeing curriculum standards and, through regional centers of excellence such as the Emergency Management Institute in Maryland, the Center for Domestic Preparedness in Alabama, and the National Domestic Preparedness Consortium, for training the instructors who will train our first responders. These instructors would then take the knowledge they learned back to their own agency and further train their colleagues. To receive future federal grants, these standards would have to be maintained by first responders through certification.

To date, the Commonwealth has begun to take action in properly training its first responder agencies. For example, since 9/11 the Massachusetts State Police has trained its personnel on WMD issues through an eight-hour course taught by Louisiana State University (LSU) on the internet. LSU established the Academy of

Counter-Terrorist Education to develop and provide a comprehensive program for emergency responder education and training on the detection, prevention, and response to WMD terrorist incidents. As noted in an earlier section, the creation of the State wide Anti-Terrorism Unified Response Network (SATURN) has also provided up to date cross-disciplinary training for the first responder community in Massachusetts. The Executive Office of Public Safety, in conjunction with the Anti-Terrorism Task Force in Boston, is working to develop an updated, comprehensive training curriculum to improve SATURN. A fire training facility for all emergency responders is being considered for construction at Otis Air Force Base on Cape Cod. This facility would become a regional training facility for the Northeast.

Victim Support System

In order to assist the victims of terrorist attacks and their families, as well as other individuals affected indirectly by attacks, both the federal government and the Commonwealth must be prepared. In the event of a terrorist attack, the Commonwealth will need to be able to call upon the Department of Homeland Security and to work with other federal agencies in providing guidance in offering victims and their families various forms of assistance. This is likely to include crisis counseling, cash grants, low-interest loans, unemployment benefits, free legal counseling, tax refunds and other forms of immediate assistance depending on the type and magnitude of the terrorist attack.

Military Support

It is important not to overlook the significant contributions that the National Guard offers to the state. The National Guard already has an emergency response capability in place. In addition, the National Guard can provide assistance and authority during a crisis, as it did, for example, at Logan International Airport and other airports immediately after 9/11. The Massachusetts National Guard will play a critical role if a catastrophic terrorist attack takes place within the Commonwealth. Therefore, it

must be well trained, equipped, and ready to provide significant assistance to the state during a terrorist incident.

Unlike the regular United States Armed Forces, the National Guard when called upon by the state governor to enforce civil laws is not bound by *posse comitatus* restrictions on performing law enforcement duties. The 1878 *Posse Comitatus* Act prohibits U.S. soldiers from participating in police actions inside the United States. This exemption allows the National Guard to provide a more flexible response than that of the regular armed forces, for example, by supplying medical, engineering, military police, and ground and air transport units to aid the state in responding to a terrorist incident under the authority of the governor. The Massachusetts National Guard can help evacuate, quarantine, and protect residents when needed; provide expertise in the event of chemical, biological, nuclear, and radiological attacks, including the capability of giving aid in response; and make available additional support and equipment to local medical centers. After the 9/11 attacks, the Massachusetts National Guard responded rapidly in deploying troops to Logan International Airport and elsewhere as needed to protect both the Commonwealth's citizens and infrastructure.

Moreover, the Massachusetts National Guard has attached to it the First Civil Support Team (CST). CSTs were established in the spring of 2000 to deploy rapidly to assist a local incident commander with expert technical advice on WMD response operations; and help identify and support the arrival of follow-on state and federal military response assets. Each team is staffed with twenty-two cross-trained, full-time members of the Army and Air National Guard.

CSTs bring unique capabilities and expertise that may be vital during a terrorist attack. The teams are unique because of their federal-state relationship. They are federally resourced, federally trained, and operate under federal doctrine. But they will perform their mission primarily under the command and control of the governor of the state where they are located, working with the adjutant general responsi-

ble for the unit, thus making them state assets. The Commonwealth should embrace the team as a vital asset. As appropriate, training exercises involving CSTs and state and local first responders should be encouraged.

The National Guard has important capabilities that can be utilized as required by the Commonwealth. However, there are issues that must be addressed to ensure an efficient response by the National Guard during crises:

- The National Guardsmen within the Commonwealth cannot all be activated at a moment's notice. It takes time and resources to get Guardsmen from their jobs and then deploy them.
- Keeping National Guardsmen on duty is becoming a problem for sustainability. More needs to be done to protect the jobs of the Guardsmen who are activated for long deployments. Despite the laws that are in place to protect these soldiers, hardships are inflicted both on the employer and employee. Additional legislation may be appropriate to give businesses who hire National Guardsmen incentives to ease the problems of dislocation.

IV

Foundations

The *National Strategy for Homeland Security* cites four fundamental tenets or foundations – law, science and technology, information sharing and systems, and international cooperation – that infuse each homeland security mission area, cut across federal, state, and local levels of government, and permeate all sectors of U.S. society. Three of these tenets, law, science and technology, and information sharing and systems, provide a useful starting point to assess needed homeland security investments within the Commonwealth. Although Commonwealth security will be shaped in unprecedented ways by events beyond our shores for which international cooperation will be needed, a principal state-level focus will be regional, cross-state cooperation. Therefore, this *Strategic Plan* includes this important area as one of the foundations for Commonwealth security.

The Law

Throughout its history, the United States has utilized the law to advance and preserve our security and liberty. The law supplies the means for the government to act and to define the proper limits of those actions. The law also provides the basis for civil relationships that affect each of our citizens. Since September 11, the federal government has enacted major legislation, including the USA PATRIOT Act, the Aviation and Transportation Security Act, the Enhanced Border Security and Visa Entry Reform Act, and the Public Health Security and

Bioterrorism Preparedness and Response Act, all designed to combat terrorism while simultaneously attempting to ensure that they do not unduly preempt state law or adversely impact our basic civil liberties.

The Commonwealth has also focused closely on legislative requirements following the events of 9/11. It has conducted an extensive review of the state's existing statutes to determine what laws are applicable to the current counterterrorism effort and what additional legislation is necessary to protect the public welfare and provide for security against terrorism. As a conse-

quence of this review, Massachusetts quickly drafted and passed a series of first round legal measures addressing issues related to the use of hoax substances, the possession of weapons at airports, limitations on public access to sensitive infrastructure data, criminalizing unauthorized possession of explosives and the use/possession of either bio- or chemical weapons, and criminalizing the communication of terrorist threats in various media. A major goal underpinning development of its anti-terrorism laws is to make certain that basic civil liberties in the Commonwealth are not undermined. A more detailed description of the priority legislation passed by the Massachusetts State Legislature is found in the section entitled *Steps Taken by the Commonwealth to Increase Post-9/11 Security*.

Currently, there is also a second round of legislation pending submission. These bills are focused on maritime security, money laundering, computer hacking, statewide grand jury, defining the crime of terrorism, bioterrorism and emergency powers, wire tapping, the tagging of explosives, and a forfeiture statute to include anti-terrorism.

As noted above, the Commonwealth is investigating what additional emergency powers are needed as a result of potential acts of terrorism. In this regard, the state has produced a draft law entitled *An Act Protecting the Public Health of the Commonwealth from Bio-Terrorism, other forms of Terrorism and Activities related to Terrorism, otherwise known as the Massachusetts Emergency Health Powers Act*. As the title implies, the goal of the law is to ensure that the Governor and the Commonwealth can cope with a range of possibly unprecedented emergencies resulting from a biological or other type of terrorist attack not deemed likely – or even considered – prior to September 11. These encompass bioterrorist attacks and the spread of infectious diseases; requirements for widespread and rapid vaccinations; quarantines and evacuation procedures; appropriation/use of private property; imposition of rationing and related restrictions; and legal liability and indemnification issues. The law directs the Commonwealth to develop a comprehensive plan to provide a coordinated

response to a public health emergency resulting from possible acts of terrorism.

Directly related to the *Emergency Health Powers Act* and the possible consequences of a terrorist attack, the Commonwealth also needs to reassess and modify as necessary laws related to the continuity of government and lines of succession issues in the event of the death or injury of the Governor and Lieutenant Governor. The Commonwealth must ensure that laws are in place providing for legitimate succession and leadership in order to carry out the functions of government during an emergency.

In addition, the *National Strategy for Homeland Security* sets forth several proposals for legal initiatives that each state should consider for enactment. As is evident from the description above, key elements of a number of the suggested initiatives have already been enacted or are under serious consideration by the Commonwealth. The federal government put forward six initiatives:

1. Coordinate suggested minimum standards for state driver's licenses
2. Enhance market capacity for terrorism insurance
3. Train for prevention of cyber attacks
4. Suppress money laundering
5. Ensure continuity of the judiciary
6. Review quarantine authority

Science and Technology

Our Nation's historic strength in science and technology is critical to protecting America from terrorism. Because of its world-class high-technology information-age industries and labor force, together with leading institutions of higher learning, the Commonwealth has a special role to play in science and technology. This includes each of the core missions of homeland security listed below. Advanced technologies for analysis, information sharing, detection of attacks, and countering weapons of mass destruction (WMD) are essential to thwart and lessen the destruction from terrorist attacks. Just as science and technology have helped the United States defeat enemies overseas, they will contribute to our efforts against terrorists who

attack our Nation. To help mitigate the risks posed by terrorism, the federal government has initiated a national effort to develop additional capabilities for the core mission of homeland security. It has identified eleven major science and technology initiatives:

1. Develop chemical, biological, radiological, and nuclear countermeasures
2. Develop systems for detecting hostile intent
3. Apply biometric technology to identification devices
4. Improve the technical capabilities of first responders
5. Coordinate research and development of the homeland security apparatus
6. Establish a national laboratory for homeland security
7. Solicit independent and private analysis for science and technology research
8. Establish a mechanism for rapidly producing prototypes
9. Conduct demonstrations and pilot deployments
10. Set standards for homeland security technology
11. Establish a system for high-risk, high-pay-off homeland security research

The Commonwealth possesses unique and robust capabilities especially in the vital science and technology areas just cited. Indeed, our state is the location of many of the world's most innovative high-technology firms and organizations, defense corporations, renowned educational centers, and medical institutions responsible for ground-breaking research ranging from software development and information technology, biomedicine and vaccines against bioterrorism, to advanced surveillance/detection techniques and systems. As a result, the Commonwealth has the potential to play a leading role in the national effort and to make significant contributions to the homeland security mission both to the Nation as a whole, and directly here in Massachusetts. This area of strength, of course, also enhances the importance of Massachusetts as a potential terrorist target.

The federal government significantly increased the amount earmarked for homeland security research and development (R&D) to approximately \$3 billion in its 2003 budget to ensure that our R&D efforts are of sufficient size and sophistication to counter the threats posed by modern terrorism. The majority of this funding is devoted to the development of bioterrorism countermeasures, detection capabilities, vaccines and antivirals against biological agents. The Department of Homeland Security (DHS) is the federal government's focal point for this effort. Given its capabilities, the Commonwealth needs to work closely with DHS in this endeavor as well as to encourage the public and private institutions in Massachusetts to become more proactive in seeking out federal contract opportunities that will not only help to bolster the security of our Nation and the Commonwealth but also serve to increase the economic vitality of the state.

Information Sharing and Systems

Information systems contribute to every facet of the homeland security mission. However, even though American information technology is the most advanced in the world, at present our Nation's information systems do not adequately support that mission. Databases used for federal law enforcement, immigration, intelligence, public health surveillance, and emergency management have not been interconnected in a manner that eliminates information gaps or redundancies.

These problems are endemic within the information systems of the Commonwealth as well. For example, most state and local first responders do not use compatible communications equipment. Relatively simple procedures like sending email are made more difficult because the software used by computers in certain state agencies is incompatible with those used in other offices. During an emergency, the negative consequences of such information system incompatibilities would be greatly magnified. Therefore, to provide more effective protection against the terrorist threat, we must connect the enormous quantity of information

located within each government agency in the Commonwealth while making sure that adequate privacy is maintained.

In this regard, the federal government has identified five major initiatives in the area of information sharing and systems, many of which are currently being addressed – or should be undertaken – by the Commonwealth:

1. Integrate information sharing across the state government
2. Integrate information sharing across state and local governments, private industry, and citizens
3. Adopt common “meta-data” standards for electronic information relevant to homeland security
4. Improve public safety emergency communications
5. Ensure reliable public health information

Massachusetts is addressing issues associated with information sharing and systems on several fronts. The Commonwealth’s Information Technology Division has formed an Information Technology Commission with the charter to address the state’s information technology (IT) systems and develop approaches to enhance their interconnectedness. The Commission, comprised of twenty-five members from the state executive branch, the legislature, and the private sector, seeks to coordinate the information technology efforts of approximately 170 state divisions/offices which utilize close to forty-five different IT systems.

With regard to emergency communications, several state agencies and first responders, including the State Police, the National Guard, the Department of Fire Services, the Massachusetts Emergency Management Agency, Massachusetts Port Authority, the Department of Transportation, the Department of Fisheries, Wildlife and Environmental Law Enforcement together with the Federal Bureau of Investigation and the U.S. Attorney’s Anti-terrorism Task Force are working closely to make emergency communications interoperable. This includes the identification and development of acquisition plans for communication devices that would allow statewide interoperability among

all emergency responders in the state as well as with federal agencies such as the FBI.

Regional Cooperation

The Commonwealth needs to place greater emphasis on regional cooperation for the homeland security mission. This requirement became obvious following September 11 for several reasons. The impact of terrorist incidents can easily transcend state borders. For example, an outbreak of smallpox in the Commonwealth could quickly spread to neighboring states and to the Nation as a whole. Moreover, for many potential terrorist incidents the number of casualties could quickly overwhelm area medical resources and hospitals at a time when the assistance of medical personnel from neighboring states may not be readily available as such states consider their own needs and hold in reserve assets to cope with a terrorist incident that may engulf them as well.

The prospects for successfully implementing regional collaboration measures are at their height during times when the government and public are cognizant of the necessity for effective emergency prevention and response. Given the events of 9/11, now is one of those times. The Commonwealth should seize the initiative to conclude mutual aid agreements with neighboring states and to institute advance planning to cope with the regional/national implications of terrorism. This will require greater planning, cooperation, and joint exercises across state boundaries in and beyond New England.

An important benefit of regional collaboration is that it may reduce the financial burdens of homeland defense to individual states by sharing resources. For example, equipment sharing and passing mutual aid arrangements can lessen the need for each state to procure the quantity of specialized gear it would otherwise require were it not in partnership with another state(s). The prospect of achieving even modest financial savings will make regional collaboration more palatable and thus easier to attain. Apprehensions about regional cooperation include the potential for equipment damage, accidents and personnel injuries, and liability for actions while assisting a state partner.

These trepidations can be minimized, however, by enacting state legislation providing insurance coverage of such damage/injuries as well as the indemnification of personnel supplying cross-state assistance.

To be most effective, however, the Commonwealth should establish the specific arrangements for regional cooperation prior to the occurrence of an incident. One promising approach to regional collaboration would be to expand the charter of the existing New England Regional Coalition of Governors to include greater emphasis on emergency preparations and response to terrorist related incidents. To the extent feasible, the Commonwealth should work with the members of the New England Regional Coalition of Governors to harmonize, coordinate, and implement homeland security strategies. Finally, where it has not already done so, the Commonwealth should conclude mutual aid agreements with neighboring states which allow Massachusetts to request out-of-state aid during an emergency situation in return for making available Commonwealth resources to out-of-state entities as needed.

Conclusions

The Commonwealth's Homeland Security Priorities

The Commonwealth's *Strategic Plan* identifies important tasks that have already been initiated together with priorities and issues that must be addressed:

A new mindset is needed. The strategic environment changed dramatically following the events of 9/11. It encompasses threats that may originate in terrorist training camps in South Asia and have their consequences in the form of terrorist acts in U.S. cities as was the case on September 11. This transformed environment, and the terrorist threat that characterizes it, requires not only a new strategy that incorporates innovative, original concepts that cut across federal, state, and local jurisdictions as well as transcend outmoded, ineffective approaches to security. Combating the terrorist threat also requires an entirely new mindset. We must think about issues, resources, and relationships in ways that “connect the dots” in unprecedented and unaccustomed ways. It is no longer possible to compartmentalize security, including intelligence, between what takes place outside the United States and what could occur as a result in the Commonwealth. Indeed, what is foreign and what is domestic are inextricably entwined in ways that could hardly be imagined before 9/11.

To think in such terms of interconnectedness is the essential precondition for the mindset that will be required at the state and local levels for post-9/11 Commonwealth security. We must be prepared to think in a novel fashion about phenomena that were once viewed as separate and unconnected. Terrorists have demonstrated the capacity to turn our commercial aircraft into weapons to be used against other civilian targets. They have shown that it is possible to receive training in distant settings such as Afghanistan or as close as the pilot-training facilities here in the Commonwealth. These concepts and principles must infuse our thinking, strategy, and actions as we organize for the complex task of safeguarding the Commonwealth from the threat of terrorism.

Organize for homeland security: How we organize for Commonwealth security highlights the critical importance that we attach to the protection of our citizens and infrastructure against terrorism. Essentially, there are four leading organizational options for homeland security. They include: 1) moving the Office

of Commonwealth Security (OCS) into an existing cabinet department, e.g., the Executive Office of Public Safety; 2) creation of a Commonwealth Department of Homeland Security patterned after the recently established federal Department of Homeland Security; 3) retention of the OCS with additional areas of responsibility and jurisdiction; and, 4) keeping the same OCS organizational structure as now exists.

In option one, the responsibilities of Commonwealth homeland security would be folded into a department such as the Executive Office of Public Safety. This approach would allow the new Commonwealth security entity to tap into the range of funding and staffing resources available to a cabinet-level secretariat. If option one is followed, the person designated to lead the Commonwealth homeland security function should, at a minimum during emergencies, have a direct line of communication to the Governor.

Option two would mirror the design of the new Department of Homeland Security which will amalgamate at least twenty-two diverse federal agencies including the U.S. Coast Guard, the Federal Emergency Management Agency, the Customs Service, the Immigration and Naturalization Service, the Secret Service, and the Transportation Security Administration. Paralleling this approach, the Commonwealth Department of Homeland Security would incorporate offices/agencies from existing state departments and organizations, possibly including the biomedical office from the Department of Public Health, the Massachusetts Emergency Management Agency, components of the Executive Office of Public Safety, the terrorism unit of the State Police, elements of the National Guard, components of the Fire Services (e.g., bomb units), and intelligence capabilities that have a role to play in the war against terrorism. The Commonwealth Department of Homeland Security would be headed by a Secretary who would be part of the Governor's Cabinet.

This organizational format would enable more efficient communications and facilitate federal funding transfers to the Commonwealth by eliminating, or at least significantly curtailing,

the cumbersome coordination process among officials in different agencies at both the state and federal levels. In this regard, the Department of Homeland Security has informed officials in all fifty states that it would prefer a single point of contact with its state homeland security counterparts.

Option three, an expanded OCS, would be given significantly greater staff personnel, a separate budget, and augmented resources. A key component of this structure is that the Director of the expanded OCS would have a direct reporting line to the Governor, although not necessarily as a member of the Governor's Cabinet. In the expanded OCS set-up, state agencies and other offices involved in various aspects of the Commonwealth security mission would not necessarily be absorbed into OCS but would work closely with its Director and staff.

Finally, option four is the continuation of the status quo. If OCS is to implement its broad charter successfully, however, maintaining the status quo is not a viable long-term organizational option. OCS presently consists of a two, at times three person staff headed by the Director. Obviously, given its range of responsibilities and the multiple tasks it needs to accomplish, OCS requires greater resources and additional personnel. Ideally, OCS would be able to address tasks simultaneously. Unfortunately, due to insufficient staffing OCS is, in general, forced to undertake tasks sequentially, one at a time, not concurrently. This limitation inhibits productivity. The organizational structure for OCS needs to reflect its wide range of specific requirements and responsibilities. As presently configured, it does not. Lacking authority over personnel and without a separate budget, OCS will not be as effective as it should be.

Whatever organizational option is chosen, the Office of Commonwealth Security, at least during emergencies, should have a direct line of communication and responsibility to the Governor. Such an organizational approach would communicate to the citizens of the Commonwealth that Massachusetts attaches as great a priority as the federal government to homeland security.

Review and update the Governor's emergency powers. The Governor's emergency powers need to be reviewed and modified as deemed necessary in order to address the exigencies of the terrorist threat. Where required, new legislation must be drafted and passed to ensure that the Governor and the Commonwealth can cope with a range of possibly unprecedented emergencies that were not deemed likely – or even considered – prior to September 11. Such emergencies include the threat of bioterrorist attack and resultant infectious diseases, requirements for widespread and rapid vaccinations, use of WMDs, etc. At a minimum, the Commonwealth needs to review and modify emergency powers related to continuity of government and lines of succession issues in case of the injury or death of the Governor and Lieutenant Governor; quarantines and evacuation procedures; appropriation/use of private property; imposition of rationing and related restrictions; and legal liability and indemnification issues.

Augment the Commonwealth's biomedical health service capabilities. The core capacity for public health and medical care needs to be greatly enhanced with respect to detection and treatment of infectious disease resulting from bioterrorism. The biomedical, public health, and human services communities should be working in greater partnership with one another, coordinating more effectively with the larger national security community. The expertise of the commercial pharmaceutical and biotechnology sectors located in Massachusetts must also be leveraged and integrated into the effort. Part of this endeavor includes expanding the pool of Commonwealth medical/health professionals who have necessary awareness of the symptoms that could be indicators of biological terrorism such as anthrax and smallpox as well as developing new techniques for surveillance and identification; boosting the Commonwealth's ability to cope with contagious diseases; and augmenting funding for research on preventive vaccines and diagnostic testing.

Expand surge capabilities. The Commonwealth must develop a comprehensive strategy for assuring surge capacity for health care in the event of a large scale terrorist incident. The Common-

wealth needs to identify all existing assets, including the number of current medical/health staff as well as retired physicians and health personnel who could be called upon for help in an emergency, and how they would be mobilized to address mass casualty care. Issues related to refresher training and legal indemnification need to be addressed before a reserve cadre of retired medical workers could be established. In addition, procedures for increasing the number of hospital beds and related health care assets need to be developed and implemented.

The Commonwealth must also develop working strategies for how the rapid statewide expansion of care can occur including the mobilization of field hospitals or establishment of alternate medical facilities such as schools, hotels, sporting arenas, etc. Another important component of this strategy is to formulate agreements with neighboring states enabling the use of medical personnel and health care assets from those states (see regional cooperation below).

First responder training. Updated and continuing courses/training for first responders related to incidents involving chemical, biological, radiological, and nuclear weapons must be an integral part of the instruction received by the firefighters, police, HAZMAT workers, public health personnel, doctors, and nurses, and other appropriate groups throughout the Commonwealth. Such instruction should be a component both of their initial training programs as well as periodic refresher courses and updated training during their careers. Legislation, probably at the federal level, should define uniform standards for training to help ensure that all individuals taking the courses, whether they be federal, state, and/or local representatives, receive compatible instruction.

Promote greater regional cooperation. The Commonwealth needs to continue to place emphasis on regional cooperation for the homeland security mission. This requirement became obvious following September 11 for several reasons. The impact of terrorist incidents can easily transcend state borders. For example, an outbreak of smallpox in the Commonwealth

could quickly spread to neighboring states and to the Nation as a whole. Moreover, for many potential terrorist incidents the number of casualties could quickly overwhelm area medical resources and hospitals. This could occur at a time when the assistance of medical personnel from neighboring states may not be readily available as such states consider their own needs and thus hold in reserve assets to cope with a terrorist incident that may engulf them as well. Nevertheless, advance planning to cope with the regional/national implications of bioterrorism is an urgent priority. This will require greater planning, cooperation, and joint exercises across state boundaries in and beyond New England.

Another important benefit of regional collaboration is that it may reduce the financial burdens of homeland defense to individual states by sharing resources. To be most effective, however, the Commonwealth should establish the specific arrangements for regional cooperation prior to the occurrence of an incident. One promising approach to regional collaboration would be to expand the charter of the existing New England Regional Coalition of Governors to include greater emphasis on emergency preparations and response to terrorist related incidents. In addition, where it has not already done so, the Commonwealth should conclude mutual aid agreements with neighboring states which allow Massachusetts to request out-of-state aid during an emergency situation in return for making available Commonwealth resources to out-of-state entities as needed. Finally, the Commonwealth, to the extent feasible, should work with the members of the New England Regional Coalition of Governors to harmonize, coordinate, and implement homeland security strategies.

Identify the Commonwealth's critical infrastructure and vulnerabilities. Continue to identify, update, and prioritize the inventory of the Commonwealth's critical infrastructure. This encompasses, but is not limited to: airports, sea and water ports, nuclear facilities, dams, water and sewer plants, electric power plants, gas pipelines, bridges, biological and chemical facilities, and our cyber infrastructure. Al Qaeda documents reveal a primary focus on three

categories of targets: those with high symbolic value such as the State House and the *USS Constitution*; targets with great commercial and economic value, such as skyscrapers, nuclear power plants, ports and railroad terminals; and, targets whose destruction would result in massive casualties, such as sporting events. Criteria being developed at the federal level to be provided to the states will furnish a clearer basis for prioritizing the Commonwealth's critical infrastructure. It will enable state emergency management officials to determine how best to defend the target as well as to plan for the range of possible consequences if an attack on a particular critical infrastructure node occurs.

Protect our seaports, harbors, and airports. Commonwealth agencies responsible for the protection of the state's harbors and airports, working closely with the U.S. Coast Guard and other relevant federal agencies, need to detect, intercept, and interdict potential threats as far away as possible to thwart criminal or catastrophic events. A strengthened partnership between federal and state agencies and the private sector must be established to provide more thorough protection of port facilities and airports.

As part of the effort to protect our harbors the federal and state law enforcement agencies including the Customs Department, the U.S. Coast Guard, and MASSPORT should adopt the Automated Manifest System (AMS) which helps identify high risk cargo containers. It is also necessary to work with the various maritime transportation lines to identify the true origin and destination of all sea cargo and containers. Moreover, it is important to construct a dedicated inspection site at Boston Harbor (and ideally at other Commonwealth seaports) that will provide a safe and secure location to inspect containers. Finally, the development of an effective and tamper-proof sensor and seal for containers is imperative. Current anti-tamper devices can be easily opened without the knowledge of maritime officials.

Foster closer relations with the private sector. Continue to develop a partnership with the private sector. Preparing for homeland securi-

ty needs to include the private sector as a vital partner in the war against terrorism considering that most of the Commonwealth's critical infrastructure is owned or operated by the private sector. One possible approach for engaging businesses and corporations in the Commonwealth is to establish a relationship between the relevant state and local first responders and the senior management and/or the head of security at key companies and corporations in Massachusetts in order to develop a foundation of partnership and planning for homeland security.

Ensure the compatibility of equipment. The Commonwealth needs to take the necessary steps to ensure the compatibility/interoperability of equipment related to emergency preparedness and response such as communication devices, respirators, and other emergency gear. Development of a state-wide communication system that encompasses interoperable/compatible telephone, radio, email, and cellular systems must be undertaken. State-wide communications systems will facilitate improved, more effective communication and cooperation among various law enforcement and emergency management agencies. The creation of such a capability is presently complicated by the fact that most cities and towns in the Commonwealth have independent, autonomous purchasing power. Nonetheless, such an effort is one of the Commonwealth's most important post-9/11 priorities.

Increase the use of simulations and related techniques. The use of simulations, tabletop activities, and "red teaming" that includes the participation of the appropriate federal, state, and local officials to help improve the Commonwealth's security against terrorist attacks should be expanded. They are indispensable tools for training, measuring readiness, and identifying shortcomings in plans, operations and tactics, and equipment (e.g., non-interoperable communication devices). In addition, they also offer valuable opportunities for face-to-face interactions and the experience of working together as well as the generation of mutual trust among federal, state, and local representatives who may need to respond as a team in the event of an actual terrorist incident.

Further increasing their utility, the lessons learned from simulation/tabletop exercises can easily be synthesized and then made available to officials throughout the Commonwealth who could not participate directly in the exercises. This would allow for better allocation and appropriation of resources and would facilitate common/compatible procedures and the use of best practices.

Develop a comprehensive media/public relations strategy. A terrorist incident, particularly if it involved the use of WMDs, could cause unprecedented casualties along with widespread fear, panic, and confusion. As a result, the Commonwealth must develop a comprehensive media and public relations plan to ensure that adequate procedures are in place to disseminate a consistent, reassuring message designed to allay public fears. The message would include information on the status of the incident, needed safety measures, locations of shelters, etc. Just as important as the provision of such information is understanding when to withhold sensitive data that, if made known, would serve only to create needless alarm and exacerbate fears. A key function of the plan would be to educate a select group of senior state officials, including first responders, public health officials, and other government personnel regarding effective approaches for dealing with both the media and public during serious crises.

The media/public relations effort would start with the Governor who is the Commonwealth's primary spokesperson to the citizens of Massachusetts. The Governor, along with other appropriate officials and experts, would provide up-to-date information. Given the ethnic diversity of the Commonwealth, information should also be disseminated in the languages spoken in particular communities. The media plan should also include creation of press kits for state and local media containing the names and contact data of local and national experts from whom the media can seek advice. Finally, the state should make sure that existing telephone and broadcast systems are capable of keeping government officials and the media connected during a crisis thus enabling

the dissemination of accurate, timely information to Commonwealth residents.

The Strategic Plan for Safeguarding the Commonwealth of Massachusetts Against Terrorist and Related Threats should be periodically reviewed, updated, and revised to take the fullest account possible of changing requirements for Commonwealth security.

The Institute for Foreign Policy Analysis, Inc. (IFPA) provides innovative studies, reports, briefings, publications, workshops, and conferences on critically important national security and foreign policy issues. IFPA's products and services are designed to assist federal, state, and local policy-makers, industry leaders, and broader policy communities in making informed decisions on such key issues as homeland security and U.S. political-military strategies, priorities, and capabilities in the uncertain world of the early twenty-first century. The Institute maintains a core staff of analysts based in Cambridge, Massachusetts and Washington, DC, together with a worldwide network of consultants. IFPA is associated with The Fletcher School, Tufts University.

675 Massachusetts Avenue
10th Floor
Cambridge, MA 02139
617 492-2116

1725 DeSales Street
Suite 402
Washington, DC 20036
202 785-2785

WWW.IFPA.ORG

MAIL@IFPA.ORG