

# EXECUTIVE SUMMARY

Few events have so crystallized the threat of terrorism that America's enemies pose to its people, its international stature, and its very civilization as have the attacks of September 11. America is dangerously vulnerable to this new form of terrorism. New means are needed to rapidly strengthen the security of the American homeland—to protect critical infrastructure, boost civil defense, and increase intelligence and military structures in order to prevent future attacks and limit the effects should one occur.

Many steps already have been taken by the Administration and Congress, such as creating the Office of Homeland Security and appointing former Pennsylvania Governor Tom Ridge to direct it as Assistant to the President for Homeland Security. But much more needs to be done.

The Heritage Foundation Homeland Security Task Force, formed shortly after the September 11 attacks with some of the best homeland security experts in the world, sought to address this need by reviewing the vast number of proposals put forth by commissions and legislative initiatives. Its members agreed unanimously that there no longer was a need to describe the threat to the homeland or to justify making homeland security a higher national priority. Rather, they saw a need to develop top priorities for action at all levels of government and to devise concrete steps to implement these priorities and make them operational. Their recommendations for action are as follows.

## PROTECTING THE NATION'S INFRASTRUCTURE

Most Americans recognize that protecting critical infrastructure from acts of terrorism is a responsibility that does not rest with any one level of government. Structural, cultural, institutional, and statutory changes are needed to secure the nation's critical infrastructure so that terrorists have less incentive to target them and the nation can respond quickly if they do. The success of efforts to defend and protect infrastructure will rest primarily on the ability of Federal, State, and Local governments to communicate and cooperate effectively with each other and with the private sector.

To protect America's critical infrastructure, such as communication networks, utilities and water supplies, banking and finance systems, transportation nodes, and

intelligence systems, the Working Group on Infrastructure Protection and Internal Security has established the following top priorities for Federal, State, and Local efforts.

- **Priority #1: Reorganize by presidential directive all Federal agencies involved in protecting critical infrastructure.** The President should reorganize the Federal government to enhance its ability to protect the homeland. President Bill Clinton issued an infrastructure protection directive, known as PDD-63, to assign responsibility for addressing the security of 12 specific infrastructure sectors to various Federal agencies. However, his directive failed to create a system of oversight or establish a clear chain of command to ensure that agency efforts were adequately enhancing the security of these sectors. The new presidential directive should correct this deficiency by requiring annual assessments of Federal agency efforts; clarifying the chain of command for infrastructure protection efforts that involve Congress, State and Local entities, as well as the private sector; and improving coordination and information sharing.
- **Priority #2: Designate the Global Positioning System (GPS) frequencies and network as critical national infrastructure.** The GPS satellite network is an enabling system for other infrastructure systems, such as telecommunications, that are vital to the nation's security. Disruption by terrorist groups or hostile states could jeopardize America's homeland security, but the GPS has not been designated as a vital national asset. President George W. Bush should immediately add the GPS to the current list of vital national infrastructure and assign responsibility for its security to the U.S. Department of Defense (DOD). Immediate steps should begin to make the GPS network more secure.
- **Priority #3: Facilitate communication on infrastructure issues between the new Office of Homeland Security (OHS) and State and Local officials.** State and Local governments play a vital role in protecting the infrastructure within their jurisdictions. In the event of a possible terrorist attack, however, they cannot do so effectively without communications from the Federal government. Before such communications—which could include classified information—can occur, many States will need to reform their public meeting disclosure laws so that information concerning suspected terrorist activities and vulnerable infrastructure will not be made public and compromise prevention, apprehension, and deterrence. Appropriate response exercises that include the relevant Federal, State, and Local officials should be conducted for various attack scenarios, which will enable better communications should an attack occur.
- **Priority #4: Enhance the private sector's role in infrastructure protection.** Market forces provide a strong incentive for the private sector to protect any infrastructure it owns and operates. Government should not inhibit industry

efforts to do so, and it should ensure that businesses have the tools they need to increase their ability to protect vital infrastructure, such as telecommunication networks. Congress should remove any legislative roadblocks that exist to improved communications with the private sector, and tax penalties that make it more difficult for private industry to invest in greater security should be eliminated. Moreover, new security standards for protecting each type of infrastructure and new risk assessment programs should be developed and shared with the relevant businesses.

- **Priority #5: Institute new rules to monitor more closely who or what is entering America's airports and seaports.** Since September 11, new efforts to increase security at vital transportation nodes have focused primarily on manpower, such as federalizing baggage handlers at airports. A comprehensive program to increase airport and seaport security requires tighter controls on who and what is passing through America's portals. New Federal systems should be developed to share passenger information that would help prevent a potential terrorist from even boarding a plane. A Federal interagency center also will be needed to analyze information about the people and products entering the United States by sea. The U.S. Customs Service should begin experimenting with a point-of-origin inspection program for maritime trade. The Sea Marshals program should be expanded quickly. And the Transportation Security Agency should issue a new regulation to require airports and port administrations to assure that only authorized people can enter secure areas.
- **Priority #6: Secure all Federal networks and information systems.** The U.S. General Accounting Office has reported that the information systems vital to Federal operations are not sufficiently protected. Without tighter security, continuity of operations cannot be guaranteed. Federal agency technology-purchasing guidelines should be revised to place a premium on security. The executive branch also should explore alternatives to the proposed government-only Internet system (GOVNET) before making a procurement decision.
- **Priority #7: Accelerate government compliance with the Nuclear Waste Policy Act.** Despite legislation requiring that it do so, the U.S. Department of Energy (DOE) has not uniformly secured the nation's nuclear waste, which could be used by terrorists to build radiologic weapons. According to the department, it is already running 12 years behind schedule. Congress should hold hearings to determine how DOE can bring the new storage facility at Yucca Mountain, Nevada, on-line more quickly and improve security.

## STRENGTHENING CIVIL DEFENSE AGAINST TERRORISM

Unlike defending the nation from military attacks, civil defense begins with preparation and planning at the local level. The first responders to an emergency are usually local emergency workers and volunteers—a fact poignantly illustrated on September 11. Should terrorism occur again in the United States, America's firefighters, law enforcement officials, emergency medical services personnel, health professionals, and hazardous materials crews will be the front-line fighters. However, they are not adequately prepared today to respond to or prevent a terrorist attack using weapons of mass destruction.

To assist Local, State, and Federal officials in improving their ability to detect and respond to an attack on civilians using chemical, biological, radiologic, or nuclear (CBRN) agents, the Working Group on Civil Defense Against Weapons of Mass Destruction has established the following top priorities.

- **Priority #1: Build a nationwide surveillance network for early detection of chemical, biological, or other attacks.** In order to mobilize a rapid response to such attacks, government officials must be able to recognize the initial stages of an outbreak of catastrophic illness or attacks on food and water supplies. This requires a nationwide network of locally based surveillance procedures and systems to monitor these vital sectors, and nationally developed monitoring standards and reporting guidelines so that information can be disseminated quickly. The Federal government should also take steps to foster the development of more sensitive monitoring technologies.
- **Priority #2: Develop a terrorism response checklist and a manual of civil defense exercises to guide officials in assessing preparedness.** Local and State authorities must prioritize the elements of any effort to improve the ability to respond to a CBRN event. The Federal government should assist the states by developing national standards of preparedness and by designing new evaluation tools to help them assess their own weaknesses and to determine how best to proceed. The guides, developed by a task force under the direction of the OHS, should be completed within the next six months and made available on the Web site of the Centers for Disease Control and Prevention (CDC). In addition, the Federal government should conduct CBRN response exercises, first with states most at risk of terrorism and building gradually to multi-state exercises over time.
- **Priority #3: Accelerate the development of pharmaceuticals that prevent or limit the spread of toxic agents by terrorists.** Given the urgency of protecting Americans from biological terrorism, which followed the recent anthrax deaths, the Federal government should facilitate more rapid development and supply of new and safer vaccines, drugs, and other medicines that would

provide immunity to such diseases as smallpox or that would limit the effects of an outbreak after a terrorist incident. This will involve establishing reasonable requests for proposals for developing CBRN-related pharmaceuticals; guaranteeing patent protection for products related to terrorism; improving the fast-track approval process for these products; and stimulating the development of generic drugs after patents have expired.

- **Priority #4: Create a national web of CBRN experts who will train first-response teams for an outbreak or terrorist attack.** A program that can identify these experts and deploy them in teams to share their expertise and train local first responders would be an affordable and effective way to prepare for a CBRN attack. Congress should provide adequate funding for expanding the Train-the-Trainer programs in the Office for Domestic Preparedness.
- **Priority #5: Simplify the process of obtaining Federal assistance for civil defense initiatives.** An OHS block grant program should be established so that State and Local authorities can target federal funding to their unique civil defense needs. Current agency grant programs should be streamlined into a single grant application process administered by the OHS. To ensure that federal funds get to the localities that need them the most to boost preparedness, a new homeland security block grant program also should be established under the Federal Emergency Management Agency (FEMA). All grants should be conditional, non-transferable, and made accountable through new reporting requirements.
- **Priority #6: Sign mutual support agreements with Canada and Mexico on responses to terrorist acts in border communities.** The possibility exists that a terrorist could release a biological or radiologic attack on the United States without ever crossing the border, with serious consequences for people in both countries. The United States should sign mutual terrorism support agreements with Canada and Mexico on preventing such attacks and managing their consequences should they occur.
- **Priority #7: Develop a nationwide education and public relations program.** In a democracy, governments at all levels must mitigate fears of attack while building support for their efforts to protect the public. Public relations campaigns can be vital to preventing panic, improving civil defense preparedness and responses, and maximizing all efforts to prevent terrorism. Successful campaigns will require a terrorism-related public relations strategy for improving cooperation with local media to enhance the dissemination of information to the public.

## IMPROVING INTELLIGENCE AND LAW ENFORCEMENT CAPABILITIES

Since September 11, many are questioning the ability of government agencies to gather and communicate actionable intelligence to enable them to apprehend terrorists before they strike and to deter them in the future. Federal, State, and Local officials recognize that more resources must be focused on improving intelligence so that government agencies, emergency personnel, and first responders can more effectively respond to those who would harm American civilians.

The capabilities of and relationships between law enforcement agencies (LEAs) at the Federal, State, and Local levels and the Intelligence Community have received comprehensive reviews, such as in hearings before the House Permanent Select Committee on Intelligence and in its 1995 report, *Intelligence Community in the 21st Century*; by the 1996 Brown–Rudman Commission; and in more recent reviews by the Hart–Rudman, Bremer, and Gilmore Commissions. Many of the excellent recommendations made by these commissions and studies have yet to be fully implemented.

September 11 sent a powerful message to decision-makers that much more needs to be done to protect the homeland, and quickly. The Administration and Congress have sought to address some of the bureaucratic problems exposed by the attacks by passing the USA PATRIOT Act (P.L. 107–56) and the FY 2002 Intelligence Authorization Act (H.R. 2883). They recognize that no single action, law, or institution—no one-step remedy—will combat all of the threats the United States and its citizens face.

A multifaceted approach to homeland security is necessary. Building on the recommendations of earlier commissions and post-September 11 legislative efforts, the Working Group on Intelligence and Law Enforcement has identified the following top priorities for improving the ability of law enforcement agencies and the Intelligence Community to protect the homeland.

- **Priority #1: Require the Office of Homeland Security to direct the assessment of threats to critical assets nationwide.** The first important step in homeland defense is providing appropriate information to government officials to help them determine what assets, critical to the nation's economy and security, remain vulnerable to terrorist attack and whether the responsible agencies and institutions are organized and equipped sufficiently to protect them. A first step in this process must be the development by the OHS of a uniform methodology for assessing the risk to possible targets and the level of threat to those targets, and establishing the methods for sharing the findings. Based on the compiled assessments, the OHS Director should establish a

national strategy for protecting the homeland and direct his office to develop a national alert and warning system.

- **Priority #2: Rapidly improve information-gathering capabilities at all levels of government.** For Federal, State, and Local law enforcement officials, a first line of defense against terrorism and other threats to the homeland is access to timely, reliable, and actionable information from both foreign and domestic sources. Rapidly enhancing government's ability to acquire and analyze this information is vital to homeland security. The President should direct the Director of OHS to establish a national intelligence coordinating group whose task is to develop a national strategy for gathering and sharing intelligence. More federal resources should be targeted to strengthening foreign intelligence-collection capabilities, as well as domestic sources of information critical to homeland defense. This includes strengthening the measurement and signature intelligence (MASINT) capabilities of the Intelligence Community and maximizing current agency capabilities to cross-cue intelligence and increase human intelligence (HUMINT).
- **Priority #3: Improve intelligence and information sharing among all levels of government with homeland security responsibilities.** The need for better sharing and dissemination of acquired information to all levels of government became clearer in the days following September 11, but improving LEA–Intelligence Community cooperation will have far more to do with changing bureaucratic cultures that resist change than with revising current statutes or regulations. The President should direct the appropriate Cabinet Secretaries and officials to work together to create an all-source Federal-level information fusion center, to which all intelligence information goes and from which it is disseminated on a need-to-know basis. The OHS Director should develop a cooperative structure for the sharing and disseminating of this information, which will include classified information. Federal funding and training should be targeted to assist State and Local LEA information-gathering efforts.
- **Priority #4: Strengthen the visa approval and border security mechanisms.** Legally entering the United States was remarkably easy for the September 11 terrorists. America's visa approval and entry–exit processes, and the ability of LEAs to enforce existing immigration laws against aliens who are in violation of those or other laws, should be strengthened. Consular officers need more information upon which to make their decision about granting each visa. A Federal-level lookout database should be created and made accessible to officials involved in border security. The “45-minute” rule that requires Immigration and Naturalization Service (INS) inspectors to clear all passengers on international flights into the United States within that time period should be repealed. The Visa Waiver Program law should be amended to allow the

Secretary of State to use it to encourage countries to institute greater anti-terrorism border control mechanisms. The U.S. government should expedite the development of tamper-proof travel documents, explore the development of an exit monitoring mechanism, strengthen INS's ability to enforce the law against aliens who violate their visas, institute comprehensive procedures for handling immigration cases that involve classified documents, and help State and Local LEAs develop a standard format for "rap sheets."

- **Priority #5: Eliminate the opportunities for identity theft and fraud in state identity document systems.** False identity documents are a major problem, and the terrorists involved in the September 11 attacks exploited the States that have the systems most liable to fraud. Any State that continues to run a document system subject to fraud and abuse must recognize that it is placing the lives of Americans in jeopardy. Current procedures for the issuance and recording of identity documents, such as driver's licenses and birth and death certificates, must be tightened and a mechanism developed to deter and prevent identity theft. Development of tamper-proof documents should be a priority.
- **Priority #6: Create a mechanism to monitor recent anti-money-laundering initiatives to obstruct the financing of terrorism.** Many of the deficiencies of efforts before September 11 to obstruct the financing of terrorist activities were addressed in the USA PATRIOT Act, but the financial services area is dynamic, and those who seek to harm the United States will continue to attempt to circumvent the current regulatory structures. To better anticipate how existing anti-money-laundering restrictions can be circumvented, the Secretary of the Treasury should create a mechanism to evaluate the current laws.

## MILITARY OPERATIONS TO COMBAT TERRORISM

The 1997 National Defense Panel (NDP) report is but one of many that gave clear warnings to the people and policymakers that the United States homeland was at risk of terrorist attack. Other studies made it clear that the U.S. armed forces must be prepared not only to identify impending catastrophic terrorist attacks, but also to preempt or respond to them rapidly, working with the Intelligence Community and Federal, State, and Local officials.

In any restructuring of the forces to meet a rising threat, care must be taken to ensure a continued balance between unconventional and conventional force capabilities. A number of studies have suggested how to accomplish these objectives, but their recommendations have not been systematically implemented.

The Heritage Foundation Working Group on Military Operations has attempted to address this problem by identifying the following top priorities for improving military anti-terrorism operations to defend the homeland.

- **Priority #1: Free the National Guard and Reserves for homeland security and boost port security quickly.** Homeland security will require enhancing the capabilities of National Guard and Reserve units to respond to terrorist events. This means freeing some of these units from having to provide combat support and combat service support for the active forces by adding more active duty personnel to current force levels. It means ensuring that the National Guard has standing emergency plans to train and work with Local authorities on homeland defense and consequence management. It will require the development of coordinated public information campaigns. It also will require reinstating a U.S. Navy–U.S. Coast Guard coordinated port security program to check all incoming ships and containers to prevent weapons of mass destruction from entering the United States.
- **Priority #2: Protect U.S. borders, coasts, and critical national infrastructure with air defense and missile defense.** The threat of attack by aircraft, cruise missiles, and ballistic missiles requires that the United States establish a robust air and cruise missile defense system and begin testing ballistic missile defenses on land and at sea at full design capability. Congress should provide additional funding for the deployment of a cruise missile defense system as a component of homeland defense. And the Pentagon should deploy air defense and cruise missile defense systems to defend major U.S. cities and critical infrastructure.
- **Priority #3: Enhance rear-area military operations to protect the homeland and prepare for terrorist attacks.** The U.S. military can assist Local, State, and Federal authorities in counterterrorism efforts by identifying critical infrastructure nodes; assessing their security levels; providing protection for them as needed as well as redundant communications, command, and control systems; and procuring and maintaining equipment to assist in the local responses to terrorist attacks. To achieve this goal, the commander in chief (CINC) for homeland defense should be the Joint Forces Command CINC. The Secretary of Defense should develop a refined list of military responses to domestic terrorist attacks and a network of interactive command-and-control centers and service mobilization directorates to enable better coordination with Federal and State agencies. The service branches should provide training to the National Guard, FEMA, and other appropriate Federal and State agencies on incident response and mitigation. And all components of the Joint Forces Command should be enabled to task units to respond to incidents around the entire country.

- **Priority #4: Provide intelligence support for military operations.** Effective military operations depend on timely and accurate intelligence about enemy forces, movements, capabilities, and intentions. Real-time, all-source intelligence fusion centers are required for effective counterterrorism military operations and homeland defense. Several of the September 11 terrorists were on different government watch lists, but these databases were not linked for common retrieval of information. To protect the homeland, the U.S. Department of Defense should institute local, low-level counterintelligence source operations for force protection near military installations. To give DOD access to cross-referenced strategic and critical databases, which are currently housed in various Federal agencies, will require establishing fusion centers at the Federal, State, and Local levels (where necessary) and staffing them with personnel who have appropriate clearances for classified information.
- **Priority #5: Ensure clear command and control of overseas anti-terrorism operations.** Regardless of whether military operations are of an offensive or defensive nature, the geographic Unified Command (such as PACOM, or CENTCOM, which is directing the war in Afghanistan) must be the command-and-control headquarters for overseas military operations. In military parlance, this means that the geographic Unified Command will be the supported command and the war fighter. The United States Special Operations Command (SOCOM) should be the primary force provider (supporting commander in chief or CINC), not the major war fighter, and the specified supporting command for managing counterterrorism operations. The Secretary of Defense should ensure that SOCOM has the authority and resources it needs to carry out this mission. The CINC for homeland defense should prepare pre-planned force packages for initiating rapid responses to terrorism contingencies.

# TOP PRIORITIES FOR PROTECTING THE NATION'S INFRASTRUCTURE

*A Report of the Working Group on Infrastructure Protection and Internal Security<sup>1</sup>*

Michael Scardaville, Working Group Rapporteur

The aftermath of the September 11, 2001, attacks on the Pentagon and the World Trade Center illustrates the high vulnerability of America's infrastructure to terrorist attacks and the massive consequences of not protecting it. While the terrorists were able to utilize deficiencies in America's overall approach to intelligence sharing and aviation security, similar vulnerabilities exist in every infrastructure vital to the security, economy, and survival of the nation, such as computer networks, energy supplies, transportation, and the global positioning satellite system.

Today, most Americans recognize that responsibility for protecting critical infrastructure from terrorism does not rest with any one level of government. Structural, cultural, institutional, and statutory changes are needed to secure the nation's infrastructure so that terrorists have less incentive to attack them and the nation can respond quickly if they do. Primarily, the success of efforts to defend and protect

- 
1. The members of the Working Group on Infrastructure Protection and Internal Security are The Honorable Carol Hallett, President and CEO of the Air Transport Association; The Honorable Frank Keating, Governor of Oklahoma; Jules McNeff, Director, U.S. GPS Industry Council, with SAIC; Col. Joseph Muckerman, USA (Ret.), former Director of Emergency Management, Office of the Secretary of Defense; Captain Bruce Stubbs, USCG (Ret.), Technical Director, Theater Air Defense, Systems Engineering Group, Anteon Corporation; Thomas L. Varney, Director of Technology Assurance and Security, McDonald's Corporation; and The Honorable Pete Wilson, former Governor of California. The following individuals contributed to this report in an advisory capacity: Dr. Billy Cook, MTS Technologies, Inc.; Richard J. Doubrava, Managing Director, Security, Air Transport Association; Rob Houseman, Counsel, Bracewell and Patterson; John M. Meenan, Senior Vice President, Industry Policy, Air Transport Association; Edward A. Merlis, Senior Vice President, Legislative and International Affairs, Air Transport Association; Robert W. Poole, Jr., Director of Transportation Studies, Reason Public Policy Institute; John Powers, Executive Director, President's Commission on Critical Infrastructure Protection; Kenneth P. Quinn, Partner, Pillsbury Winthrop LLP; Scott Rayder, Director of Government Relations, Consortium for Ocean Research; Maureen Sirhal, reporter, *Technology Daily*; and Gary Tyler, Director, Matcom Corporation.