

APPENDIX: SUMMARY OF CHAPTER RECOMMENDATIONS

1. INTRODUCTION: BUILDING HOMELAND SECURITY IN OUR CITIES AND STATES

- 1.1 Every major metropolitan area should have complete vulnerability and mitigation assessments.
- 1.2 Every major metropolitan area should have personal protective equipment for all first responders.
- 1.3 Every major metropolitan area should have interoperable communications.
- 1.4 Every major metropolitan area should have a public health and biological/chemical/radiological surveillance system.
- 1.5 Every major metropolitan area should have an intelligence collection and sharing program.
- 1.6 Every major metropolitan area should conduct realistic training and preparedness exercises.
- 1.7 Every major metropolitan area should have closed-circuit television (CCTV) systems to secure infrastructure.
- 1.8 Every metropolitan area should have an enhanced security program for public transportation.
- 1.9 Metropolitan areas should create and periodically test evacuation/shelter-in-place plans.

2. A COUNTERTERRORISM POLICY FOR OUR OWN BACKYARD

- 2.1 Create COPS II first preventers program.
- 2.2 Build and inspire a culture of “first preventers.”
- 2.3 The homeland security secretary should create a regional network integrated with state and local fusion centers for coordinating prevention, preparedness, and response activities with the states and municipal areas.

- 2.4 The Department of Homeland Security (DHS) should establish standards for collection, analysis, and reporting for state and local intelligence fusion centers.
- 2.5 Provide advanced prevention training and proper security clearances.
- 2.6 Ensure that prevention training and exercises include realistic adversarial play for scenarios involving both conventional attacks and weapons of mass destruction (WMD).

3. SECURITY FOR A NATION IN MOTION

- 3.1 Increase visibility and frequency of personnel and increase use of CCTV systems.
- 3.2 Promote public engagement to foster security awareness.
- 3.3 Ensure interoperable communications systems and robust command and control systems are extended to ground transportation systems.
- 3.4 Conduct annual vulnerability assessments and review potential threats, vulnerabilities, and risks with local and federal officials.
- 3.5 Ensure adequacy of crisis management and communications plans, awareness of plans, readiness of equipment and personnel, and accuracy of all contact information.
- 3.6 Continue development of new explosive and WMD detection and countermeasures. Allow the use of DHS grant money for deployment of canine detection until effective detection technologies can be brought to bear.
- 3.7 Direct federal funding to support capital improvements that will help prevent attacks, mitigate their effects during an attack, and allow the transit system to be rapidly recoverable.

4. A HEALTHY MEDICAL RESPONSE SYSTEM

- 4.1 Metropolitan health and hospital plans should be developed based on federally set standards; federal funding initially should be targeted at our largest cities.
- 4.2 Detection systems for chemical weapons should be installed in subways and metro stations, convention and athletic centers, and other public areas where large numbers of people congregate.

- 4.3 BioWatch must be redesigned to include developing cooperative agreements for the maintenance of the systems and the use of the data; increasing the number of air monitoring stations in each city to 40 to 60; and the fast-tracking of research for real-time detection.
- 4.4 Building syndromic surveillance systems in all major metropolitan areas and tying them into a federal backbone should be a top priority of the Centers for Disease Control and the DHS.
- 4.5 The Strategic National Stockpile (SNS) should revert to the Department of Health and Human Services with a DHS liaison; the SNS formulary should be released to local officials with a legitimate need to know; the program should be expanded to include treatment for radiation sickness and additional all-hazards material; the Vendor Managed Inventory should be expanded to include food, water, and other basic supplies.
- 4.6 The CHEMPACK program should be redesigned to put the antidotes in mobile emergency units.
- 4.7 The Cities Readiness Initiative (CRI) should be redesigned based on input from the public health community; funding should be provided to hire a fulltime CRI coordinator for each metropolitan area with the goal of implementing a plan within one year.
- 4.8 Additional financial incentives and policy adjustments must be made to bring private sector interest to the BioShield program.
- 4.9 Decision makers at local, state, and national levels must prepare graduated quarantine measures; plans to carry out quarantine must be prepared and drilled; states that do not have the authority to quarantine should make necessary legal modifications.
- 4.10 Hospital surge capacity must be built, starting with the nation's largest metropolitan areas.

5. INTRODUCTION: A NEW APPROACH TO THE PRIVATE SECTOR AND HOMELAND SECURITY

- 5.1 Focus on securing high-impact targets and assuring continuity of essential systems over a blanket approach to critical infrastructure.

- 5.2 Establish joint planning committees for each HITS and ACES sector. Exercise authority under Section 871 of the Homeland Security Act of 2002 to exempt joint planning committees from FACA. Amend provisions of relevant anti-trust laws to exempt explicitly standard-setting discussions and planning sessions. Establish a congressional select committee to oversee joint planning.
- 5.3 Once established, these committees should develop infrastructure security plans that specify the security end-state to be achieved, goals and milestones for achieving it, standards for implementation and compliance, and timelines for accomplishing intermediate actions.
- 5.4 Integrate chief executive review into joint planning process; obtain approval and commitment to carry out plans according to agreed upon timelines.
- 5.5 Implement the Infrastructure Protection Regional Security and Area Security framework as set out in the Chemical Facility Anti-Terrorism Act of 2005.
- 5.6 Adopt smart regulation on a sector-by-sector basis to encourage the development and implementation of appropriate security measures.
- 5.7 Revamp the Terrorism Risk Insurance Act (TRIA) to promote risk mitigation and create a safe harbor against litigation following a terrorist attack where targeted companies have complied with government-approved security standards.
- 5.8 Develop a CEO-level system for managing resource allocations during recovery and reconstitution phases following a catastrophic national event to allow a coordinated effort with the federal government.

6. FINANCIAL SERVICES: LEARNING FROM SUCCESS

- 6.1 Diverse and resilient communication channels are essential. Elements such as cell phones, wireless e-mail devices, landline phones, and the Internet are required.
- 6.2 The power grid must be considered among the most vital of critical infrastructures and needs investment to make sure it works across the nation.

- 6.3 Recognize the interdependencies among critical infrastructure sectors.
- 6.4 Recognize the dependency of critical infrastructures on software operating systems and the Internet.
- 6.5 As Hurricane Katrina has poignantly illustrated, establishing improved coordination procedures across all critical infrastructures and with federal, state, and local government is essential to rapid, coordinated, and effective response when events occur. To minimize the economic and social risks during a crisis, coordination in planning and response between the private sector and public emergency management must improve.

7. CHEMICAL PLANT SECURITY: PREVENTING A TERRORIST BHOPAL

- 7.1 Providing a stronger framework for developing regulations that will focus companies on investing in passive security over active security.
- 7.2 Using a “design basis threat” for developing security requirements for facilities in the highest-risk tier.
- 7.3 Giving security personnel at high-risk facilities the legal authority to use deadly force against attackers.
- 7.4 Establishing a training and certification program under which security professionals can conduct vulnerability assessments and establish security plans.
- 7.5 Providing liability protection and terrorism insurance premium reductions for facilities certified as being compliant.

8. PROTECTING ENERGY INFRASTRUCTURE

- 8.1 Relocate the most vulnerable assets, such as LNG terminals, away from population centers. Where this is not feasible, mandate increased security measures.
- 8.2 Increase the redundancy of our energy infrastructure to reduce vulnerability.
- 8.3 Increase system resiliency and recovery speed.

- 8.4 Strengthen other infrastructures and systems, those that both support and depend on energy systems.
- 8.5 Focus on energy security, that is, the long-term availability of reliable, affordable energy supplies to the nation.
- 8.6 Increase the use of small-scale distributed generation (including renewables and combined heat and power) close to energy users.
- 8.7 Increase investment in research, development, and deployment of designs that will make energy infrastructures and networks more resilient and resistant to failure.

9. CYBER SECURITY: A SILENT CATASTROPHE

- 9.1 A new national information assurance policy should formally establish a framework for protecting critical cyber systems.
- 9.2 The directive should clarify roles and responsibilities, eliminating overlapping responsibilities.
- 9.3 A single committee should replace the six that currently advise the federal government on cyber security and should reside in the White House.
- 9.4 The position of cyber czar should be reinstated and, among other duties, should head the committee.
- 9.5 Joint exercises involving the DHS and the Department of Defense, as well as key players in the private sector, should be held to test capabilities and coordination.
- 9.6 Defense Indications and Warnings efforts must be expanded and fully integrated into a national cyber attack sensing, warning, and response capability.
- 9.7 The position of assistant secretary for cyber security and telecommunications must be filled immediately.
- 9.8 A concerted effort must be made to develop and deploy resilient networks.
- 9.9 A synoptic, real-time view of the condition of key cyber nodes and systems throughout the United States should be developed.
- 9.10 Legislative changes concerning public-private partnerships and information sharing and protection should be made.
- 9.11 Legislative changes to the Wartime Production Act to bring those emergency powers into the information age should be made.

- 9.12 Increased sentencing guidelines that treat cyber crimes as real crimes and deter would-be hackers should be put in place.
- 9.13 In support of this directive, an annual report should be prepared for the president for his approval, including a requirements-driven multiyear budget, research and development plan, and roles and missions statements for all relevant agencies, including the Department of Defense, the FBI, the CIA, the National Security Agency, and the DHS.

10. INTRODUCTION: FEDERAL ROLES AND RESPONSIBILITIES

- 10.1 Abolish the Homeland Security Council and strengthen homeland security policy and functionality within the National Security Council.
- 10.2 Establish DHS domestic regions to push disaster management, infrastructure protection, and intelligence out to states and localities. These should be based on the eight existing Federal Emergency Management Agency (FEMA) regions.
- 10.3 Reestablish FEMA as an independent cabinet-level agency.
- 10.4 Resist structural solutions to functional problems.
- 10.5 Provide adequate funding for homeland security missions under an integrated homeland security budget strategy.
- 10.6 Push for congressional reform to limit the number of committees with jurisdiction over homeland security operations.

11. EMERGENCY RESPONSE: RESTORING DISCARDED STRATEGIES THAT WORKED

- 11.1 Reestablish FEMA as an independent cabinet-level agency.
- 11.2 Review existing authorities for federal management of disasters when local authorities are overwhelmed.
- 11.3 Make FEMA once again an international leader in emergency management and use the agency as a tool of public diplomacy.
- 11.4 Establish two new White House positions: deputy assistant to the president for crisis management; and special assistant to the president for emergency preparedness.

- 11.5 Designate FEMA as the executive agent for federal disaster planning and liaison and coordination with state and local governments and the lead agency for federal disaster crisis management in the field, whether in support of state and local efforts or as the overall controlling organization.
- 11.6 Invigorate Project Impact and ensure that local authorities have the medical and interoperable mobile communications capabilities to spur development of “disaster-resistant” cities.
- 11.7 Develop communication strategies for informing the public and inspiring confidence in crises, while avoiding undue risk to law enforcement or intelligence collection efforts.
- 11.8 Focus on making the Homeland Security Advisory System useful.
- 11.9 Create law enforcement response teams (LERTs) to help reestablish order following catastrophic incidents.
- 11.10 Involve the private sector in planning and preparation for catastrophic terrorist attack.

12. AN INTELLIGENCE APPROACH TO DOMESTIC SECURITY

- 12.1 The president should establish by executive order an intelligence transformation group (ITG)—or its functional equivalent—of the National Security Council, chaired by the president with delegation to the national security advisor, to include the secretary of defense, the secretary of homeland security, the attorney general, and the director of national intelligence.
- 12.2 Resist structural buildup. The hasty establishment of the TTIC and National Counterterrorism Center (NCTC) taught us that the resistance encountered to these centralized models was in part the result of legitimate leadership concern about degrading critical capabilities needed in an increasingly decentralized intelligence community.
- 12.3 Strengthen the DHS’s intelligence role. The president should publicly, as well as in his leadership of the ITG, make clear his support for DHS as an intelligence assessment and sharing center. Under this arrangement, the FBI must share information with DHS and, through DHS, state and local authorities. A joint DHS-FBI committee on intelligence chaired by the White House would ensure that sharing of information became a reality.

- 12.4 Use regional offices for information sharing. The DHS second-stage review should be revised to give the secretary responsibility for assuring a two-way intelligence exchange with state and local governments—as well as with the twenty-two agencies incorporated into DHS.
- 12.5 Clarify the FBI's particular role in domestic intelligence. The FBI, its fifty-six field stations, and its growing network of Joint Terrorism Task Forces (JTTFs) have a part to play in the development of a national intelligence capability, which in an ideal world would be a collaborative and not a leading role. We should, once and for all, lower expectations of the Bureau's intelligence role. The FBI should not be expected to produce at a local level either the authoritative analysis or the integrated collection assessments that it cannot provide nationally.
- 12.6 Clarify departmental roles and responsibilities. The president and the ITG should work urgently to clarify roles and responsibilities of key agencies with responsibilities for intelligence and homeland security missions. The NCTC, the DHS, the Department of Defense (especially Northern Command), the CIA, and the FBI, while understandably enlarging their missions, are bumping into each other in the integration of foreign and domestic intelligence, and colliding in establishing working relationships with state and local governments. This is a manageable problem if caught early, but a serious issue with implications for preparedness, response, and civil liberties if ignored.
- 12.7 Promote government-wide information sharing. The program director for information sharing, a position given government-wide authorities by statute, should be placed in the National Security Council (NSC), not under the DNI, where it recently has been placed by the White House at least partly on the misguided recommendation of the WMD Commission.
- 12.8 Make the National Counterterrorism Center (NCTC) work. The NCTC, now a key institution, will continue to struggle to establish itself as the dominant provider of terrorism analysis because of the long-standing and growing pressures for decentralization of analytic production in the intelligence, defense, and law enforcement communities.

- 12.9 Support the director of national intelligence, but hold him accountable. The president and the ITG should actively support and carefully monitor the implementation of the director of national intelligence's agenda to reform management, to professionalize the intelligence service, and to improve intelligence collection and analysis.
- 12.10 Clarify the CIA's role under the director of national intelligence (DNI).
- 12.11 Push congressional reform. On domestic intelligence, it appears that some overseers are more protective of the FBI than they are disappointed with its post-September 11 performance. None of this has changed the inadequate oversight of the intelligence committees or otherwise gone far enough to align, in any lasting way, executive and legislative branch priorities for intelligence community reform.

13. LOSING FOCUS ON AVIATION SECURITY

- 13.1 Passenger screening
- ◆ The Transportation Security Agency (TSA) needs to bring Secure Flight online as rapidly as possible. The TSA must assure passengers that their personal information will be strictly safeguarded from unauthorized use, and will be used only for the purposes of distinguishing high-risk from low-risk passengers. The TSA may also consider segmenting the passenger population into travelers who are willing to give extra personal information for Secure Flight and those who are not willing to provide information.
 - ◆ Several technologies may potentially help to improve passenger screening at security checkpoints. One option is the multiview X-ray, which provides screeners with much higher resolution images that can be rotated on the screening monitor in order to improve detection rates. A second and more traditional option is to expand the canine explosive detection teams to operate at security checkpoints.
 - ◆ To keep screeners sharp and alert, the TSA should expand the use of the Threat Image Projection (TIP) program.

- ◆ Biometric identity verification is the obvious next step to enhancing screening effectiveness. The TSA's Registered Traveler pilot program, which uses iris and fingerprint verification, was completed on September 30, 2005, and seems to have been a widespread success. The TSA should aim for a quick review and expansion of this program to all major airports.
- 13.2 Checked baggage security
- ◆ The TSA should develop a plan to rapidly deploy in-line EDS systems at the busiest passenger airports, and ultimately at all passenger airports.
 - ◆ Screeners should have access to ongoing training and every Online Training Center should be available by high-speed Internet so that trainers can access and complete training courses more rapidly. TSA should also systematically monitor and document the completion of required screener training.
- 13.3 Air cargo security
- ◆ The TSA should screen all of the cargo that travels by passenger aircraft with canine explosives detection teams and machines.
 - ◆ Cargo containers should also be sealed with tamper-evident tape, which offers a visual indication of tampering at a very low cost.
 - ◆ The use of hardened unit loading devices (HULDs) should also be explored more vigorously.
 - ◆ The TSA should make the Known Shipper Program mandatory for air carriers and should develop strict monitoring procedures to verify that shippers in the database are actually securing their cargo according to TSA standards.
- 13.4 Shoulder-fired missile threat
- ◆ The TSA should vigorously explore and test countermeasures for airlines against these weapons. Countermeasures should contribute to a layered defense, including securing a perimeter around airports that would prevent an attacker from firing within range of the missile system.
- 13.5 In-flight and crew member security
- ◆ The TSA should fund and monitor mandatory self-defense and security training for flight crews rather than relying on air carriers to train their own flight crews according to varying standards.

- ◆ The TSA should explore the development and installation of special visors on cockpit windows whose light-blocking properties would be activated only when a laser threat is detected—technology already in development by the Department of Defense.
 - ◆ The TSA should mandate that federal air marshals establish a standard procedure for compiling, analyzing, and responding to mission reports of security incidents.
- 13.6 Aviation worker screening
- ◆ The TSA should aggressively pursue development of biometric verification for all aviation workers. The Transportation Workers Identification Card is a good start and should be expanded to include all passenger airports and major air-cargo shipping ports.

14. PREVENTING NUCLEAR TERRORISM

- 14.1 Issue a policy that delegitimizes highly enriched uranium in the civilian sector. Congress should reenact the 1992 Schumer amendment restrictions on exporting highly enriched uranium (HEU).
- 14.2 Expand the Global Threat Reduction Initiative program to include all HEU-powered civilian reactors. Speed up conversion of U.S. research reactors from HEU to non-weapons-usable uranium.
- 14.3 Expand the amount of U.S. highly enriched uranium slated for conversion to non-weapons-usable form. Accelerate the conversion of HEU already scheduled for conversion. The United States could set aside this converted material as a strategic nuclear fuel reserve.
- 14.4 Do not pursue plutonium reprocessing methods that would lead to separated weapons-usable plutonium.
- 14.5 Increase consolidation of weapons-usable materials in the U.S. nuclear complex. Work toward the secretary of energy's advisory board recommendation to move these materials to one highly secure site. Further consolidation could pay off in billions of dollars of cost savings.

- 14.6 The Department of Energy (DOE) and the National Nuclear Security Administration (NNSA) should develop a comprehensive strategic security plan. Such a plan must be based on frequently tested performance and not just on compliance with security requirements. The DOE and the NNSA should coordinate their security efforts with the Department of Defense. Protecting against the most likely route for terrorists or criminals to gain access to weapons-usable materials, the DOE and the NNSA should increase vigilance against the insider threat to nuclear facilities.

15. THE PERILS OF NEGLECTING AMERICA'S WATERFRONT

- 15.1 Over the next eighteen months, the Department of Defense must work closely with the Coast Guard (now part of the Department of Homeland Security) and with local authorities in organizing and participating in exercises that involve simulated attacks on the nation's largest commercial seaports.
- 15.2 The Department of Defense needs to take the lead on funding and setting up joint operations centers in all major U.S. commercial ports: to outfit them with advanced information and communications technology that supports surveillance and data sharing; and to provide the necessary training to the local, state, and federal agency participants. This should be completed by 2007.
- 15.3 The U.S. Navy should reposition one of its two salvage ships in Norfolk, Virginia, to the West Coast and take the lead in drawing up commercial salvage contracts to support domestic harbor clearance. Over the next five years, the Navy should double its salvage fleet from four vessels to eight, and base two of them on the West Coast, two on the Gulf Coast, and two on the East Coast. The remaining two can be deployed overseas to support navy operations.
- 15.4 The National Oceanographic and Atmospheric Administration (NOAA) hydrographic research vessels should receive additional funding to complete bottom surveys of all major U.S. commercial seaports. This baseline information is indispensable in quickly spotting mines, should an adversary deploy them.

- 15.5 The Coast Guard needs to see annual funding doubled to \$2 billion to replace its ancient fleet of vessels and aircraft, and to bring its command and control capabilities into the twenty-first century. Many of its cutters, helicopters, and planes are operating long beyond their anticipated service life and are routinely experiencing major breakdowns. Under the current delivery schedule, it will be thirty years before the Coast Guard has the kind of assets it needs today to perform its mission. This could leave a two-decade gap in capability as the existing fleet becomes too decrepit and dangerous to operate.
- 15.6 Congress should authorize the reallocation of all seaport duties and fees back into the ports to support security upgrades and infrastructure improvements.
- 15.7 The federal government needs to develop a national port plan that takes into account long-term trade and security trends. Relying on a patchwork quilt of locally based decisions for managing this critical infrastructure is just not acceptable.

16. RECREATING OUR BORDERS

- 16.1 Security from the threat of terrorism should be the primary focus of U.S. border efforts. Strong physical barriers on the border with Mexico are essential. Approximately 150,000 “OTMs,” or other-than-Mexican illegal immigrants, crossed this border in 2005, and are able to blend into American society and pose a serious security threat once inside our borders.
- 16.2 Utilizing technology and personnel, the entire U.S. northern and southern border must be continually monitored. Capability must be developed to respond to the detection of illegal crossings.
- 16.3 Eliminate “whack-a-mole” responses, such as the Arizona Border Control Initiative, that simply relocate major crossing points without reducing overall flow. The practice of redeployment to targeted areas should be ended and focus placed instead on augmenting capabilities.
- 16.4 U.S. visa and asylum processes must be made to conform with the Mexican and Canadian systems, so that, except in rare cases, all three countries agree on who is admitted.

- 16.5 Development and deployment of counterfeit-proof visitor identification for guest workers and permanent aliens.
- 16.6 Workplace enforcement of immigration rules must be done on a continual basis. Sponsoring institutions must have personnel certified in understanding the immigration process and documentation.
- 16.7 Detection of radioactive sources must be prioritized and ineffective personal radiation detectors should be replaced by radiation portal monitors and X-ray systems.

17. LAND OF SWEET LIBERTIES

- 17.1 It is vital to spark a structured national discussion now about the tradeoff between security and liberty. The Civil Liberties Protection Board, created by executive order of the president in August of 2004, could lead the effort.
- 17.2 Governors and big-city mayors should consider appointing regional liberty protection boards to work with state and local law enforcement authorities.
- 17.3 Local liberty protection boards should sponsor outreach and educational activities in schools, civic organizations, places of worship, and local media.
- 17.4 The national Civil Liberties Protection Board should issue a yearly report on its activities and on threats to American freedoms, brief Congress on the report (including classified annexes if necessary), and convene an annual national conference to review its report.
- 17.5 The board should file a civil liberties impact statement with the executive branch and Congress on any proposed measure or program that may raise public concern about potential abuses of liberty.

