CONTENTS

Chapter 1—Introduction ......................................................................................................... NS-1
Chapter 2—Federal and State Policy and Duties ................................................................. NS-2
Chapter 3—Intelligence and Surveillance ........................................................................ NS-10
Chapter 4—Public Health ................................................................................................ NS-14
Chapter 5—Infrastructure Protection ............................................................................... NS-17
Chapter 6—Civil Liberties .............................................................................................. NS-22
Conclusion ....................................................................................................................... NS-26
Discussion Questions ....................................................................................................... NS-27
Chapter 1—Introduction

DEFINING SECURITY

What exactly does it mean to be secure? How far do we go as a nation to become more secure? In the five years since 9/11, the answers to these and other related questions are not clear. The United States has made a huge effort and has made much progress toward security. However, budget deficits, controversy over threats, and disagreement about how best to prepare against these threats or attacks leave us in a state of “guarded preparedness.” No one knows if or when we will be attacked again. There are many groups that have vowed to work against the United States through violent or political means. Natural disasters such as earthquakes, hurricanes, and floods pose an entirely different set of challenges.

Several questions arise when defining what it means to be secure. How far do we intrude into an individual’s privacy? How much do we restrict travel and speech? How much do we fortify our buildings, power plants, schools, and military bases? Given the wide range of existing needs, we can reasonably ask how much we can spend to make us as safe as possible. Thus far, our answer to this last question is “more than nothing but less than everything.” Some of these are budget questions involving federal, state, and local taxes. Others are technological issues. We can only go where technology allows us. Some are questions of civil rights that involve no less than a thorough review of the Bill of Rights and the expectations of an American public very much used to nearly total freedom.

Answers to these questions are determined through the political process in the U.S. Congress, by the White House and its team, by state legislatures and governors, by mayors and city councils, and by the public. Each level of government has a different set of responsibilities and duties. State and local responders bear the burden of getting there first with the right personnel and material and staying, for several days if necessary, until the federal teams arrive. As Hurricane Katrina showed, we still have a lot to do. These duties will require no less than a modernization and “professionalization” of many administrative offices, some of which must learn entirely new ways of operating. Private businesses must also play their role in this security effort by adopting government’s standards or by creating their own where the government has none. Finally, citizens must be watchful, be sensible, and be willing to hold the government accountable for maintaining our quality of life and upholding our rights in one of the potentially most intrusive tasks—that of maintaining order and security.
Chapter 2—Federal and State Policy and Duties

Since the Cold War, the United States’ security network has evolved from the civil defense programs of the 1950s and 1960s to today, where a new sprawling cabinet, the Department of Homeland Security, stands atop a large security and response hierarchy. “Homeland Security” incorporates several existing government offices, 180,000 employees, and 22 agencies to build our security capacity. New missions, goals, objectives, plans, laws, and programs help us identify threats, assess risks, and devise new ways to think about what it means to be secure.

Our 14 other cabinet departments also have roles to play in our security mission. Each is charged with assessing risks within its area of expertise and forming a security and a response plan. For example, from Executive Orders written by President John F. Kennedy in 1962, the Department of Commerce will take control of our nation’s federal, state, and local roads and railways in a national emergency if the president so declares. The Department of Agriculture will issue emergency regulations for farms and food production facilities. The Post Office will register men for a military draft.1

After the attacks of September 11, 2001, President Bush issued several directives and executive orders that set in motion one of the largest governmental efforts in the history of any nation. It is these efforts to which we now turn.

At the top of the homeland security hierarchy sits the President and the new Directorate of National Intelligence (DNI). The DNI coordinates intelligence that works its way up the chain of command from agencies below, but the Department of Homeland Security remains in general control of each cabinet department and its security mission, directing them to meet certain goals. Each department receives funding from Congress to develop programs to meet these goals. Looking more closely at the DHS, one finds a large set of administrative offices as shown in Figure 2-1.

HIERARCHY AND MISSION

The offices of the DHS are staffed by those with expertise in various areas such as intergovernmental relations, science and technology, and emergency management. Also under the umbrella of DHS are law enforcement agencies such as the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATFE) and intelligence agencies such as the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the Defense Intelligence Agency (DIA). With the exception of the Department of Defense, the DHS is the nation’s largest administrative structure. President George W. Bush’s administration has developed nine security “strategies” as follows, without rank.
Fig. 2-1 DHS Organizational Chart
Strategies

1. The National Security Strategy of the United States
2. The National Strategy for Homeland Security
3. The National Military Strategy of the United States
4. The National Military Strategic Plan for the War on Terrorism
5. The National Strategy for Combating Terrorism
6. The National Strategy to Secure Cyberspace
7. The National Strategy to Combat Weapons of Mass Destruction
8. The National Money Laundering Strategy

LAWS AND GOALS

The task of securing America is huge and each Strategy directs the appropriate federal agency to take action to promote security in one or more areas, such as transportation or health. The National Strategy for Homeland Security focuses on domestic security and problems that we can address in specific sub-areas. There are six “mission areas” that orient all DHS activities and are included within the Strategies. The six include:

1. Intelligence
2. Border and Transportation Security
3. Domestic Counterterrorism
4. Protecting Infrastructure
5. Defending Against Catastrophic Threats
6. Emergency Preparedness and Response

These mission areas organize the federal, state, and local government’s efforts to mount our defense against threats. To support these strategic missions, planners within all governments, private businesses, nonprofit organizations, and think tanks such as the Rand Corporation or the Council on Foreign Relations (CFR) have partnered to create more focused directives that are outlined in several separate “Homeland Security Presidential Directives” (HSPD). Each is in the implementation stage and is continuously evolving.

HSPD 1 Organize and Operate a Homeland Security Council (HSOC)
HSPD 2 Combating Terrorism through New Immigration Policies
HSPD 3 Develop an Advisory Alert System
HSPD 4 National Strategy Against Weapons of Mass Destruction, Classified
HSPD 5 Management of Domestic Incidents through the National Incident Management System (NIMS) and the National Response Plan (NRP)
HSPD 6 Integration & Use of Screening Information
HSPD 7 Critical Infrastructure Identification, Prioritization, and Protection
HSPD 8 Develop National Preparedness Capabilities
HSPD 9 Defending Agriculture and Food Production
HSPD 10 Biodefense for the 21st Century
HSPD 11 Develop Comprehensive Terrorist-Related Screening Measures
HSPD 12  Develop Policy for Common Identification Standard for Federal Employees
HSPD 13  Develop Improved, Secure, Maritime Procedures
HSPD 14  Develop Domestic Nuclear Detection Policies
HSPD 15  Develop Homeland Security Policy for the War on Terrorism
HSPD 16  Develop Policies for Aviation Security
HSPD 17  Develop Policies against Weapons of Mass Destruction-Classified
HSPD 18  Medical Countermeasures against Weapons of Mass Destruction.

From HSPD 1, a Homeland Security Council is organized and consists of the president, the vice president, secretaries of several cabinet offices, the heads of the FBI and CIA, as well as others that the president shall name. It acts as a major planning body. Information to state and local governments is distributed through the Homeland Security Information Network. Under the authority of the other HSPDs and laws that have been passed, the DHS, other cabinet departments, and states and localities are simultaneously developing new methods, plans, and programs to control the borders, screen cargo and passengers, protect against biological threats, and protect our food supply, just to name a few.

President George W. Bush and Congress have passed many laws to build upon the strategies and fund security programs, research and development, technology, and preparedness activities at the federal, state, and local levels. Perhaps the most well-known law is the PATRIOT Act of 2001 and its reauthorization in 2005. PATRIOT authorized domestic spying of those suspected of aiding and abetting terrorism on authority from a secret court. The Homeland Security Act of 2002 (HSA), created the cabinet-level Department of Homeland Security and redefined terrorism to include many crimes previously prosecuted by states and local governments. HSA established a partnership role between federal law enforcement (FBI) and state and local personnel to improve coordination and information sharing between all three levels of government. The HSA also created the Homeland Security Advanced Research Projects Agency to produce hi-tech solutions to support the security missions and strategies.

In 2004 the Intelligence Reform and Terrorism Prevention Act created new security committees in the House and Senate, reordered intelligence networks with a Director of National Intelligence at the top, authorized more foreign aid to interdict terrorists, and included a number of surveillance and tracking regulations to prevent terrorists from coming into the United States. In 2005, Congress passed the Real ID Act to standardize all 50 states’ driver’s licenses to one common federal standard by May of 2008. The states have yet to implement this law.

Preparedness (HSPD 8) is probably the largest activity that helps organize all the other activities. To this end, the National Response Plan (NRP) has been constructed. The Plan is a “map” of sorts that outlines a sequence of responsibilities for federal, state, and local managers and includes a role for the military to act in support of civilian authority. See Figure 2-2 for an illustration of an NRP flow chart. The NRP is based on a common management framework called the National Incident Management System, or NIMS. NIMS establishes a chain of command and a management hierarchy for how federal, state, and local emergency managers will coordinate their activities during a disaster. All state and local governments must comply with the NIMS framework in order to be eligible for grant funding.
Figure 2-2 NRP Flow Chart

Key:

INS- Incident of National Significance
LEOPS- Local Emergency Operations Plan
EMAG- Emergency Management Assistance Groups
HSOC- Homeland Security Operations Council
NRP- National Response Plan

Arrows indicate policy making authority
GOALS

HSPD 8 directs DHS to promote and improve federal agency and state and local emergency capacity to become full partners under the National Response Plan and the National Incident Management System. As part of the effort, planners have created 15 hypothetical disaster scenarios to enable agencies and states and local governments to prepare for the worst things that could possibly happen.

Disaster Scenarios

1. Improvised Nuclear Device
2. Aerosolized Anthrax
3. Pandemic Influenza
4. Plague
5. Blister Agents
6. Toxic Industrial Chemicals
7. Nerve Agents
8. Chlorine Tank Explosion
9. Major Earthquake
10. Major Hurricane
11. Radiological Dispersal Device
12. Improvised Explosive Device
13. Food Contamination
14. Foreign Animal Disease
15. Cyber Attack

Federal, state, and local officials have carried out three major drills. These “TOPOFF” (short for “Top Officials”) drills were carried out in Denver and Washington D.C. (2000), Chicago and Seattle (2003), and in New Jersey and Connecticut hospitals (2005) to test emergency operations. Many improvements in medical and emergency capacity need to be made and are discussed in Chapter 4.

Security officials have also created a broad set of “Target Capabilities” and a refined, narrower list of “Universal Tasks (UTL).” Thirty-six capabilities are defined around each of four mission areas of the UTL—prevention, protection, response, and recovery. Prevention includes tasks like managing data, analyzing intelligence, and monitoring areas for biological agents. Protection incorporates activities such as identifying assets, safeguarding public health, and preparing the public. Under response fall efforts like managing an incident, implementing protective actions, and caring for the public. When engaged in recovery, government managers might provide long-term health care, social services, or even reconstitute the government itself. The Department of Homeland Security does not expect every emergency management team to be instantly able to perform all of the 36 capabilities immediately, but rather to build their capacity through grants, education, training, drills, and by sharing their best practices with other similar jurisdictions in a “Lessons Learned” online network operated by the Office of Domestic Preparedness.

36 Target Capabilities for Federal, State, or Local Responders

1. Planning
2. Interoperable Communications
3. Information and Threat Recognition
4. Intelligence Fusion and Analysis
5. Information Sharing and Collaboration
6. Terrorism Investigation
7. CBRNE* Detection
8. Risk Analysis
9. Critical Infrastructure Protection
10. Food/Ag Safety and Defense
11. Public Health Investigation
12. Citizen Preparedness and Participation
13. On-Site Incident Management
14. Emergency Operations Center
15. Critical Resource Management
16. Volunteer Management and Donations
17. Worker Health and Safety
18. Public Safety and Response
19. Animal Health Support
20. Environmental Health
21. Explosive Device Operations
22. Firefighting Operations
Most of these activities will be carried out by state or local responders during the first hours or days of an incident of national significance.\textsuperscript{15}

In 2006 a DHS team reviewed state and local abilities. While many states and local governments have come a long way since 9/11, the Nationwide Plan Review reveals many concerns about their preparedness. State and local governments have not developed their plans in accordance with either the National Response Plan or the National Incident Management System. Communication links that were so crucial during 9/11 still do not exist between all players within a jurisdiction, and a command system has not been clearly identified. Full evacuation plans for all population groups are nonexistent, there is insufficient mass care ability, and progress on the Universal Tasks and Target Capabilities is too slow.\textsuperscript{16} Clearly, we have more to do.

**GRANTS**

Through the Office of Domestic Preparedness (ODP), the DHS awards grants to state and local governments for anti-terrorism efforts and for some equipment. Though states and cities claim the funding is too slow, too little, and directed more toward terrorism and less toward prevention and recovery, over $100 billion has been awarded from 2003 to 2006.\textsuperscript{17} The “risk of terrorism” has usually been the priority when granting funds, but apparently, funding has been awarded on the basis of political considerations. In some cases more money has been given to places with comparatively little risk, like Wyoming, than to cities like Los Angeles, with huge risks. Much of the money has also gone for the Urban Areas Security Initiative (UASI) for the nations’ largest 125 cities.\textsuperscript{18} Some smaller cities still have not received any federal funding.

**ACCOUNTABILITY AND PERFORMANCE**

The Department of Homeland Security has set forth performance measurement standards by which their work can be assessed. Much the same as any large bureaucracy, DHS has developed its own goals of awareness, prevention, protection, response, recovery, service, and organizational excellence. All programs that DHS carries out or directs are included within these seven goals. In the Performance Report for 2006, DHS claims to have met 68 percent of its target objectives within each goal. DHS has also created its own rating system of its performance and rates three programs as “effective,” six as “moderately effective,” five as “adequate,” and five as “not demonstrating results.” However, deep within the report under each “goal” is language indicating data on performance was estimated or not available but forthcoming. This lack of hard data on whether targets were met questions the DHS 68 percent effectiveness rating.\textsuperscript{19} The Government Accountability Office (GAO) is a nonpartisan, administrative office within the executive branch of the U.S. government that issues performance reports for almost every government program. GAO reviewed the DHS National Performance Goals and found that the DHS needed a clearer, risk-based strategic plan so as to allow better use of money and personnel resources, better coordination of state and local responders, and improved training and data standards.\textsuperscript{20}
The language describing the nation’s Homeland Security Strategy fills thousands of pages not including the reviews by congressional committees, study groups like the 9-11 Commission, or reports by nonprofit corporations, the media, and think tanks. To fully understand the entire security effort would take years of study; but this short review should provide a clear vision of the enormity of the task to which we have set ourselves and great insight on the human condition, as it has evolved.

NOTES

3. The Rand Corporation and Council on Foreign Relations are conservative “think tanks.” Documents can be found at http://www.rand.org and http://www.cfr.org, respectively.
6. The Homeland Security Act of 2002 can also be found at the Library of Congress’s site, although numerous commentaries can be found through common search engines. It is Public Law 107-56.
7. The Intelligence Reform and Terrorism Prevention Act attempted to support many of the recommendations put forth by the 9-11 Commission. PL 108-458.
8. The Real ID Act has generated much controversy among the states and civil liberties groups. It is PL 109-13.
10. The documents supporting the National Incident Management System can be found at http://www.dhs.gov/xpreppresp/programs/gc_1166653070655.shtm
11. Grant information for states and local governments is located in several places, but one good location is http://www.dhs.gov/xgovt/grants
12. Disaster Planning Scenarios can be found at http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm
13. Data from the TOPOFF drill is not generally available to the public. An overview of events and a summary of findings may be found at http://www.dhs.gov/xnews/releases/press_release_0635.shtm
14. Target Capabilities and supporting documents for the Universal Task List (UTL) may be found at http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm
15. The Universal Task List is a large document, as are most DHS documents. It can be found at http://www.ojp.usdoj.gov/odp/assessments/hspd8.htm
16. The Department of Homeland Security Nationwide Plan Review was completed in 2006. States and local governments are continuously improving their plans and capacities. The Review is located at http://www.dhs.gov/xpreppresp/programs
18. Grant information for states and communities is located in the Office of Domestic Support at http://www.dhs.gov/xpreppresp/programs. Additional information on exact dollar amounts can be found at http://www.dhs.gov/xlibrary/assets/grants_st-local_fy06.pdf
Chapter 3—Intelligence and Surveillance

Central to any security effort are intelligence and surveillance. Sixteen federal cabinet departments and agencies in partnership collect intelligence from every conceivable source. The Departments of State, Justice, Treasury, Energy, and Homeland Security, along with the CIA, FBI, the National Security Agency (NSA), and the Drug Enforcement Agency (DEA), as well as all branches of the military, are partners in surveillance. The National Geospatial Intelligence Agency (NGIA) produces maps of the earth used by other agencies, and the National Reconnaissance Office (NRO) operates the satellite system through which the collection of intelligence is made. Each year about 3 billion conversations are intercepted, but only one in a thousand is actually interpreted by human beings. Agency websites are listed in the notes at the end of the chapter.

LEGAL BASIS FOR SURVEILLANCE

Several laws authorize government collection of intelligence. In 1968 the Crime Control and Safe Streets Act allowed the government to wiretap conversations to collect evidence of a crime. Then, in 1978, as technology developed, Congress passed one of the most sweeping intelligence laws ever passed by any country—the Foreign Intelligence Surveillance Act (FISA). This law also created a secret FISA court that approves collection of information without requiring the normal Fourth Amendment protection of “probable cause” unless the target is a U.S. citizen. In 1986, as technology matured, Congress aided law enforcement by passing the Communications Assistance for Enforcement Act (CALEA) that required manufacturers of electronic devices (cell phones, etc.) to incorporate software that would enable law enforcement officials to remotely access conversations—even when a phone is off. After 9/11, Congress passed the PATRIOT Act, which broadened the FISA and the government’s power of surveillance of almost all forms of electronic communication—including Internet usage. The PATRIOT Act allows the government to collect some domestic law enforcement information under the guise of “foreign intelligence.” Many citizens feel the government wields too much power, citing domestic spying abuses of the 1970s when the FBI and CIA illegally spied on Vietnam War protestors.

In 2002 Congress passed the Homeland Security Act (HSA) to promote federal, state, and local law enforcement partnerships and information sharing. In 2001 the FBI set up “Joint Terrorism Task Forces” (JTTF) in cities nationwide to be alert on the “front lines” and respond immediately to various perceived threats. Numerous threats have been intercepted, and those responsible have been prosecuted. Thirty-seven states, in order to blend information from federal, state, and local government, have created their own version of these task forces called “fusion centers.”

FEDERALLY FUNDED RESEARCH AND DEVELOPMENT CENTERS (FFRDCS)

The federal government funds a wide variety of state-of-the-art “centers” to devise new and improved ways to gather information and develop tools for anti-terrorism protection. The Homeland Security Advanced Research Projects Agency (HARPA) and the Biomedical Advanced Research Projects Agency (BARDA) are two newly created, high-tech, secret FFRDCs. The work of both centers is classified and not subject to the Freedom of Information Act. Other centers are more open about their work. Los Alamos National Laboratory in New Mexico and Sandia National Laboratory in California maintain partnerships with the nation’s research universities to create new intelligence products. Hand-held biological air sensors and new mobile command intelligence technology for military use are two
examples of new products from these centers. Information about events and research done at Los Alamos or Sandia can be found in newspapers and on the Internet (see the websites in the chapter notes).  

IDENTITY AND TERRITORIAL INTEGRITY

A large part of security lies in controlling access to one’s country. Identity is at the heart of that access. Being sure of someone’s identity is perhaps the best way to promote security. Thus, accurate identity is necessary for territorial integrity at the borders and at air and seaports. Legitimizing identity is the subject of the Real ID Act of 2005. The Act mandates that states reissue all 260 million driver’s licenses according to federal standards in order to be certain of each driver’s identity. Drivers may be required to obtain official birth and marriage documents before a state will reissue their driver’s license. In the future, the new ID card will have a biometric identifier such as a fingerprint, digital photograph, or microchip containing personal information. State and civil liberties groups are resisting implementation of the Act, citing violation of privacy and unwarranted costs as reasons.

TRAVEL AND TRADE

Identity is at the heart of the new travel restrictions. As of January 2007, American citizens traveling to and from Mexico and Canada must have passports with biometric measurements, also known as e-passports. Those traveling to America from 27 (mostly westernized, European) countries will not need a visa but can travel on an electronic passport under the Visa Waiver program. Visa Waiver places personal information on a microchip in an individual’s passport. The chips can then be scanned using “radio-frequency identification,” or “RFID,” technology by Customs and Border Patrol (CBP) officers. Those countries having Visa Waiver programs in effect are shown in Figure 3.1. Those entering the United States from countries outside the Visa Waiver program fall under the jurisdiction of the U.S. Visit program and must have a regular visa and will be prescreened against a database of known or suspected terrorists prior to the individual’s arrival.

Table 3.1 Visa Waiver Program Nations

<table>
<thead>
<tr>
<th>Andorra</th>
<th>Iceland</th>
<th>Norway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>Ireland</td>
<td>Portugal</td>
</tr>
<tr>
<td>Austria</td>
<td>Italy</td>
<td>San Marino</td>
</tr>
<tr>
<td>Belgium</td>
<td>Japan</td>
<td>Singapore</td>
</tr>
<tr>
<td>Brunei</td>
<td>Liechtenstein</td>
<td>Slovenia</td>
</tr>
<tr>
<td>Denmark</td>
<td>Luxembourg</td>
<td>Spain</td>
</tr>
<tr>
<td>Finland</td>
<td>Monaco</td>
<td>Sweden</td>
</tr>
<tr>
<td>France</td>
<td>Netherlands</td>
<td>Switzerland</td>
</tr>
<tr>
<td>Germany</td>
<td>New Zealand</td>
<td>United Kingdom</td>
</tr>
</tbody>
</table>


The Customs and Border Patrol agency (CBP) has 11,000 officers at 170 land checkpoints on our borders. The Secure Border Initiative will provide 6,000 more CBP officers by the end of 2008 as well as more detection systems, helicopters, detention beds, and related equipment. Although many immigrants come to the United States through legal channels, millions more cross our borders illegally. It is likely that terrorists have entered both legally and illegally. Many Congressional members from both major parties and the George W. Bush Administration feel the best way to settle the immigration issue is to pass
“guest worker” or amnesty programs for immigrants that would allow those currently inside the United States illegally to stay without penalty or threat of removal.\(^\text{16}\)

All airline passengers are screened through a program called “Secure Flight” in which names are compared to names on the terrorist watch list. As of 2007, the program is operating only partially until management, technology, and privacy concerns are resolved.\(^\text{17}\) Almost 100 percent of carry-on and checked baggage are screened for weapons or explosives but currently, there is no foolproof way to tell whether someone has smuggled a biological agent on board. Knives, scissors, and nail files are captured every day. The Transportation Security Administration (TSA) reports that a “sizable portion” of air cargo is screened but not all.\(^\text{18}\) FFRDCs are working to develop more efficient and accurate detection systems.

We have also improved our seaport security. The Maritime Transportation Security Act of 2002 (MTSA) covers all vessels from 50 participating nations. Every port facility and shipper must have a security and an emergency plan, and all vessels must electronically submit a cargo and passenger manifest describing their goods and personnel prior to entering the port.\(^\text{19}\) The Container Security Initiative (CSI) covers, in theory, all foreign ports, but presently, ports in only 50 foreign nations are participating. The Department of Homeland Security is responsible for establishing partnerships with foreign nations’ port authorities, but host countries are responsible for the actual screening.\(^\text{20}\)

Within our territorial waters, the U.S. Coast Guard is responsible for port security, but most ports are operated either by a state or local government—or by a foreign-owned company. A disaster at one of our 360 ports could have huge economic ramifications for the entire country. Additionally, the “Known Shipper” program allows a company to legitimate itself through a series of certifications and the review of documentation.\(^\text{21}\) However, this raises the question of how we can protect ourselves against various kinds of fraud.

Some are concerned that we are becoming a surveillance society and that intelligence collection is so widespread, leaving very little that remains private. Through satellite and communications technology, governments are able to listen to, see, and/or record almost everything that we say, do, where we go, and what we view on the Internet or buy on a credit card. Most cities use intersection cameras to issue traffic citations or to locate crime. Perhaps, soon, our personal data will be “scannable” on our driver’s licenses. One may wonder what remains of our private lives. The balance between security and privacy will be explored in Chapter 6, Civil Liberties.

NOTES

8. Homeland Security Advanced Research Projects Agency & Biological Advanced Research Projects Agency do not publicize their work but some information about them can be found at \textcolor{red}{http://www.dhs.gov/xnews/releases/press_release_0268.shtm}
9. Los Alamos National Laboratory and Sandia National Laboratories publish public journals and bulletins. Not all of their work is publicly available, but some information can be found at \textcolor{red}{http://www.lanl.gov} and \textcolor{red}{http://www.sandia.gov}

**OTHER WEBSITES**


The National Geospatial Agency [http://www.nga.mil](http://www.nga.mil)

The National Reconnaissance Office [http://www.nro.mil](http://www.nro.mil)

Chapter 4—Public Health

A biological or chemical attack is one of the most feared events. Anthrax, smallpox, plague, and bird flu are potential weapons of mass destruction. Chemicals such as VX or sarin nerve gas are lethal and easy to disperse. Harder to acquire and use but equally as deadly are radiological materials for use in a dirty bomb. How ready is our nation’s public health network to protect against and respond to these threats? What successes have we achieved in promoting state, local, and private provider readiness?

TOPOFF DRILLS

The year is 2005. Doctors and nurses and other hospital staff scurry through the halls of hospitals in New Jersey and Connecticut trying to cope with a chemical weapons attack. Short of isolation rooms, ventilators, and beds, the staff does the best that it can to treat hundreds, even thousands, of casualties—victims of poison gas. When computers freeze or hospital phone lines are jammed, staff members resort to their personal cell phones in the mad dash to diagnose and treat patients and keep good records essential for administration and insurance. What happened? Relax, for now. It was only a drill—one of many in a series of public health emergency exercises called “TOPOFF,” short for top officials exercise in which federal, state, local and private officials coordinate their common response. Since 2000, these TOPOFF emergency drills in cities around the country have taught us that we need to do more to prepare for any emergency involving public health. Quarantine wards, better communications systems, bed space, antiviral drugs, and knowledge of the emergency plan all need improvement.

All states have a public health laboratory that carries out disease research and educational programs. Many of these programs are performed at county health facilities. Actually, despite the cuts in the state public health network over the period 1960-2001, we have made notable achievements in modernizing our public health infrastructure. From 1960 to 2001, public health was a forgotten effort subject to numerous state budget cuts. Perhaps as a result of September 11 and the anthrax attack, or perhaps a result of a renewed concern about flu and other outbreaks, we have modernized our detection, prevention, and response capacity—to some extent. Homeland Security Presidential Directive 10, “Biodefense for the 21st Century,” establishes the framework for laws and programs.

MODERN PUBLIC HEALTH NETWORKS

The Public Health Security and Bioterrorism Response Act of 2002 provided $1.6 billion for state and health provider networks to implement disaster response plans and conduct drills. The Bioterror Hospital Preparedness program, funded at $491 million, will help purchase isolation equipment, drugs, and supplies. Besides participating in the TOPOFF drills, all states have bioterror and pandemic flu plans and are engaging in role plays in mock attacks with the state health labs and private hospitals and doctors. Entire sections of each state’s emergency plan are devoted to a public health crisis, and at least 81 percent of states and/or counties have strengthened their relationships between local doctors and hospitals, emergency medical technicians, emergency management, and public safety.

The CDC, or Centers for Disease Control, is on the front lines of any public health threat, whether man-made or natural, and this federal agency is responsible for some pretty amazing successes. Since 2001, over 8,800 lab technicians have been trained in recognizing and dealing with a bioterror attack. The new Laboratory Response Network connects 142 member laboratories in all 50 states, more funds have been given to local health departments, and a new Public Health Information Network can reach one million people in the health system in a matter of minutes. Project BioSense advances our capacity to detect an attack by gathering real-time epidemiological data from hospitals and sending it throughout the
network. If something occurred in a college town where 100 students contracted a strange disease, all participants in the network would know about it the same day. Project BioWatch further supports detection and prevention efforts by placing airborne detection sensors, like the one described above and developed by Los Alamos, in all major cities.

In the event of a public health disaster, several types of responses may occur. “Push Packages,” 12-ton units of drugs and supplies from the Strategic National Stockpile, can be sent within a few hours notice anywhere in the continental United States. Either CDC National Disaster Medical Assistance Teams or pre-selected hospitals and doctors would distribute the drugs, perhaps with the help of the National Guard. The CDC in Atlanta cooperates with the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) in Fort Detrick, Maryland, to diagnose the agent that caused the illness and prescribe the correct course of treatment as they did during the anthrax attack in 2001. USAMRIID and CDC are home to the world’s deadliest bacteria and viruses, used for research and safely stored well below ground.

Yet, with thousands of viruses on the planet, can we cope with something new? Not well, say our TOPOFF drills. We must improve. Encouragingly, Project Bioshield has committed to providing $5.6 billion over the next ten years for new antibiotics, antivirals (where we are particularly weak), and vaccines. Over 50 initiatives are in progress, overseen by the National Institute of Health (NIH).

“DIRTY BOMBS”—RADIOLOGICAL ATTACK

But there are other concerns. In 2006, Customs and Border Patrol (CBP) officials disguised as businessmen smuggled enough radioactive material to make a dirty bomb across the U.S.-Mexican border, without detection by CBP personnel. Apparently, the detection system was not sophisticated enough to detect the lower levels of radiation in a radiological device or the quantity of material was just under the limit set by CPB to require detention of the two businessmen. Radiological material has military and nonmilitary uses in hospitals for diagnostics, university labs for experiments, and industry for weapons and various metals processes. Though tight security is required and the Department of Energy tracks some small purchases of radioactive substances, it is possible that enough material could be stolen from several sources, combined, and used to build a dirty bomb. Silent and unobtrusive, a dirty bomb left in an airport might not be discovered for days until radiation sickness was diagnosed. Fortunately, the Army has mobile medical and hazmat teams ready to deploy to the scene in a few hours. The cost in lives, illness, and economic loss would be great indeed.

QUARANTINE

Should there be a health emergency necessitating quarantine, the governors of each state have a new tool to protect the public. The Model States Emergency Heath Powers Act of 2002 allows the governor to use the National Guard (the governor is in control of the guard anyway) to either detain people in their homes or forcibly remove them to a relocation center to stop the spread of a contagious disease that threatens to overwhelm the government and society. If, for example, bird flu turned into a pandemic, governors would have a tough decision to make regarding who to “relocate.” As we saw during Hurricane Katrina, people do not always like to follow orders and may resist—sometimes violently. Careful, calm planning and execution must accompany the implementation of this Act.

Though we have made much progress, nature is as determined a foe as any terrorist group. One needs only to consider how many people are sickened every year by common bacterial and viral infections. Despite the existence of our large drug companies and all of our protective measures, we have not conquered bacteria or viruses. Nor, apparently, do we understand it well. Should a biochemical or radiological attack occur, we will know whether our renewed public health efforts measure up. Let us hope we never have to find out.
NOTES:

   [http://www.hhs.gov/faq/disaster/projectbioshield]
10. The CDC and USAMRIID function independently. The CDC lies within the jurisdiction of the Health and Human Services Department, while AMRIID is an agency within the Department of Defense. More information can be found at [http://www.cdc.gov] and [http://www.usamriid.army.mil], respectively.
Chapter 5—Infrastructure Protection

In 1941 FBI Director J. Edgar Hoover noted the critical importance of our infrastructure.¹ Pearl Harbor was destroyed in December of that year, and the bombings in Europe brought home the necessity to protect our bridges, dams, and factories. The Department of the Interior and the Army Corps of Engineers began risk assessment programs for our public infrastructure and defense facilities. In the 1970s, after the creation of the Environmental Protection Agency (EPA) and the Federal Emergency Management Agency (FEMA), programs and funding for infrastructure grew and spread to more infrastructure assets.

Although we may have thought about infrastructure protection and made improvements after the war, modern efforts began in the Clinton administration. President Clinton issued Presidential Directive 63 and created the Critical Infrastructure Assurance Office (CIAO) to collect risk and threat information about the eight types of infrastructure assets then identified.² Few concrete security measures were made, but the Agency began what has turned out to be a gargantuan task.

SEPTEMBER 11 CHANGED EVERYTHING

When 9/11 occurred, no sector of infrastructure had anything like an anti-terrorism plan, only plans to cope with natural disasters and ensure business continuity. Section 1016 (e) of the PATRIOT Act defined critical infrastructure as “systems and assets, whether physical or virtual, so vital to the nation that the incapacity or destruction of such systems would have debilitating impact on security, national economic security, or national public health and safety.”³ The Bush administration passed the Homeland Security Act of 2002 (HSA), produced the National Strategy to Protect Infrastructure and Key Assets, and issued several directives, among them HSPD 7 regarding infrastructure security. Title II of the HSA is the Critical Infrastructure Information Act of 2002 that mandates new protection programs to collect information, plan, and provide assistance to state and local governments for infrastructure security. To prevent unauthorized disclosure, Subtitle B of Title II made this effort exempt from the Freedom of Information Act (FOIA) so that infrastructure protection remains, generally, a classified government effort.⁴

No plan would be complete without connections to intelligence agencies to facilitate information sharing regarding ongoing threats to infrastructure. Several “Infrastructure Information Sharing and Analysis Centers” (ISAC) have been developed for many of the “sectors.” They provide real-time threat information and guidance to private stakeholders. All of these above efforts have resulted in the National Infrastructure Protection Plan (NIPP).⁵ From the Plan, Table 5-1, 17 “sectors” of infrastructure and key assets are identified within the oversight of federal agencies.
### Table 5-1 Infrastructure Sector Responsibility

<table>
<thead>
<tr>
<th>Responsible Agency</th>
<th>Sector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Departments of Agriculture 1</td>
<td>Food—Meat, Eggs and Poultry, All other Foods</td>
</tr>
<tr>
<td>&quot; Health and Human Services 2</td>
<td></td>
</tr>
<tr>
<td>Department of Defense 3</td>
<td>Defense Industrial Base</td>
</tr>
<tr>
<td>Department of Energy</td>
<td>Energy 4</td>
</tr>
<tr>
<td>Department of Health and Human Services</td>
<td>Public Health and Healthcare</td>
</tr>
<tr>
<td>Department of the Interior</td>
<td>Monuments and Icons</td>
</tr>
<tr>
<td>Department of the Treasury</td>
<td>Banking and Finance</td>
</tr>
<tr>
<td>Environmental Protection Agency</td>
<td>Water and Treatment Systems</td>
</tr>
<tr>
<td>Department of Homeland Security</td>
<td></td>
</tr>
<tr>
<td>Office of Infrastructure Protection</td>
<td>Chemical, Commercial Facilities, Dams, Emergency Services, Commercial Nuclear Reactors</td>
</tr>
<tr>
<td>Office of Cyber Security and Telecommunications</td>
<td>Information Technology, Telecommunications</td>
</tr>
<tr>
<td>Transportation Security Administration</td>
<td>Transportation Systems</td>
</tr>
<tr>
<td>U.S. Coast Guard 5</td>
<td></td>
</tr>
<tr>
<td>Transportation Security Administration 6</td>
<td>Postal and Shipping</td>
</tr>
<tr>
<td>Immigration and Customs Enforcement Federal Protective Service (FEMA)</td>
<td>Government Facilities</td>
</tr>
</tbody>
</table>

1. The Department of Agriculture is responsible for agriculture and food (meat, eggs, and poultry).
2. The Department of Health and Human Services (HSS) is responsible for food other than meat, eggs, and poultry.
3. Nothing in the plan impairs or otherwise affects the authority of the Department of Defense, including the chain of command.
4. The Energy Sector includes production, refining and storage, and distribution of oil, gas, and electric power, except for commercial nuclear facilities.
5. The U.S. Coast Guard is the Agency for maritime transportation trade.
6. As stated in HSPD 7, the Department of Transportation and the Department of Homeland Security will collaborate on all matters relating to security and transportation infrastructure protection.


Protection of infrastructure is no simple task because 80 percent of the nation’s infrastructure is privately owned. Except for roads, bridges, and dams, most of America’s energy, financial, industrial, and shipping facilities are private corporations. The federal government may mandate security measures for states and cities, but it has not mandated security plans for private corporations. Even most of our 104 nuclear power plants are privately owned but regulated by the Department of Energy and the Nuclear Regulatory Commission. Consequently, both the Clinton and George W. Bush administrations have focused on the creation of public-private partnerships, advocacy groups, and grants to provide incentives for corporations to secure our infrastructure assets.

Before 9/11, most industries had safety plans. As part of the NIPP, the Department of Homeland Security established the Critical Infrastructure Partnership Advisory Council (CIPAC) to coordinate the
governmental-private effort. CIPAC includes “sector-specific” councils and government coordinating councils as shown in Table 5-1. The former is composed of industry representatives and professional organizations, the latter of the responsible federal agency overseeing the plan effort. For example, the American Waterworks Association (AWWA), representing water systems, and the American Chemistry Council (ACC), representing the chemical industry, met with their federal coordinating councils throughout 2006 and into 2007 to adopt new or modify existing plans to make their facilities secure.

All sector-specific councils have produced some guidelines for infrastructure security within their area and suggest that all facilities work toward adoption of these guidelines. CIPAC government councils will critique the sector plans during 2007 in a process of continuous improvement. CIPAC may receive advice from or share information with a larger council—the National Infrastructure Advisory Council (NIAC), which communicates directly with the President.

**VOLUNTARY GUIDELINES**

Note two interesting things here. One, for most infrastructure sectors, there is no complete, well-defined, tested security plan based on the all hazards approach mandated by the National Incident Management System (NIMS). Most of the plans are designed to ensure business continuity. Sector councils, such as transportation, airports, and seaports are developing their plans as they receive input from stakeholders, but it is a slow process.

Two, any guidelines that emerge from sector-specific councils or CIPAC government councils are voluntary. Neither Congress nor Homeland Security have passed mandatory laws or rules for infrastructure security although the councils and the Governmental Accountability Office (GAO) feel legislation is necessary.

A fair question is why infrastructure security plans are incomplete. Does the effort require government assistance? Since 2001, $1.1 billion tax dollars have been provided for infrastructure security. Where has the money gone? Table 5-2 shows additional 2007 funding for 6 sectors.

<table>
<thead>
<tr>
<th>Sector</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Security</td>
<td>$201.2 million</td>
</tr>
<tr>
<td>Transit Security</td>
<td>$171.8 million</td>
</tr>
<tr>
<td>Buffer Zone Protection</td>
<td>$48.5 million</td>
</tr>
<tr>
<td>Intercity Bus Security</td>
<td>$11.6 million</td>
</tr>
<tr>
<td>Trucking Security</td>
<td>$11.6 million</td>
</tr>
<tr>
<td>Rail Security</td>
<td>$110.0 million</td>
</tr>
</tbody>
</table>

1. A “Buffer Zone” is an area around a location where an event has occurred. Those within the zone may either be considered safe or require evacuation. Source: Department of Homeland Security, 2007. “DHS Announces $445 Million to Secure Critical Infrastructure.”

http://www.dhs.gov/xnews/releases/pr_1168366069190.shtm

All presidential administrations realize mandates are politically unpopular and costly. Both Presidents Clinton and Bush have instead relied on a variety of very specific programs, like grants, and the sector councils to jumpstart the security process. Other efforts include the Offices of Cyber Security and Communications (CS&T) and the Critical Infrastructure Assurance Office that connect appropriate government personnel with private industry requesting help. Several other offices within DHS and the FBI are devoted entirely to security of the nation’s computer network, which, if severely attacked, could jeopardize the operation of our interconnected power grid.
**REMAINING QUESTIONS**

Corporate CEOs are answerable to government and society in general for safety but, more importantly, to their shareholders for making a profit. Security programs are expenses that cut into the bottom line with no return. Corporations also lack longstanding trusted relations with the government and fear release of their information to competitors. Corporations donate millions to Congressional campaigns to buy access and private industry perspective to Congress. Perhaps it is no accident that tighter security laws and rules have not been mandated. Corporations are also unsure their facilities may really be terrorist targets, so that the equation of security and safety has no known solution.13

No one doubts that our infrastructure needs to be safe. Numerous reports show that our bridges, dams, sewers, and transportation facilities are old and in need of repair. Nuclear plants need to be decommissioned. What happens if sewer systems fail? We hardly think of the banking system until the ATM is down or out of money, but a cyber attack on the nation’s financial network could devastate the economy. Most of us have telecommunications options if the land line phone fails. All of our utilities, telecommunications, and industries run on computer systems, and that is precisely why several cyber security offices exist in nearly every cabinet-level department today. If these few examples have not convinced you that infrastructure is important, remember the northeast power blackout of 2003 where 50 million people, businesses, and governments lost power because of the integrated, antiquated patchwork of electric generation systems that make up our “power grid.”15

All in all, our infrastructure network has grown remarkably in the last few decades. Perhaps even more remarkable is the fact that we have not had many major accidents with loss of life. The Government Accountability Office identified 50 different agencies that play some part in securing our infrastructure. Does it take 50 agencies to do what those who own and operate our utilities, banks, computer systems, and other threads in the fabric of our lives have not done on their own?

**NOTES**

Chapter 6—Civil Liberties

A marriage between cold war spying programs, modern terrorism, and satellite and computer technology has brought society to the point where everything communicated and most of our actions can be tracked, collected, and used for some security-related purpose. The fact that we are able to do these things makes it more likely that we will do them. Indeed, did we think technology would always entertain but never interfere, never threaten? Is the expansion of government power to gather information, detain persons without charge, enforce quarantines, and otherwise impinge upon rights justified to promote security? While no definitive answer can be made here, there are several issues to bear in mind.

Civil rights were never intended to be absolute. The Framers of the Constitution knew that living in a complex society would require restrictions on some liberties so that we would also have security and order. They also provided legislative and judicial ways to make adjustments when the times demand such response. Gradually, over our 200-plus-year history, some new rights have been “granted,” found in judicially constructed language of high-profile cases. The right to privacy is one such right, nowhere stated explicitly in the Constitution but judicially inferred from other rights and a right expected by a majority of the human race.1 Just as some rights have been “found,” might not others be altered?

The argument is not made here that the recent measures taken in the name of security are just, but rather that basic rights must not be eliminated. The question becomes, then, which rights need to be restricted, and how much security results from that restriction? Is it worth the sacrifice? Table 6-1 outlines Constitutional rights and the law or program that affects those rights.

Table 6-1 Potential Rights Affected by Security Procedures.

<table>
<thead>
<tr>
<th>Amendment No.</th>
<th>Right or Liberty</th>
<th>Law/Program of Concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st</td>
<td>Religious Freedom, Freedom of Speech, Press, Assembly</td>
<td>PATRIOT/FISA Act—new definition of terrorism (Sec 802, PATRIOT)</td>
</tr>
<tr>
<td>2nd</td>
<td>Right to Bear Arms</td>
<td>Numerous state and city gun restrictions; Brady Bill.</td>
</tr>
<tr>
<td>4th</td>
<td>Right to be Free from Warrantless Searches, to Keep Ourselves and Belongings Private</td>
<td>PATRIOT/ FISA</td>
</tr>
<tr>
<td>5th</td>
<td>Right to “Due Process,” (the right to have a government treat you fairly in investigations and prosecutions)</td>
<td>Military Detention programs Model State Emergency Health Powers Act (quarantine) PATRIOT/FISA Military Commissions Act</td>
</tr>
<tr>
<td>6th</td>
<td>Right to Speedy and Public Trial by Impartial Jury of the State, to Be Confronted with Witnesses Against You, to Be Informed of the Charges Against You</td>
<td>Military Detention programs outside U.S. Military Commissions Act</td>
</tr>
<tr>
<td>8th</td>
<td>No Cruel and Unusual Punishments</td>
<td>Prolonged Detention</td>
</tr>
<tr>
<td></td>
<td>Main Body of Constitution</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Article 1, Section 9</td>
<td>“The Privilege of the Writ of Habeas Corpus Shall not Be Suspended, Unless, When in Cases of Rebellion or Invasion the Public Safety Shall Require it.”</td>
</tr>
</tbody>
</table>
Since FISA was passed in 1978, less than one percent of FISA eavesdropping requests have been rejected; and, in 2004 and 2005, none was rejected.\(^2\) Those records are sealed. The PATRIOT Act expanded government’s warrantless surveillance ability to include U.S. citizens. The National Security Agency (NSA) and FBI routinely search electronic forms of communication without warrant or probable cause and those investigated do not have to be notified.\(^3\) In 2006 we learned that the Justice Department sent approximately 500 “National Security Letters” to businesses and organizations asking for information about individuals.\(^4\) What is being done with this information? The federal government and local police departments have kept files on thousands of innocent Americans. Virtually all of them led to dead ends.\(^5\) European countries are enacting similar phone tracking and Internet surfing programs.\(^6\) Are these programs necessary for security? Could governments maintain security under existing probable cause standards and warrant requirements?

CAMERA PROGRAMS

Surveillance cameras are now in use in every major city in America. New York, Chicago, and Los Angeles all boast thousands of cameras throughout their cities to reduce crime and prevent terrorism. Britain plans to monitor every car on every major road.\(^7\) Cameras catch everything from the largest criminal act to the most mundane. Frustrating motorists, forty-five states now prosecute traffic violations through surveillance cameras.\(^8\) While cameras can catch crime in the act, the manner of implementation must have clear purpose and be responsibly done. The loss of privacy contributes to a decline in the quality of life.

GUN RESTRICTIONS

Aside from the federal Brady Bill that requires a five-day waiting period for states without the instant background check, 16 states have passed legislation to require permits to own or carry any gun.\(^9\) Handguns are illegal entirely in some cities. In a landmark 1982 decision in *Quilici v. Morton Grove, Illinois*, Mr. Quilici was charged with a violation of a statute that forbade owning a handgun inside the city limits. Arriving at the U.S. Supreme Court, the Court ruled in favor of the city’s ban, saying that the 2\(^{nd}\) Amendment did not mean that average, law-abiding citizens should “keep and bear arms,” but, rather, the “militia,” or, in this case, the National Guard.\(^10\) Hearing of the decision, the City of Kennesaw, Georgia, passed an opposite ordinance mandating that every head of household keep a firearm in the home.\(^11\) After the April 2007 Virginia Tech shooting of 33 people, renewed calls were made for more restrictions or bans of all firearms. Responsible gun owners, sportsmen, and hobbyists will endure the same restrictions as those who should not own a weapon.

FORCED DETENTION

During the Republican Convention of 2004, over 1,000 people were detained for marching peaceably in the street, exercising their freedom of assembly in the 1\(^{st}\) Amendment. They were held in an abandoned warehouse that formerly contained chemicals and many detainees (all U.S. citizens) became ill. Thirty-two hours passed before some detainees were brought before a judge. Finally after two days, all were freed without charge and were never informed of the reason they were detained.\(^12\)

If a true public health emergency occurs—bird flu or smallpox—those who are ill may need to be quarantined in order to contain the disease. The earlier-mentioned Model States Emergency Health Powers Act of 2002 allows governors, through the National Guard and each state’s emergency response plan, to remove persons from their homes at gunpoint and place them in relocation centers.\(^13\) Failure to comply is a crime. A related scenario occurred during Hurricane Katrina when police and FEMA forcibly removed many people from homes they refused to leave.\(^14\) While quarantines have been upheld throughout history, a wide range of privacy and property rights could be violated. In 1984, FEMA began a
construction program for detention camps in the United States. “Readiness Exercise 84” was created to prepare for a mass influx of immigrant aliens from Central America. Though the influx has not materialized, the camps are still operational. It is reported by alternative news sources that about 600 camps exist around the country.

**“DOMESTIC TERRORISM”**

Section 802 of the PATRIOT Act defines “domestic terrorism” as

```
(A) acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
(B) appear to be intended
   (i) to intimidate or coerce a civilian population;
   (ii) to influence the policy of a government by intimidation or coercion; or
   (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and
(C) occur primarily within the territorial jurisdiction of the United States.
```

The language here equates domestic crime with “terrorism.” Could bank robbery, extortion, or even pyramid schemes fall under this statute? Would someone convicted here be a “terrorist?” If one is hereunder considered a terrorist, is it a big leap to also be an “enemy combatant” as described by the Military Commissions Act of 2006? The Act creates a system of justice outside the U.S. court system ostensibly for non-U.S. citizens declared to be enemy combatants. An “enemy combatant” is, by Section 1, Subsection 948a, “a person who has engaged in hostilities or who has purposefully and materially supported hostilities against the United States.” Such persons are to be held and tried by “military commissions” where normal procedural and substantive rights such as those in the 4th, 5th, 6th, and 8th Amendments do not apply. Furthermore, Section 7 of the Act specifically denies an enemy combatant the right of habeas corpus spelled out in Article I, Section 9 of the U.S. Constitution. Habeas corpus means that the government must produce evidence of a crime or set a person free. If one has no right of habeas corpus, then what is to prevent one’s case from being mired in the military commission system forever much those like at Guantanamo Bay, Cuba? More than 388 people have been there for more than five years without being charged.

The question of balance between security and liberty is a thorny one, and we will not decide it here. The public would like to see accountability. Many assume arbitrariness in the manner of warrantless wiretapping, and some investigations have shown the government overstepped its authority in some instances. With 16 federal intelligence partners all collecting information, several different police forces, cameras, and now a new military justice system for terrorists, whoever they be, the potential for abuse of this power is huge. We all know a balance between good order and individual liberty is needed. We just do not know where to draw the line. Did the Framers guarantee perfection? No. But, as Benjamin Franklin so aptly put it, “they who can give up essential liberty for a little temporary safety deserve neither security nor liberty.”

**NOTES**

3. Section 213 of the PATRIOT Act states notice does not have to be given to those under investigation and a Department of Justice Document titled, “The Attorney General’s Guidelines on General Crimes, Racketeering Enterprise and Terrorism Investigations” at
http://www.usdoj.gov/olp/generalcrimes2.pdf explains the very broad power to search personal records and documents for any purpose.


15. In 1984 FEMA held multi-agency drills. One was called “Readiness Exercise 1984.” A series of detention camps was constructed and they appear to be operational today. http://www.army.mil/cmh/books/DAHSUM/1984/ch02.htm


**Conclusion**

We have touched on some very important issues in this volume. The larger homeland security effort will likely be with us for the foreseeable future and will have a sizeable impact on our lives. Indeed, it already has.

Homeland security represents the largest reorganization of our government in the last 50 years through the construction of new offices and the reformation of old ones. The United States has adopted new missions and created new strategies. We have outlined a series of “tasks” both general and specific for federal, state, and local agencies to be able to perform. We have created a nationwide response plan and a management framework to support that plan, each extremely complex in its own way. One can question whether those responsible will be able to carry out their assigned roles in the excitement and shock of a future event. When the situation becomes complex, the decision rules need to get simpler.

Through the above framework of strategies, directives and missions, we have created programs for traveling, programs for shipping and doing business, programs to ascertain identity, and programs to “watch,” among others. Organized around the four basic categories of security activity; “prevent,” “prepare,” “respond,” and “recover,” scarcely any category of life or behavior is left uncovered by one or more programs. We have vaulted technology into a high place to assist us in these new missions, sometimes placing reliance on technology above reasoned human judgment.

We have engaged in a federal partnership in which the burdens of security are shared by government at all three levels. Every dollar spent on the homeland security effort is a dollar not spent on roads or schools or healthcare or any of the myriad of competing priorities our three levels of government routinely face. We are attempting to engage the private sector as well because of the preponderance of assets owned and controlled by them. The assets of infrastructure, the banks, the utilities, the phone companies, all combine to order and guide our lives and therefore must be included in any security attempt.

The bulk of this effort has also raised the specter, to many, of the “police state,” or “Big Brother.” The saying, “be careful what you wish for, you might get it,” looms large in this attempt. The weight of the laws, missions, strategies, programs, and bureaucracy that has been created threatens the value and primacy of the individual and civil rights. We return to the questions posed in the Introduction. How much security do we need and how much liberty are we willing to give up to get it? Only time will tell.
Group/Discussion Questions

1. Should the national government force states and cities to adopt the National Response Plan and the National Incident Management System?

2. If you were making an emergency plan, where would you begin?

3. How did the National Strategy for Homeland Security come about?

4. What tasks must state and local governments be prepared to fulfill?

5. How would you define security? What would you include under the term?

6. Should the national government or the state and local governments be responsible for security? Should it be shared?

7. If you were going to begin a surveillance program on your campus, where would you start and what would be included in “surveillance?”

8. Looking at the Target Capabilities List in Chapter 2, which of the tasks would be most difficult to accomplish and why?

9. If an event, natural or man-made, were to occur in your city, what is the chain of events that would likely occur?

10. The PATRIOT Act allows surveillance of U.S. citizens without warrants issued by a judge, possibly without “probable cause.” Would you alter the Act and how?

11. What do you think the government should do with respect to infrastructure security? Should the taxpayers fund security efforts?

12. If pandemic flu, or some other public health emergency, should arise, what actions would you and your family take?

13. How would you and your family cope with a nationwide cyber attack or a collapse of the financial system of this country?

14. Would you be willing to pay an extra fee to obtain your driver’s license so that biometric information could be placed on the license in the name of security?

15. If the government mandated smallpox vaccinations but required individuals to pay for the vaccine, would you show up and pay the fee?

16. The number of agencies and persons involved in homeland security continues to grow each year. With a minimum of 22 agencies and 180,000 individuals, do you think the effort is going well?