

December 15, 2002

‘America Still Unprepared’

Bipartisan report warns that the nation remains highly vulnerable to terrorist attack

Last October, an independent, bipartisan task force commissioned by the Council on Foreign Relations (CFR) released a report assessing the nation’s progress in building a defense against terrorism. Chaired by former Senators Gary Hart (D-Colo.) and Warren B. Rudman (R-N.H.), the task force issued the following warning: “A year after September 11, 2001, America remains dangerously unprepared to prevent and respond to a catastrophic terrorist attack on U.S. soil. In all likelihood, the next attack will result in even greater casualties and widespread disruption to American lives and the economy.”

The 40-page report, “America Still Unprepared—America Still in Danger,” concisely summarizes the risks confronting the United States and recommends specific actions to mitigate those risks. The task force members credit federal and local government efforts in the wake of September 11, 2001, to respond to the threat of catastrophic attacks. The task force does not seek to allocate blame for the security failings that contributed to the success of those tragic assaults but to close the gap between the recognized terrorist threats—as gained through U.S. intelligence sources—and the nation’s ability to prevent, minimize and respond to these dangers.

Many of these suggestions require government action, such as emergency funding and legislation, but others involve the participation of the private sector to fortify critical vulnerabilities. In addition, private industry can play an important role in convincing the government to continue making the war against terror a top priority. Unfortunately, economic pressures have forced many entities to reduce security coverage even below the levels predating September 2001, thereby increasing the country’s vulnerability to future assaults.

Several important developments have occurred since the terrorist attacks of September 2001 that impact the state of national security. Last month, for instance, President George W. Bush signed a bill to create a new Cabinet-level Department of Homeland Security. Enactment of this ambitious legislation is timely, but based on historic precedents, it will likely take years—if not decades—for this widespread reorganization to come to fruition. American citizens cannot rely on this super-department to quash the immediate terrorist threats and must take other action.

Meanwhile, the country has gained support within the United Nations to back military action against Iraq should Saddam Hussein continue to defy U.N.-imposed sanctions against weapons of mass destruction and associated inspections. Many people believe that confronting Iraq is an important step toward protecting American interests. At the same time, the CFR task force warns that a war with Iraq could command all of the nation’s attention and available resources, possibly diverting the country’s focus from the continuing terrorist threat and thereby increasing domestic vulnerability.

The current recession also threatens national security as discontent brews between the haves and the have-nots. Growing financial hardships may spark social unrest of the nature that led to the ultimate demise of the medieval feudal society—sometimes through extremely violent means. Homeland security initiatives must address this potential threat from within the nation’s borders, lest the external focus leave the United States vulnerable to homegrown malcontents.

Strengthening homeland security

In examining the current state of homeland security, the task force began with three basic premises, which must be accepted as “facts of life” in the post-September 11 world. First, the United States of America is engaged in a war against terrorists who want to attack its homeland, and the nation must take immediate action to rectify its greatest vulnerabilities. Second, moving quickly to increase the country’s emergency preparedness is essential to minimizing casualties in the event of a domestic attack. Finally, an ill-prepared response can ultimately inflict more damage than any single terrorist assault by compelling the U.S. government to enact extreme, reactionary legislative measures that compromise individual liberties.

(continued on next page)

‘America Still Unprepared’

Bipartisan report warns that the nation remains highly vulnerable to terrorist attack

(continued from preceding page)

The task force presented the following guidelines to help shape the country’s course of action in fighting the war on terror:

Limit the impact of an attack. Fortifying homeland security initiatives can reinforce counterterrorism actions abroad by making the United States a less attractive target. Securing the country so that a terrorist attack will either fail outright or produce minimally disruptive consequences at best will significantly decrease the likelihood of a future assault.

Capitalize on the strengths of federalism. The diverse complexity of American society precludes the use of a “one-size-fits-all” approach to the terrorist threat. The federal government plays a key role in ensuring homeland security through national coordination and resource allocation, but much of the expertise to reduce the nation’s vulnerabilities is found at local levels and in the private sector. National leaders have a civic responsibility to encourage the participation of these groups, allowing the United States to benefit from the knowledge of local, state and regional experts, both public and private.

Save lives through emergency preparedness. The ability of the United States to strike back with swift, devastating force does not deter agents of terror. Consequently, the nation must invest the resources necessary to protect citizens in the event of a chemical, biological or even nuclear attack. These weapons of mass destruction represent “equalizers” to the present enemy, which recognizes its inability to compete with the U.S. military. Failure to address this vulnerability could produce heavy losses of veteran firefighters, police, medical professionals and other emergency responders.

Adopt a proactive mindset. Even today, the country continues to focus on thwarting future attacks that follow the pattern of the September 11 hijackings. While this reactionary approach is understandable, the task force members warn that such a mindset can inevitably waste resources

and distract agencies from anticipating—and developing defenses for—more likely scenarios.

Homeland security measures have other societal benefits. Like the U.S. government and businesses, terrorists also have limited resources, which forces them to plan their attacks carefully to achieve the greatest impact. Selling stronger security to combat a low-probability, but potentially high-consequence, risk such as a terror strike can prove especially difficult in today’s economic circumstances. At the same time, such investments almost always have other, immediately tangible benefits. Improving the public health system, for instance, will not only mitigate a potential biological attack, but it will also enhance the nation’s ability to respond to natural disease outbreaks. Focusing on such benefits may help fund additional security through loss reductions elsewhere.

An action plan

Using the above premises as a guide, the report identifies several key areas to focus national efforts in hardening the U.S. homeland against terrorist attacks.

Strengthen local counterterrorism efforts.

More than 650,000 local, county and state law enforcement officers can assist the Federal Bureau of Investigation (FBI) with the identification and investigation of potential terrorists, but they operate in an information void. Antiquated legislation denies local access to the terrorist watch lists that the U.S. Department of State provides to immigration and consular officials. Additionally, local responders still lack the appropriate protective gear and detection equipment—and the required training—to identify and manage a chemical, biological or radiological attack. In fact, most U.S. metropolitan areas do not have interoperable systems that would enable local, state and federal response personnel to communicate with one another in a major emergency. Even at the municipal level, little coordination typically occurs between police and fire departments, which could contribute to a signifi-

cant breakdown in communication following a terrorist incident or other large-scale disaster.

To help correct this huge vulnerability in the nation's local defenses, the task force urges the following actions:

- Establish a 24-hour command center in every state to provide a real-time link between local and federal law enforcement. When suspects are apprehended by local or state police, the center could check their identities against federal and Interpol databases and give either a red or green light to hold or release them.
- Crack down on identity fraud by increasing anti-counterfeit safeguards in the driver's license and passport systems and launching joint task forces at the local, state and federal levels to investigate and prosecute false identification traffickers.
- Provide immediate funding to enable firefighters and other first responders to obtain the equipment and training necessary to handle a biological, chemical or radiological attack. This single step will dramatically reduce the risks to emergency responders, as well as the injury and death rates of victims.

Protect the critical infrastructure. Terrorists can strike anywhere, but they will likely choose high-profile facilities with the potential for massive disruption. When it comes to the national infrastructure, however, "critical" is a relative term. The nation must focus its attention on infrastructure sectors based on relative vulnerability and consequence. Many of the country's energy distribution systems, for example, are highly concentrated and sophisticated—and vulnerable. A coordinated attack on several key points in the electrical power system could produce multistate blackouts, with acute shortages requiring rolling blackouts for as long as several years in some regions of the country. Likewise, the U.S. food and agriculture industry is yet another largely unprotected sector with tremendous potential for

severe economic disruption through biological attack, and the vulnerabilities in the nation's water supply present a rich opportunity for terrorists to inflict civilian casualties. The securities and banking industries are also highly concentrated, relying heavily on a small number of core organizations for clearing and settlement activities; the loss of one of these financial clearinghouses could have disastrous economic consequences both inside the United States and abroad.

The CFR report recommends the following steps to protect these essential functions:

- Conduct a cross-sector analysis of the national infrastructure and determine which vulnerabilities have the greatest potential cascading interruption and losses across multiple sectors.
- Fund risk assessments of U.S. energy distribution centers, to be completed within six months. Meanwhile, create a stockpile of modular backup components that will restore operation to the energy grid in the event of an attack or other disaster.
- Increase funding to improve the U.S. Department of Agriculture's ability to detect and manage plant and animal disease and to enable the agency to host an online communications network connecting it with states and U.S. trade partners.
- Develop integrated networks and real-time data backup repositories among the key players in the government securities market, testing regularly for recovery and resumption capabilities.

Improve public health systems. Few cities are capable of handling the unique challenges associated with a chemical or biological attack. In chemical terrorism, the primary goal is to identify the substance used and to administer the appropriate antidote within a very small window of opportunity, usually ranging from a few minutes to two hours. Biological attacks, on the other hand,

(continued on next page)

‘America Still Unprepared’

Bipartisan report warns that the nation remains highly vulnerable to terrorist attack

(continued from preceding page)

are more insidious, as it often takes several days before victims begin to show symptoms—even longer before the attack is identified as such. Few medical professionals, the first line of defense against biological terrorism, have received training on how to diagnose, treat and report symptoms associated with a biological attack. This lack of preparedness could have disastrous effects within the medical community in the early stages of such an assault.

The state of the American public health system requires a sustained focus to correct the widespread deficiencies within, but these recommendations can increase the nation’s ability of successfully mitigating a chemical or biological assault:

- Require all major cities and counties to plan and train for catastrophic situations. These scenarios may seem too terrible to contemplate, but preparing for them may significantly reduce the casualty rate.
- Create public health surveillance systems that include monitoring ambulance calls, reports from pharmacies concerning a surge in request for certain over-the-counter medications, and increased absenteeism in schools and businesses.
- Enlist corporations and schools to assist in distributing medications during a crisis. The federal government will soon have the ability to deliver drugs and vaccines to virtually all urban areas within six hours, but no system for distributing these pharmaceuticals has yet been developed.

Remove federal obstacles to public-private partnerships. Although most people view the burden of homeland security as resting with the federal government, much of the preparation must take place at the local and state levels and in the private sector, which operates much of the nation’s critical infrastructure. Additionally, much of the expertise about the vulnerabilities and the

best protective measures is also found at these levels. Consequently, the government needs to relax existing barriers to sharing information between the public and private sectors, including concerns about antitrust violations. Such partnerships also need to extend to global allies that have greater experience in dealing with the terrorist threat.

To facilitate this exchange of information, the task force recommends the following measures:

- Solicit the participation of private-sector authorities in government-sponsored risk assessments. Draw upon the knowledge of the experts involved in the design and operations of the nation’s critical infrastructure sectors.
- Organize survey teams to conduct studies in other nations with experience in managing urban terrorism, analyzing transportation security, and studying intelligence-sharing arrangements between the public and private sectors.

More than one year after the attacks of September 11, 2001, yet another bipartisan task force has concluded that the United States of America is no more prepared to counter another catastrophic attack than it was on that fateful day. Contributing to this vulnerability is the fact that many organizations have actually reduced their security levels in light of continuing economic pressures. Local and state entities must join forces with companies in the private sector to support the monumental task facing the federal government.

The warning is clear. The potential consequences of ignoring this message are devastating. Corporate America must use its influence and heed the call to arms now, before more innocent citizens fall victim to the new war of the 21st century: the war against terror.



The Lipman Report Editors