

September 15, 2002

## One year later — September 11, 2002

### Security awareness heightened, yet progress still needed in homeland protection

*In Washington, D.C., an analyst for the Central Intelligence Agency immediately relays disturbing information: intercepted radio communications indicate that al Qaeda forces are planning an attack against a high-profile American target. Unfortunately, the transmission offers no clues as to the target's location. Her stomach sinks as she passes on the message. In all probability, this is simply another false alarm, but she lives with the fear that each new threat could herald another catastrophe of the magnitude experienced last fall.*

*In Dallas, Texas, a purchasing manager for a private business examines the proposed budget for the new fiscal year. Sales have declined because of the economic slowdown, and senior management demands that he reduce expenses by 20 percent. He realizes that achieving his mission will involve cutting benefits and renegotiating rates with existing vendors. As he wrangles with the difficulty of the task before him, he does not worry about the ongoing war on terror. He has more pressing concerns at hand, and the chances of a terrorist strike in the middle of the country seem beyond remote.*

*These two individuals illustrate the dichotomy that currently exists in the United States, one year after the horrific events of September 11, 2001. For certain individuals—those who live in the Northeast, for instance, and those directly involved in protecting the nation—the fight against terror is an ever-present issue that shapes everything they do. For the vast majority of the population, however, time has created enough distance for them to feel safely removed from the tragedy, believing the attacks to be a one-time occurrence, rather than a foreshadowing of things to come.*

*This issue of The Lipman Report examines the progress made in increasing security during the past 12 months and explores further measures that must be taken.*

#### National complacency

One factor that contributed to the September 11 attacks was the mistaken notion that the United States was safe from an assault on domestic soil. Before that day, the worst attack within U.S. borders was the Oklahoma City bombing, committed by a native-born American. Foreign terrorists only struck at U.S. targets abroad, with the exception of the 1993 bombing of the World Trade Center. The United States felt comfortable in its role as the sole

remaining superpower. The nation possessed the strongest military and the best intelligence network. The country successfully fought in two world wars while keeping the battles confined to foreign soil—again, with one notable exception: Pearl Harbor. Few people believed that outside terrorists could strike Americans on their home ground.

Largely as a result of this complacency, the United States has historically regarded terrorist attacks as nuisances. The nation identified and prosecuted the perpetrators of previous incidents—such as the World Trade Center bombing and the bombings of the U.S. embassies in Kenya and Tanzania—as individual criminal cases, instead of addressing the greater threat presented by the militant Islam movement. Consequently, the forces of al Qaeda came to regard the United States as a paper tiger, one that would run away if dealt a significant blow.

The American response to September 11 proved the error of this assumption, but the sleeping giant has not fully awakened. The continuing pressure of an uncertain economy—further depressed by new reports of corporate misconduct—has focused attention on preserving the nation's financial well-being. Stronger security initiatives, once the top priority of lawmakers and private businesses alike, have again receded in importance. Complacency has started to settle in across the country, rendering the nation vulnerable to future assaults.

One terrorist expert predicts that it will take another attack on the scale of September 11 to fully motivate the nation to act against the forces that threaten the American people. He describes the process as “education by murder”: as more Americans lose their lives, the nation becomes smarter.

#### Intelligence gathering

Another problem that enabled the September 11 attacks stems from the fact that obsolete laws and attitudes have historically hindered U.S. intelligence agencies. At the time of the assaults, for example, legislation limited agencies' efforts to

(continued on next page)

---

## One year later — September 11, 2002

### Security awareness heightened, yet progress still needed in homeland protection

(continued from preceding page)

obtain information that could help prevent a terrorist act, instead focusing on the response to reported threats and actual incidents. Additionally, prevailing attitudes disdained the use of human intelligence—which involved interaction with unsavory characters—in favor of the “cleaner” electronic intelligence that relied on technology. This trend created significant gaps within the government’s information stores.

During the past year, the federal government has enacted legislation that increases the ability of intelligence agencies to investigate leads that could prevent future attacks. Changes in the Federal Bureau of Investigation embody the nation’s significant shift in attitude. Formerly dedicated to the response and prosecution of criminal acts, the Bureau is moving toward a more proactive role in fighting acts of terror, as evidenced by increased recruitment that focuses on individuals with key language skills. The proposed Cabinet-level Department of Homeland Security will help streamline the processing and sharing of intelligence, but the logistics of this monumental government reorganization will take many years, if not decades. Private organizations must therefore assist in national security efforts by acting in some of the areas addressed below.

#### **Airport security**

The failed bombing attempt at the World Trade Center in 1993 demonstrated that conventional explosives would not topple the gleaming towers, so the terrorists achieved their objective through previously inconceivable means, using commercial passenger jets as weapons. The act of hijacking four planes in a single morning for this deadly purpose brought the national spotlight to flaws in the country’s airport security. Had security been as tight as most Americans believed, these attacks might not have succeeded.

In November 2001, the U.S. government enacted the Aviation and Transportation Security Act, which mandates federalization of the security pro-

grams at all airports, allowing for a few pilot programs with private security providers after one year. This act represents an important step toward improving airport security, but little has truly changed since its enactment. Although the legislation called for the transition to federalized security by February 2002, the same individuals who provided security before September 11 continue to screen passengers in many cases. Not only is the government experiencing difficulty recruiting people for airport security, but recent reports also reveal that some organizations that provided security in the months following the terrorist attacks opportunistically increased their rates, in some cases nearly doubling them.

The government has encountered several difficulties in implementing the provisions of the law. For example, the original deadline to equip all airports with explosive-detection machines—December 31, 2002—is in serious jeopardy. As of August, site assessments for installing the equipment had not even been completed due to such problems as lack of funding and change of leadership.

The situation does show signs of improvement, however. Last month, U.S. Secretary of Transportation Norman Mineta announced the appointment of 20 Federal Security Directors to oversee security and enforcement at the nation’s airports. This development may facilitate progress as the new directors evaluate the programs under their responsibility and implement changes.

#### **Biochemical defense**

The events of, and following, September 11 pointed out two terrible realities. First, the deadly resolve of the enemy makes a biochemical attack more possible than ever. Second, the United States is not prepared to handle such an event, as evidenced by the nation’s response to the still-unsolved anthrax mailings last fall, when widespread panic placed tens of thousands on antibiotic treatment despite limited exposure.

Since then, the nation has improved its readiness for a biochemical event, demonstrating how quick-

---

ly the government can mobilize its resources when the need arises. Because experts believe a smallpox attack is one of the more likely—and deadlier—forms of biological assault, efforts are currently underway to produce enough smallpox vaccine for every U.S. citizen, and the government is exploring ways to begin preventive immunization for first responders, medical staff and individuals in high-risk occupations. The Centers for Disease Control and Prevention (CDC) has emergency stockpiles of vaccines and antibiotics ready for immediate deployment to the site of a biological attack. Additionally, organizations such as the CDC have started training medical professionals and other emergency responders how to respond to the unique demands of a biological or chemical attack.

State health agencies have also begun efforts to improve their preparedness. These organizations recently received additional funding and objective benchmarks, such as how quickly they can identify a disease and administer vaccinations, which will provide measurable areas by which to evaluate their progress within the next year.

All of these actions are necessary to increase the country's biochemical defense, but more work remains to be done. The private sector must take an active role in preventing an attack through increased security measures and vigilance. Physical security audits need to identify and mitigate the risks of a biological attack on the premises. Tight access control can prevent a stranger from walking in and implementing an attack, just as careful background screening can help protect an organization against infiltration by a terrorist. Not only do these measures enhance national security as a whole, but they also have the added benefit of protecting companies from more common security threats, including industrial espionage and employee theft.

### **Immigration regulation**

The U.S. immigration and visa system is notoriously ineffective, which enabled most of the 19 hijackers to obtain tourist or business visas. Currently, the United States issues several different

kinds of visas, but there is little follow-up to ensure that visitors respect the time limits. Although applicants are checked against a State Department database of known security risks, the information is often outdated. Further compounding the problem is the fact that many of the embassy workers who issue visas are nationals of the host country, who do not share the same allegiance to the United States as American citizens. Lack of resources prevents immigration officials from tracking down visitors with expired visas, and existing regulations restrict U.S. businesses in their efforts to verify applicants' employment eligibility.

In response to these flaws in the present system, the U.S. Congress has introduced 13 separate legislative initiatives since September 11. Numerous redundancies exist between the five Senate and eight House bills, but all address important security lapses that contributed to the success of last fall's attacks. Even the passage of such laws, however, does not ensure swift enactment, and the proposed Department of Homeland Security complicates the situation by splitting the functions of the Immigration and Naturalization Service (INS) with the new department. This new development not only separates closely related activities, but it could also make it even more difficult for the INS to obtain the necessary attention and funding for improving its service operations—a dilemma that must be solved before the proposed bills become law. Private organizations need to actively lobby their legislators to keep these initiatives a high priority.

The lack of coordination seen in the immigration and visa system exists throughout the federal government. Improving communication and cooperation between agencies could have averted the September 11 disaster, but the world will never know for certain. The proposed Cabinet-level department would help solve many of these problems, but the U.S. Congress continues to wrestle with obstacles in making the department a reality, including decisions affecting the management of

**(continued on next page)**

## One year later — September 11, 2002

### Security awareness heightened, yet progress still needed in homeland protection

(continued from preceding page)

department employees and the extent to which these personnel would be protected as civil servants.

#### National identification card

The September 11 attacks forced the nation's leaders to consider new methods of protecting the American people. One proposed solution was a travel identification (ID) card that would include a photograph and the bearer's fingerprint. When traveling, cardholders would undergo a fingerprint scan that would confirm their identity by accessing a database. Another recommendation was the addition of photographs and fingerprints to Social Security cards, a move that would strengthen national security and decrease fraud within the Social Security system. Currently, citizens need only apply once for a card, with the exception of name changes; a photo ID would require periodic renewal to ensure that the photo remained current. These extensive changes would incur additional expense that exceeds the Social Security Administration's operating budget, but could be offset by the reduction in fraud.

Suggestions of a national ID card raise numerous red flags among civil liberties groups, but the situation could be addressed simply by improving the current system used to issue driver's licenses—the most commonly accepted form of identification in the United States. The issuance of driver's licenses is rife with inconsistencies and prone to fraud. Several states are working to strengthen standards for issuing driver's licenses, but solutions must be implemented nationwide. Individual states should retain authority to regulate the administration of licenses, while adhering to agreed-upon minimum standards. Suggestions under consideration include verifying applicants' identities through background checks and fingerprints. Increasing the integrity of the driver's license system would be a relatively easy, effective way to fortify national security. To give the issue the attention it needs, private organizations must lobby their government representatives to take action.

*As the anniversary of the September 11 tragedy passes and time distances us from the horror of those events, we cannot allow complacency to again settle in and render us vulnerable to the murderous plans of terrorists. Although the nation has taken many important steps toward ensuring domestic safety, much work remains to safeguard the peace and prosperity that has characterized this great democracy. We must remain vigilant, increasing the security of individual establishments in the private and public sectors, while lobbying for stronger legislation that will assist our law enforcement agencies in pre-empting future strikes. Protecting our homeland requires many difficult decisions as we strive to balance personal liberty with measures such as a proposed national identification card. Still, these issues require swift resolution. Each day that passes could bring the country closer to the next assault.*

*We have not won the war against terror, but we can mitigate the impact of future attacks. The federal government can improve national security on several levels: tightening existing immigration regulation, expanding the authority of federal law enforcement agencies and streamlining the sharing of intelligence; uniting the myriad aspects of national security under a single entity, reducing the potential for fatal communication breakdowns. Businesses can practice tighter screening measures and implement tougher access control, preventing potential terrorist agents from infiltrating their organizations while reducing more common threats, such as workplace violence. Individuals can maintain a watchful eye as they continue with the necessary business of living their lives to the fullest extent.*

*We as a nation can and will prevail, but we must maintain constant awareness and unite to ensure that terror never again exacts the toll we paid on September 11, 2001.*



The Lipman Report Editors