# Less Talk, More Walk

## *Strengthening Homeland Security Now*

EXECUTIVE SUMMARY

BY DAVID ISENBERG

The Center for Defense Information is a non-partisan, non-profit organization committed to independent research on the social, economic, environmental, political and military components of global security. To ensure the ability to provide objective analysis, CDI accepts no government or defense industry funding. Its central aim is to educate the public and inform policymakers about issues of security policy, strategy, operations, weapon systems and defense budgeting, and to produce creative solutions to the problems of today and tomorrow. To encourage the intellectual freedom of the staff, CDI does not hold organizational positions on public policy issues. Instead, staff members are dedicated to the concept that the public and political leaders can, and will, make wise choices on complex security matters when provided with facts and practical alternatives.

*The views expressed in CDI publications are those of the authors.*

Center for Defense Information
1779 Massachusetts Avenue, NW
Washington, D.C. 20036-2109

# Less Talk, More Walk

*Strengthening Homeland Security Now*

EXECUTIVE SUMMARY

by
David Isenberg

CENTER FOR DEFENSE INFORMATION
Washington, D.C.
November 2002

## ABOUT THE AUTHOR

**David Isenberg** is an independent consultant on defense and security affairs. From 1998 to 2001, he was an analyst at DynMeridian where he worked on biological weapons arms control issues. From 1989 to 1998, he was a senior research analyst at the Center for Defense Information where he researched U.S.-Third World security issues, i.e., international arms trade, Persian Gulf, regional and low-intensity conflicts, power projection capabilities, military anti-drug efforts and covert operations.

He has worked as a research associate at the Project on Military Procurement and as a research fellow at Business Executives for National Security.

He served in the U.S. Navy from 1973 to 1977.

He is an adjunct scholar at the CATO Institute, associate fellow at the Matthew B. Ridgway Center for International Security Studies at the University of Pittsburgh, research director of Military Insights, advisor on international security issues to *The World* (one-hour daily international news radio journal produced by BBC World Service, Public Radio International and WGBH Boston) and a member of the Council for Emerging National Security Affairs.

He has published more than 100 articles, papers, studies, television scripts, book reviews, and op-eds on defense, military, arms control, and international security issues, and testified before Congress and at professional military schools.

He received his B.A. in International Studies from the University of Oregon and M.A. in International Affairs from American University.

## ACKNOWLEDGEMENTS

The author would like to thank CDI Vice President Theresa Hitchens for initiating this project, and for her guidance, insights and many helpful suggestions. Thanks also to Martin Calhoun for his editing.

# Executive Summary

It is now a truism to say that Sept. 11, 2001, changed everything. But this is not true when it comes to efforts to prevent terrorism and attacks against the U.S. homeland. Since 1960, there has been a proliferation of U.S. counterterrorist measures. Dealing with the burgeoning number of counterterrorist agencies and bureaucracies created over the past decades is only part of the challenge to improving homeland security.

Additionally, much of the planning, with a few significant exceptions, has been on paper without commensurate funding or realistic training to back it up. Some of the programs were developed without recognizing existing state and regional coordinating mechanisms for emergency preparedness. Moreover, some of these programs overlapped because several federal agencies had similar efforts that were not well coordinated with each other.

Long before Sept. 11, the U.S. government was preparing for the worst-case scenarios. For example, on June 5, 2000, the National Commission on Terrorism, a congressionally mandated bipartisan body, issued its report. Similarly, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, also known as the Gilmore Commission after its chairman James Gilmore, the former governor of Virginia, which was charged with assessing the capabilities for responding to terrorist incidents in the U.S. homeland involving weapons of mass destruction (WMD), has issued several reports.

Part of the problem in preparing for and implementing effective homeland security was that government officials were reluctant to create a sense of crisis. So the wisdom of many who had anticipated the brutal truth that a terrorist attack against the United States was likely — like the U.S. Commission on National Security/21st Century, known as the Hart-Rudman Commission after its co-chairs, former Sens. Gary Hart and Warren Rudman, which recommended that the president propose and Congress should agree to create a new Department of Homeland Security — was ignored.

On June 6, 2002, President George W. Bush announced that he would move to establish a Department of Homeland Security, following his creation of a Cabinet-level Office of Homeland Security (OHS). However, at this time it remains unclear how the new department will function or even how it will be structured, since Congress has yet to sort out and approve the details.

## Bureaucratic Wonderland

There are a dizzying array of governmental departments and agencies involved in planning for homeland security. Previously, these included the Na-

**Table 1. Appropriations for Combating Terrorism and Protecting Critical Infrastructure Since 1998 and the Funding Requested for 2002 Before Sept. 11, 2001**
***(In millions of dollars)***

| Department or Agency | 1998 | 1999 | 2000 | Original Funding for 2001 | President's Request for 2002 |
|---|---|---|---|---|---|
| DoD and Intelligence Agencies | 4,919 | 5,485 | 6,757 | 7,267 | 8,252[a] |
| State | 202 | 1,654 | 792 | 1,311 | 1,549 |
| Justice | 630 | 716 | 765 | 939 | 1,038 |
| Energy | 505 | 619 | 724 | 754 | 834 |
| Treasury | 401 | 423 | 406 | 475 | 474 |
| Health and Human Services | 53 | 218 | 325 | 387 | 446 |
| Transportation | 192 | 296 | 313 | 366 | 401 |
| All Others | 295 | 385 | 372 | 537 | 573 |
| **TOTAL BUDGET AUTHORITY** | **7,197** | **9,794** | **10,454** | **12,036** | **13,566** |

SOURCE: Congressional Budget Office based on Office of Management and Budget, *Annual Report to Congress on Combating Terrorism* (July 2001).

NOTE: The totals shown here are larger than those presented by the Congressional Research Service and other organizations because CBO has included funds for protecting critical infrastructure.

a This figure for the Department of Defense (DoD) and intelligence agencies is different from the one in the Office of Management and Budget's report because CBO has included an adjustment made in the president's FY 02 amended budget request.

**Table 2. Comparison of Funding for Combating Terrorism and Protecting Critical Infrastructure Before and After Sept. 11, 2001**
***(In millions of dollars)***

| | 2001 | | | 2002 | | |
|---|---|---|---|---|---|---|
| **Department or Agency** | **Original Funding** | **Funding with Supple-mental** | **Change** | **President's Request** | **Estimated Funding[a]** | **Change** |
| DoD and Intelligence Agencies | 7,267 | 10,833 | 3,566 | 8,252[b] | 9,314 | 1,062 |
| Health and Human Services | 387 | 405 | 18 | 446 | 3,067 | 2,621 |
| Justice | 939 | 1,020 | 81 | 1,038 | 2,633 | 1,595 |
| State | 1,311 | 1,467 | 156 | 1,549 | 1,549 | 0 |
| Transportation | 366 | 916 | 550 | 401 | 1,360 | 959 |
| Energy | 754 | 759 | 5 | 834 | 1,065 | 231 |
| Treasury | 475 | 554 | 79 | 474 | 711 | 237 |
| Agriculture | 60 | 60 | 0 | 50 | 341 | 291 |
| FEMA | 35 | 35 | 0 | 3 | 281 | 245 |
| Postal Service | 0 | 175 | 175 | 0 | 250 | 250 |
| Legislative Branch | 0 | 376 | 376 | 0 | 232 | 232 |
| NASA | 117 | 117 | 0 | 117 | 226 | 109 |
| General Services Administration | 114 | 123 | 9 | 117 | 210 | 94 |
| District of Columbia | 0 | 6 | 6 | 0 | 200 | 200 |
| Interior | 10 | 13 | 3 | 10 | 128 | 118 |
| Judiciary | 10 | 31 | 21 | 10 | 105 | 95 |
| Social Security Administration | 71 | 71 | 0 | 101 | 105 | 4 |
| Environmental Protection Agency | 5 | 5 | 0 | 5 | 93 | 88 |
| Commerce | 47 | 47 | 0 | 55 | 71 | 16 |
| Executive Office of the President | 0 | 82 | 82 | 2 | 50 | 48 |
| Veterans Affairs | 22 | 22 | 0 | 22 | 24 | 2 |
| Labor | 15 | 15 | 0 | 23 | 23 | 0 |
| International Assistance | 13 | 18 | 5 | 12 | 12 | 0 |
| Education | 12 | 12 | 0 | 9 | 9 | 0 |
| Office of Personnel Management | 1 | 1 | 0 | 0 | 0 | 0 |
| Other Independent Agencies | 5 | 5 | 0 | 5 | 185 | 180 |
| **TOTAL BUDGET AUTHORITY** | **12,036** | **17,166** | **5,130** | **13,566** | **22,242** | **8,676** |

SOURCE: Congressional Budget Office based on Office of Management and Budget, *Annual Report to Congress on Combating Terrorism* (July 2001).

NOTES: These figures include funds associated with combating terrorism and protecting critical infrastructure according to the Office of Management and Budget's classifications in its July 2001 report. They exclude an estimated $1.25 billion authorized by P.L. 107-71 for aviation security, which is to be offset by fees. Of the roughly $8.7 billion in added funds for 2002, about $8 billion was from emergency supplemental legislation (P.L. 107-117), and about $700 million was added in the 13 regular appropriation acts, according to CBO's estimates.

a. Figures in this column reflect CBO's estimate of homeland security funding for each agency. Actual spending will not be known until agencies make their budget allocations and report to OMB.

b. This figure for DoD and intelligence agencies is different from the one in OMB's report because CBO has included an adjustment made in the president's FY 02 amended budget request.

tional Security Council (NSC), State Department and the FBI, to name a few of the most prominent.

The 1995 Presidential Decision Directives (PDD) 39 and PDD 62, and the 1998 PDD 63 reaffirmed these roles.

In February 2001, Bush signed National Security Presidential Directive No. 1, which fine-tuned the existing NSC structure.

On Oct. 8, 2001, Bush signed an executive order establishing the OHS to lead, oversee, and coordinate a comprehensive national strategy to protect the nation against terrorism. Former Pennsylvania Gov. Tom Ridge chairs the OHS.

The executive order relies on coordination, but never mentions control. The new organization's mandate is carefully circumscribed to involve only coordination, leaving unaltered the existing authorities of the operating departments and agencies. In the meantime, many questions remain to be answered. For example, will Ridge have direct control over the counterterrorism budgets in other agencies, which could be key to shaping the anti-terror bureaucracy?

How effective will the newly created OHS be? That depends. Ridge has the job of coordinating many different agencies, but he does not direct any of them. Months after taking the job, he faces doubts about his abilities and authority. Keen rivalries still exist between the various agencies, and even at the best of times, coordination is an inherently difficult job. And this is not the best of times.

Although the Bush administration subsequently announced it would establish a Department of Homeland Security (see below), it appears that the OSH will continue to exist. On July 17, 2002, Bush presented the new Homeland Security Strategy to Congress.

Still, devising a strategy is easy compared to implementing it. A national strategy for homeland security will engage players who have not been part of the traditional U.S. national security apparatus — such as the Department of Health and Human Services (HHS) and the Department of Agriculture.

There should be no mistake about the magnitude of the task now facing America. The defense of the U.S. homeland can be improved but it will not be easy. And there will never be a 100 percent foolproof defense, if for no other reason than the sheer abundance of targets available to potential attackers.

When the objective is to kill large numbers of people in spectacular fashion and cause panic and disruption, the United States constitutes a "target-

rich environment" and is extremely vulnerable to terrorist attacks. Drugs and illegal immigrants move across U.S. borders with ease; guns and stolen cars move out. Dangerous activities occur in modern society every day. Aircraft take off and land. Hazardous materials — flammable, explosive, or poisonous — move by truck, train and ship.

## Vulnerabilities and Threats

What are the challenges confronting those charged with strengthening the defense of the U.S. homeland?

### *Borders*

To say that U.S. borders are open is an understatement. According to the Census Bureau, there were close to 9 million people living illegally in America in 2000. Terrorists can slip across remote places on the U.S.-Canadian border. As of February 2002, just 345 Border Patrol agents have permanent assignments to watch the 3,987-mile line dividing Canada and the United States.

Bringing illegal immigrants across the border is big business. Drug smugglers have devised elaborate means, including tunnels, to penetrate the border.

### *Aviation*

With 9 million commercial flights each year carrying about 600 million people, and countless targets on the ground, the consequences of another aviation-centered attack could easily match those of Sept. 11.

Aviation security problems are longstanding. Today, only a small percentage of passenger luggage on domestic flights is screened for explosives. In addition, the industry must now guard against suicidal hijackers.

Nor is commercial aviation the only concern. The stealing of a Cessna 172 by a 15-year-old student pilot in Florida and his subsequent suicidal crash into a downtown Tampa skyscraper illustrated the threat posed by small planes and the general aviation system. It showed that short of grounding most private planes, the government's air defense system is unable to prevent another suicide flight. The Federal Aviation Administration (FAA) is incapable of monitoring the more than 500,000 private pilots flying more than 200,000 airplanes from 18,000 airports all over the country, much less stopping these small planes from making attacks.[1]

***Mass Transit***

Mass transit systems clearly are potential targets. Members of Japan's Aum Shinrikyo cult proved it in 1995 when they released nerve gas into Tokyo's subway system, killing 12 and injuring 5,500.

Much of the heavy freight in the United States, including large quantities of hazardous materials, is transported by rail. In addition to being critical components of the nation's transportation system, trains can become targets for terrorists. Rails often pass close to metropolitan centers and also travel through rural areas. This can represent problems in terms of massive releases of chemicals being transported as cargo, which can burn or explode, or may themselves be toxic.

***Maritime Security***

Seaports are the conduits through which 95 percent of U.S. imports and exports — excluding trade with Canada and Mexico — flow. "Maritime security" covers a variety of different, distinct industries and elements, including inland waterways, port facilities, marine terminals, non-maritime facilities located on navigable waters, bridges, cruise ships, tankers of various types, and the liner industry.

Most ports are near population centers and are packed with bridges, power plants, and combustible and hazardous materials. Thus ports represent significant points of vulnerability.

In terms of possible targets and means, the scenarios are near infinite. Terrorists may sabotage or attack installations like the natural gas tanks along Boston Harbor, the petrochemical complexes of Houston, or the vast collection of oil tanks at the terminus of the Trans-Alaska Pipeline in Valdez, Alaska.[2]

About 6 million containers arrive in the United States each year by ship, but only a fraction of those containers get inspected. U.S. Customs searches approximately 2 percent of them.

Currently, the United States has no credible way to reliably detect and intercept illegal and dangerous people and goods that infiltrate our maritime and surface transportation networks.

***Nuclear***

Information about basic weapon designs is commonly available. Given reports of lax nuclear material controls in Russia and other parts of the world,

it is only prudent to assume some sort of nuclear device could be made by a would be terrorist.

Although concern about nuclear terrorism is not new, the proliferation of nuclear materials and knowledge since the end of the Cold War has made at least the likelihood of a nuclear incident more feasible. Worldwide stockpiles of fissile material — the essential ingredients of nuclear weapons — are estimated to include some 450 tons of military and civilian separated plutonium, and more than 1,700 tons of highly enriched uranium.

The Department of Defense (DoD) defines an improvised radiological device as "any device, including any weapon or equipment, other than a nuclear explosive device, specifically designed to employ radioactive material by disseminating it to cause destruction, damage, or injury by means of the radiation produced by the decay of such material."[3] Although use of such a device would probably kill few people, it would spread panic and produce severe economic damage, if only because of the difficulty of cleanup. This is because techniques for dealing with radioactive contamination rely largely on demolition and removal.

***Nuclear Power Plants***

None of the nation's 104 nuclear power plants, which provide 20 percent of the nation's electricity, were built to withstand direct, full-speed impact by today's commercial jetliners. Nor were any of the 16 decommissioned plants that store spent fuel. Might the accidental or intentional crash of an aircraft into a nuclear power plant — whether one built to withstand such a disaster or not — precipitate a radiation release? The U.S. Nuclear Regulatory Commission (NRC) now admits that the agency "could not exclude the possibility" of a radiation release "that could impact public safety." The agency formulates policies and regulations governing nuclear reactor and materials safety, issues orders to licensees, and adjudicates legal matters brought before it.

Although the possibility of a terrorist attack on civilian nuclear reactors is not new, plans to defend them seems woefully inadequate. Aside from physical design, security procedures at nuclear facilities also are in dire need of improvement.

***Nuclear Labs***

Security problems at government weapons sites are also rampant. In a drill at Los Alamos National Laboratory in 1997, the "terrorists" used a garden cart

to steal enough weapons-grade uranium for numerous nuclear weapons. In a test at the Rocky Flats nuclear production facility in Denver, Navy SEALs successfully "stole" enough material to make several nuclear weapons. The Energy Department lacks the necessary funds to adequately protect the nation's nuclear weapons research facilities.

### *Nuclear Waste*

Terrorists could also target the storage facilities for spent nuclear fuel, which is kept in special pools onsite at both power and production plants. There are about 40,000 tons of spent fuel, including hundreds of tons of plutonium, stored at operating and shutdown plants around the country, usually in concrete-reinforced cooling pools that were supposed to be temporary but now hold more radioactive material than the reactors themselves.

Despite legislation requiring it to do so, the Department of Energy has not uniformly secured the nation's nuclear waste, which could be used by terrorists to build radiological weapons. According to the department, it already is running 12 years behind schedule.

## Chemical and Biological Agents

### *Chemical Attacks*

The chemical threat can be divided into two categories: regular chemical weapons and toxic industrial chemicals.

In regard to the former, the good news is that it is easier said than done. Nerve agents are difficult to produce and require a synthesis of multiple precursor chemicals. The production and transfer of chemical weapon precursor chemicals is internationally monitored under the Chemical Weapons Convention and the informal international export regime of the Australia Group, providing some degree of control over their distribution.

### *Chemical Plants*

Pathogens may have to be "weaponized" to turn them into agents of mass destruction, but industrial chemicals already are. Some of the chemicals produced or stored in the country have the potential to match or exceed the 1984 disaster in Bhopal, India, in which a methyl isocyanate gas leak at a Union Carbide Corp. pesticide plant killed at least 2,000 people and injured 100,000. Approximately half of them suffered permanent disabilities.

Since Mohamed Atta, the ringleader of the Sept. 11, 2001, attacks, had inquired about the chemicals at a plant in Tennessee he had flown over, security agencies must assume that such facilities are being considered as potential targets.

There are many potential targets and reasons for concern, even if terrorists do not attack them. There are about 850,000 facilities in the United States that work with hazardous or extremely hazardous substances. Many of these sites are located in urban areas, and transport of hazardous substances is a routine matter. Every year, more than 60,500 accidents and incidents occur at these facilities or during the transport of these chemicals. In the past decade, about 95 percent of the counties in this nation have experienced this type of emergency. Accordingly, it stands to reason that U.S. rescue crews and hospitals need to be well prepared to contend with chemical casualties.

***Biological Attack***

Biological terrorism is not a "lights and sirens" kind of attack. Unless the release is announced or a fortuitous discovery occurs early, there will be no discrete event to signal that an attack has happened, and no site that can be cordoned off while authorities take care of the casualties, search for clues, and eventually clean up and repair the damage.

Because of the ability of microorganisms to multiply rapidly within the host, small quantities of a biological agent, if widely disseminated through the air, could inflict casualties over a very large area. Weight-for-weight, biological and toxin weapons agents are hundreds to thousands of times more potent than the most lethal chemical warfare agents, making them true WMD, or more properly put, weapons of mass *casualty*, with a potential for death and injury that can exceed that of nuclear weapons.

Biological and toxin weapons also pose, potentially, greater dangers than either chemical or nuclear weapons, because these agents are so lethal on a pound-for-pound basis that their production requires a much smaller and cheaper industrial infrastructure.

Biological and toxin weapons are much harder to control than nuclear or chemical weapons because they are readily found in nature. Any nation, group or person that wants to acquire such weapons can find the pathogen or source of most of the toxins and diseases that could be used as weapons against humans, animals and agricultural crops.

***Agroterrorism***

Unfortunately, use of microorganisms against people is not the only biological threat that must be considered. Biological warfare against crops and animals is another. The evidence suggests that an agricultural bioterrorist attack would have very serious consequences. And the threat is hardly theoretical; it has happened before in U.S. history.

The destruction or contamination of crops and/or livestock not only would deal a direct, severe financial blow to growers and breeders, but also would hurt shippers, stockyards, slaughterhouses, distributors and many others. An attack of this kind would also impact consumers, threatening not only their pocketbooks but also their confidence in the safety of the food supply.

***Ballistic Missiles***

Countries of proliferation concern vary widely in their ability to produce missiles, extend their capabilities, or design new types. While several developing nations essentially have no indigenous capability, others match that of the United States in the mid-to-late 1960s.

Only China and Russia are able to attack the United States with nuclear warheads on long-range, land-based intercontinental missiles. This has not changed since Russia and China deployed their first ICBMs (intercontinental ballistic missiles) in 1959 and 1981, respectively.

A key point that is overlooked in the WMD and missile threat debate is that missiles are not the most likely means of attack. In fact, a past National Intelligence Estimate found that "U.S. territory is more likely to be attacked with WMD using nonmissile means."

***Cruise Missiles***

Cruise missiles are an obvious system for conducting precision strikes. They can fly at low altitudes to stay below radar and, in some cases, hide behind terrain features. Cruise missiles are smaller and therefore much less visible to radar than aircraft or ballistic missiles.

Newer missiles are incorporating stealth features to make them even less visible to radars and infrared detectors. Multiple missiles could attack instantaneously from different directions and they can fly circuitous routes to get to different targets.

It is unclear how rapidly cruise missiles will spread from state to substate actors, i.e., terrorist groups. To date, no terrorist group has used a cruise missile, but they may obtain one from a state sponsor, or even build one on their own. As the relevant technology is widely available, it is possible that short- or even long-range missiles could spread to new actors.

### *Water Supplies*

Two types of water system sabotage, vandalism and terrorism, need to be considered. Vandalism interrupts the supply of water and reduces its quantity. Terrorism contaminates the water and reduces its quality.

Supply interruptions deny the population drinking water or firefighting protection, and include the destruction of, or interference with, reservoir dams, water towers or storage facilities, pumping stations, intakes, valves, treatment plants, the distribution system or fire hydrants. Supply interruptions can be caused by any number of acts, including physical destruction, interruption of the supervisory control and data acquisition system, or acts that could reduce the water pressure in a system. Supply interruptions can also occur as an indirect result of contamination. As drinking water is essential to human life, denying it for any period could cause panic and disrupt society.

Much public concern is focused on the safety of water reservoirs and treatment plants. In terms of vulnerabilities, however, the real danger may be the pipes that carry the water, not facilities that store or purify it.

By contrast, across the country, water utility officials are taking steps to prevent terrorists from reversing the flow of water into a home or business — which can be accomplished with a vacuum cleaner or a bicycle pump — and using the resulting "backflow" to push poisons into a local water-distribution system. Such an attack would use utility pipes for the opposite of their intended purpose: instead of carrying water out of a tap, the pipes would spread toxins to nearby homes or businesses.

## What Is Being Done

- On Oct. 8, 2001, Bush signed the executive order establishing the OHS to lead, oversee and coordinate a comprehensive national strategy to protect the nation against terrorism. A Homeland Security Council similar in structure and function to the existing NSC was established as well. The strategy was released July 17, 2002, and is being evaluated by Congress.

- On June 6, 2002, Bush announced he would establish a Department of Homeland Security. Though it is still unclear as to how it will work, since Congress has yet to sort out and approve the details, its structure would have four main divisions: Border and Transportation Security; Emergency Preparedness and Response; Chemical, Biological, Radiological and Nuclear Countermeasures; and Information Analysis and Infrastructure Protection.[4]
- The Pentagon has established a new unified command, called the Northern Command (NORTHCOM), for homeland defense. On April 17, 2002, the command was assigned the mission of defending the United States and supporting the full range of military assistance to civil authorities. NORTHCOM began operations on Oct. 1, 2002. However, questions such as what the relationship is between NORTHCOM, the OHS, the Homeland Security Council and the new Department of Homeland Security, remain unanswered.
- In the wake of the Aum Shinrikyo Tokyo nerve gas subway attack in 1995, several U.S. initiatives were undertaken. The Marine Corps created a new Chemical and Biological Incident Response Force, and the Office of Emergency Preparedness within the HHS developed the Metropolitan Medical Response System. Starting in 1998, the DoD created Rapid Assessment and Initial Detection Teams (later renamed Weapons of Mass Destruction Civil Support Teams). Congress created a new domestic preparedness program whose aim is to train first responders in 157 cities.
- Major responsibility for consequence management of a terrorist attack in the United States now rests with the Federal Emergency Management Agency (FEMA). FEMA created the Office of National Preparedness to coordinate all federal programs dealing with WMD consequence management.
- A new effort is the Bush administration's Customs-Trade Partnership Against Terrorism. U.S. companies that agree to impose tougher anti-terrorist safeguards will be rewarded with faster processing times at U.S. borders. The companies, deemed low-risk shippers, agreed to install point-of-origin-to-point-of-delivery security in return for expedited border handling of their imports and exports by the Customs Service.

- In 2001, Congress created a new Transportation Security Administration (TSA) within the Department of Transportation. The TSA is responsible for creating a new federal airport security force, an expanded Federal Air Marshal program, deployment and creation of new screening technologies, administrative and support staff, and high-tech researchers, as well as a host of other new improvements in aviation and transportation security.
- Coast Guard Port Security Units are patrolling "keep-out" zones around Navy warships and key facilities, including nuclear power plants. The Coast Guard also has changed the 24-hour Notice of Arrival requirement for ships entering U.S. ports to 96 hours before arrival at the first U.S. port. The notice requires a list of the crew and a cargo manifest from every incoming ship so that the Coast Guard can bounce that list off many law enforcement databases.
- To deal with container shipping, the Customs Service has proposed a "Container Security Initiative" that would establish security criteria for identifying high-risk containers, use technology to prescreen those containers, and develop and use smart and secure containers. The initiative would expedite the processing of containers prescreened at mega-ports overseas that participate in the initiative.
- The United States is seeking approval from the International Maritime Organization (IMO) for the Customs-Trade Partnership Against Terrorism, which would give U.S. inspectors authority to inspect cargo containers at their points of origin in foreign countries.
- The NRC issued a mandatory security upgrade order announcing new security measures to shield the nation's 104 nuclear power plants from terrorist attack.
- The FAA, in partnership with private technology companies, is developing an air security screening system designed to use data-mining and predictive software to profile passenger activity and intuit obscure clues about potential threats even before the scheduled day of flight.
- The federal Nuclear Emergency Search Team, one of the Energy Department's seven major radiological emergency response units, has been ordered to launch periodic searches for a "dirty bomb" in Washington and other large U.S. cities.

- The NRC has created a new Office of Nuclear Security and Incident Response that will work with the OHS to protect U.S. nuclear power plants from terrorist attack
- The HHS has contracted with British-based Acambis PLC for 209 million doses of smallpox vaccine by the end of 2002. This will supplement the 15 million doses of vaccine currently available in the stockpile. It is also possible that the stockpile can be increased through dilution. In addition, Aventis Pasteur, a French vaccine maker has agreed to make available to the United States more than 75 million doses of vaccine made in its factories more than 40 years ago. According to HHS, America will have at least 286 million doses of vaccine by year's end. The figure could be as high as 711 million doses, depending on how well the Aventis vaccine can be diluted. Depending on the estimates, these quantities should be sufficient to vaccinate most Americans.
- The U.S. Centers for Disease Control and Prevention (CDC) will distribute $918 million to state health departments for bioterrorism preparedness.
- The Plum Island Animal Disease Center in New York is being upgraded by the Agriculture Department, in accordance with a Clinton administration initiative, into the sort of heavily protected laboratory at which the most dangerous animal diseases are studied.
- The Food and Drug Administration (FDA) is improving capabilities to identify and characterize food borne pathogens, and is identifying biological agents using animal studies and microbiological surveillance.

## What Should Be Done?

***Domestic Response Recommendations***

- Develop future years plans and coordinated program budgets. Each federal department and agency with a homeland security mission should develop five-year plans and long-term research, development, testing and evaluation plans.
- Congress should establish a homeland security working group. This group should be chaired and vice-chaired by members of the majority and minority parties, respectively, and include senior staff from the various authorizing and appropriations committees with jurisdiction over federal agencies concerned with terrorism, crisis, consequence management and

homeland defense. By means of a monthly report, the working group would keep the authorizing and appropriations committees apprised of ongoing legislative initiatives and funding issues in Congress.

- The Justice Department should fully fund the National Defense Preparedness Office clearinghouse for information on planning and policy regarding WMD preparedness.
- The Justice Department should fund its Center for Domestic Preparedness at Anniston, Ala., to allow it to achieve full capacity of 10,000 trainees a year. Also, HHS should continue to fund the U.S. Public Health Service's Noble Training Facility at the same location.
- The Justice Department should coordinate with the U.S. Army Chemical School at Fort Leonard Wood, Mo., to share training techniques and lessons learned on dealing with chemical and biological devices and defense operations.
- The Justice Department should increase training and exercising of state and local emergency responders. The department should expand Nunn-Lugar-Domenici training, which was established by the Defense Against Weapons of Mass Destruction Act of 1996. It is known as the Nunn-Lugar-Domenici program after its Senate sponsors, which stipulated the training of first responders to deal with WMD terrorist incidents. It began in fiscal year 1997 (FY 97) to train first responders — fire, police and emergency medical technicians — in 120 of the largest cities (later increased to 157 cities and counties in the country), and to exercise for additional state and local jurisdictions, broaden the range of participants (i.e., public health, environmental health and human services personnel), and provide funding for the purchase of equipment — all with an eye toward standardizing training and equipment for interoperability across jurisdictions. The program should also develop measures for judging the effectiveness of the training.
- Each state should harmonize state and local emergency preparedness plans and equipment. Harmonization raises the preparedness levels of laggard state and local jurisdictions, facilitates interoperability, and then promotes greater economies of scale with respect to purchasing personal protective equipment.
- The future Department of Homeland Security should integrate emergency responders into federal planning for domestic response prepared-

ness. Emergency responders must have an effective seat at the intergovernmental table to ensure seamless coordination between emergency responders and late-arriving federal assets.

- The Justice Department should identify and remedy legal ambiguities or inadequate authority. An interagency task force, with state and local representation, should immediately begin efforts to identify legal issues raised by a WMD threat or attack and work to resolve those issues, whether through proposing new laws or simply clarifying the application of existing laws and authorities.

***Communications Recommendations***

- The Federal Communications Commission (FCC) should establish regulations governing the upgrade of public safety voice and data communications networks to ensure regional compatibility and interoperability.
- Congress should fund a nationwide system of regional voices and data communications systems for state and local government use.
- The FCC should disseminate information concerning recent orders that set aside portions of the electromagnetic spectrum for public-safety use.
- The FCC Homeland Security Policy Council should develop a system to prioritize cellular traffic.
- The OHS needs to promote the sharing of homeland security information — including classified information — between federal intelligence, law enforcement agencies, and state and local entities.

***Border Recommendations***

- The government should codify the border security arrangement the United States has made with Canada and Mexico into formal treaties allowing enforcement activities across international borders.
- The Immigration and Naturalization Service (INS) should tie applications for student visas and green cards to Interpol and other law enforcement databases.
- The INS should expel students attending U.S. colleges and universities on student visas from the United States within 180 days if they are not actively enrolled in courses.
- The INS should automate immigration databases to include biometric identification and maintain information as to the whereabouts and activities of foreign nationals in the United States.

***Aviation Recommendations***

- The FAA should link airline ticketing systems and databases to law enforcement information systems to prevent wanted and suspect individuals from obtaining tickets for airline flights.
- Similarly, the FAA should link federal watch lists to airline ticketing systems and these systems should be updated to flag any record containing obvious warning signs, including cash transactions, absence of luggage, unusual passports or visas, recorded reports of odd behavior, and past histories of security issues.
- Congress should require the FAA to revise its plan to deploy computerized tomograph X-ray screening devices in airports because of their limitations. Instead, the FAA should install combinations of computerized tomograph X-ray, baggage X-ray, and explosive trace detection machines to achieve 100 percent screening of checked baggage with acceptable throughput to meet airline scheduling needs.
- The FAA should require bag matching on all legs of all flights.
- The TSA, the FAA, and the airlines should develop and implement a "trusted flyer" program for frequent flyers that incorporates background checks, fingerprinting, and biometric identification to allow more limited screening of these persons at airport check-in and check points.
- The appropriate agencies should revise computerized passenger profiling systems to include ethnic and national-origin factors with respect to passengers from countries known to support terrorism.

***Mass Transit Recommendations***

- The Transportation Department should develop a regulatory system that can reliably identify legitimate transportation activity by truck and rail to allow closer inspection and regulation of activity deemed otherwise by exception.
- The Transportation Department should require satellite tracking of hazardous materials shipments by carriers.
- The Transportation Department should require all truck and rail shippers to submit route plans, driver links with personal identification numbers and cargo identification, and configure these systems to report by exception those loads that deviate significantly from their route plan. Deviations should be immediately reported to the appropriate law enforcement agency.

- The Transportation Department should first require such identification and tracking regulations for shipments of hazardous materials; second, on shipments of non-hazardous materials; and third, on commercial rental fleets.
- The Transportation Department should identify and monitor key bridges, tunnels and transit infrastructures in terms of hazardous materials traffic on or through them. Hazardous materials should not be allowed in, on, or near these structures.
- The Transportation Department should re-evaluate passenger rail security taking into account current and future threats.

***Maritime Security Recommendations***

- The Coast Guard and Transportation Department should immediately assess the equipment and staffing needed to protect U.S. harbors and the shipping vessels using them.
- The Coast Guard should monitor activities in major seaports, particularly those handling hazardous cargos and military vessels in a manner similar to that described above for the trucking industry.
- The U.S. delegate to the IMO should encourage it to push up the date for implementation of its forthcoming new security regulations.
- The Transportation Department should work with the IMO to require full transparency of identity, ownership and financial responsibilities of all ship owners.

***Nuclear Recommendations***

- In the long term, as recommended by the International Atomic Energy Agency, Congress should require the incorporation of built-in measures and external controls in future nuclear reactors, thus making diversion of nuclear materials more difficult
- Congress should reverse the past policy of the NRC, which has been systematically backing away from rigorous enforcement of nuclear power plant design requirements, to take into account the new sophisticated terrorist threat and ensure that these requirements, known as the Design Basis Threat, are fully implemented for all nuclear reactors.
- Because private industry cannot be relied on to make the necessary investments, the new Department of Homeland Security should enforce

all security measures at all nuclear power plants, as is being done for security at airports.

- The United States should reaffirm the importance of the 1972 nuclear Non-Proliferation Treaty. As part of this reaffirmation, the United States needs to reduce reliance on nuclear deterrence in its security policies and make dramatic cuts in the number of its nuclear weapons. Continued reliance on a nuclear threat and large nuclear arsenals undermines U.S. efforts to stem weapons proliferation.
- The United States should work closely with the International Atomic Energy Agency and other nations to increase physical safeguards of nuclear plants and materials around the world.
- The United States should forge a global coalition to secure WMD stockpiles and their essential ingredients everywhere; appoint one U.S. and one Russian official to lead their respective efforts to secure nuclear weapons and materials; strengthen security upgrades for warheads and materials in Russia; launch an effort to eliminate or secure stockpiles of weapons-usable nuclear material worldwide; create a stringent global nuclear security standard; accelerate the blend-down of highly enriched uranium; and create new revenue streams for nuclear security.[5]
- The U.S. government, working though the Department of Energy and DoD, should undertake an internal evaluation of its bilateral Materials Protection, Control, and Accounting program in Russia and consider ways to accelerate progress in safeguarding nuclear weapons and special nuclear materials, especially to counter potential insider threats.
- Future U.S. proliferation resistance measures should include: nuclear energy systems designed to use fuel where weapon-grade material cannot be easily removed, such as a pebble-bed reactor; systems that do not use highly enriched uranium; systems that produce the lowest possible amounts of plutonium-239; combinations of nuclear energy systems in which spent fuel from one can be used as fuel for another; and improved enrichment and reprocessing abilities to prevent stockpiling of weapon-grade material.
- The Department of Homeland Security should ensure that U.S. states with a population within the emergency planning zone of commercial nuclear power plants include sufficient stocks of potassium iodide as a protective measure for the general public in the event of a severe plant incident.

- Research, funding and deployment of sensors designed to detect radioactive materials need acceleration.
- The NRC and states with agreements with that agency should tighten regulations for obtaining and possessing radiological sources that could be used in terrorist attacks including requirements for securing and tracking these sources. Additionally, licensees possessing large sources should be encouraged to substitute nonradioactive sources when economically feasible.

***Chemical Attacks Recommendations***

- The United States should work to ensure that the Organization for the Prohibition of Chemical Weapons, the organization monitoring compliance with the Chemical Weapons Convention, has the money and political support to do its job.
- The Environmental Protection Agency (EPA) should require industry to reduce or eliminate the possibility of a chemical release by choosing inherently safer materials and technologies.
- The EPA should require industry to conduct background checks of key employees.
- The Transportation Department should enhance physical security of barge terminals, rail, and truck facilities and their staging areas that handle chemicals.
- The Transportation Department should prohibit rail cars with toxic cargo from parking by residential areas.
- The HHS should develop incentives for hospitals to be ambulance-receiving hospitals, to stockpile nerve-agent antidotes and selected antitoxins and put them in the hands of first responders, to purchase appropriate personal protective equipment and expandable decontamination facilities and train emergency department personnel in their use.
- The HHS should survey major metropolitan hospitals regarding supplies of antidotes, drugs, ventilators, personal protective equipment, decontamination capacity, mass-casualty planning and training, isolation rooms for infectious disease, and familiarity of staff with the effects and treatment of chemical weapons.

***Biological Weapons Recommendations***

- The Bush administration should take steps to enhance the public health infrastructure to include improved access to information technologies and the Internet, as well as additional staffing.
- The HHS, along with the CDC and the state departments of health, should establish and maintain a national epidemiological tracking system that employs both nontraditional and syndromatic surveillance technology. The system should include data from emergency department visits, 911 centers and health clinics, and should track the sale of antibiotics and other relevant medications.
- FEMA and CDC should develop a national response capacity for rapid assessment of a bioterrorist emergency occurring anywhere in the United States. These agencies should develop a Biological Emergency Support Team that can rapidly assess and set priorities following a bioterrorist event. This will ensure that FEMA can rapidly galvanize other federal departments around a common assessment and set out response priorities during a national emergency. Furthermore, this arrangement links state and local infectious disease control agencies through CDC to the disaster management skills of FEMA.
- The Bush administration should move to expand CDC's national bioterrorism laboratory response network and laboratory standardization efforts. This multidepartment initiative should act as a nationwide coordinated laboratory network for bioterrorism, and should include the DoD, FBI, HHS, and the departments of Energy and Agriculture.
- The federal government should increase funding for CDC's Bioterrorism Preparedness and Response Program, including the hiring of new lab analysts.
- FEMA should expand the provisions on bioterrorism in the Terrorism Annex of the Federal Response Plan.
- The HHS should strengthen and make more widely available epidemiological training programs, with curricula appropriate for public health and law enforcement professionals.
- The HHS should purchase, deploy and maintain baseline stocks of pharmaceuticals, vaccines and antidotes in the 30 largest cities in the United States, and in strategic locations in all 50 states.

- The FBI should require registration of university labs and research facilities working with known or suspected chemical or biological agents.
- The HHS should establish a National Vaccine Authority to oversee research, development and distribution of vaccines that are too risky or too unprofitable for industry to make. A central component would be a government-owned, contractor-operated vaccine-manufacturing plant.
- The DoD and HHS should sponsor an integrated plan for biomedical research. Civilian and military research efforts should dovetail, and applied research should not be forsaken in favor of long-term bench research projects.
- Congress should fill in the gaps in current law with respect to criminalization of possession of biological pathogens and improvement of security at U.S. labs. Such measures could include:
  - Requiring individuals to report their possession of biological agents to the designated agency, with failure to report resulting in a criminal or civil penalty.
  - Prohibiting the transfer of biological agents to a person who is not registered.
  - Requiring certain security clearance to work with certain agents.
- The U.S. government should prevent proliferation of former Soviet biological weapon capabilities by increasing funding for the State Department's science centers (International Science and Technology Center, and the Science and Technology Center in Ukraine) and the Redirection of Biotechnical Scientists Program; the Department of Energy Initiatives for Proliferation Prevention Program; and the DoD Biological Weapons Proliferation Prevention Program.

***Agroterrorism Recommendations***

- The U.S. Department of Agriculture should establish a veterinary "push-pack" where key pharmaceuticals necessary to react to a variety of livestock and plant diseases are pre-positioned in strategic locations, similar to that established by the CDC for human diseases.
- The Agriculture Department should set up a biosecurity training program to counter the threat of diseases and pests at the farm level.
- The Agriculture Department should devote more resources to disease detection, surveillance and diagnostic technologies including creating linked

animal-human disease databases, developing more rapid diagnostic tests, increasing capacities at the Plum Island laboratory, and establishing a contingency network of veterinarians that could respond to emergencies.
- The Agriculture Department should establish a program of security assessment and detection for food-processing facilities.
- The Agriculture Department, FDA and CDC should link their disease monitoring databases and jointly develop surveillance systems that use this combined data to improve early warning systems.

***Biological Arms Control Recommendations***

The Biological and Toxin Weapons Convention (BWC), which bans the development, production, stockpiling, and biological and toxin weapons transfer, has been hobbled since it took effect in 1975 by a lack of formal measures to monitor and enforce compliance. The United States should rethink its rejection to the BWC's verification protocol and undertake the following measures:

- The United States should pass integrated legislation that addresses national implementation of the BWC. This is in accordance with Article IV of the BWC which requires that "each State Party shall, in accordance with its constitutional processes, take any necessary measures to prohibit and prevent the development, production, stockpiling, acquisition or retention of the agents, toxins, weapons, equipment and means of delivery specified in article I of the Convention, within the territory of such State, under its jurisdiction or under its control anywhere."
- The United States should support the establishment of a BWC oversight committee and secretariat to promote adherence to the BWC and to aid implementation of politically binding confidence-building measures for information exchange. Moreover, it should develop a legal framework to ensure that breeches of the BWC by individuals or groups are treated as an international crime.
- Continue the biological weapons verification protocol negotiations, utilizing the existing draft as the basis for talks.

***Ballistic Missiles Recommendations***

- The Pentagon's Missile Defense Agency should reorient the missile defense development program to focus its near-term efforts on short-range theater missile defense systems.

- Congress should eliminate space-based missile defense funding, and prohibit the development of nuclear-tipped interceptors. Congress also should cut Missile Defense Agency funding by approximately 50 percent, from nearly $8 billion in the FY 03 request to $4 billion, and shift those funds into Cooperative Threat Reduction programs.
- Congress should redirect the funds aimed at the planned missile defense test bed and interceptor deployment facilities in Fort Greely, Alaska, to intelligence efforts to find, monitor, and potentially target with conventional weapons both ICBM launch facilities and WMD facilities of concern.

***Cruise Missiles Recommendations***

The U.S. government should move, both unilaterally and with partner nations, to strengthen the Missile Technology Control Regime (MTCR), an existing voluntary multilateral arrangement, by:

- Creating a uniform set of ground rules for determining the range and payload of cruise missiles and unmanned aerial vehicles;
- Implementing tighter controls on stealthy cruise missiles;
- Examining and implementing tighter controls on countermeasure technologies specially designed to enhance cruise missile penetration; and
- Broadening current MTCR parameters governing controls on jet engines.

***Water Supplies Recommendations***

The Information Analysis and Infrastructure Protection division of the new Department of Homeland Security should require all facilities to comply with the following standards:

- All facilities (treatment plants, reservoirs, reservoir dams, water storage facilities and towers, pumping stations, water intake facilities, chlorine booster stations, and meter and valve boxes) should be fenced, well lighted, and monitored by surveillance cameras and motion detectors. All gates should be locked and barricades set up to stop trucks from running through them. Landscaped berms should surround reservoirs and storage facilities, with an approach slope greater than what a truck could negotiate.
- To prevent hacking, supervisory control and data acquisition systems should not be connected to the Internet. Remaining cyber-security should be enhanced, and passwords should be changed regularly.

- Fire hydrants and other entry points to the distribution system should be tamperproof. Surveillance cameras should be located onsite at key points, such as chlorine storage facilities, chlorine injection areas, filter beds, hazardous chemical and fuel storage areas, and finished water storage areas.
- Redundancy should be built into all systems.
- All sites should have a backup power source or a generator available.
- Good communication and coordination among neighboring water utilities is needed. Valve cross-connections should be established. If one facility goes down the other could be used as a backup.
- All reservoir and tank-access panels and vents should be tamperproof.
- The public should be sensitized to watching for and reporting suspicious vehicles and people near water facilities, especially in remote locations.
- There should be good communication and coordination with local police and fire departments. Police units should make mandatory stops at water facilities (treatment plants, reservoirs, reservoir dams, water storage facilities and towers, pumping stations, water intake facilities, and meter and valve boxes) during their beats at random intervals.
- Finished water reservoirs should be covered.
- There should be one-way valves installed at strategic points in the distribution system to prevent backflow.
- Additional testing and monitoring of chemical agents delivered to the plant should be conducted to make sure that the contents are as indicated on the label.
- Filtration and disinfection should be enhanced as much as possible to remove bacterial agents. Reducing turbidity levels will increase the removal of microbial and chemical agents.
- Continuous monitoring for various contaminants in the influent and in the distribution system should be conducted for various agents. Israel has developed sensitive real-time water quality monitoring devices to test for various chemical and biological agents.
- The chlorine delivery schedule should be known, and there should be a clear line of communication with the supplier to discuss changes in the schedule. Chlorine containers should be stored in secure, clean, ventilated, fire-resistant, sheltered areas away from other chemicals. Chlorine storage facilities should be inspected regularly. Police and fire departments should be aware of the location of chlorine storage so that they can respond appropriately in an emergency.

- Alarm levels that trigger an investigative or emergency response should be established for all monitored parameters.
- Pressure changes within the distribution system should be monitored for abnormalities. Also, agencies should monitor water quality for significant changes at raw water intakes, distribution system entry points, finished water storage reservoirs and key monitoring locations within the distribution system.
- Conduct an inventory of wastewater and storm-water infrastructure, evaluating their position relative to sensitive locations, to see if it represents a security risk.
- Tamperproof manholes and sensors should be installed in sewer and storm-sewer lines in sensitive areas.

## Conclusions

Clearly, in a world where the number of threats is almost unlimited, prioritization is vital. One cannot defend perfectly against every possible threat, but it is feasible to strengthen existing defenses and create new ones, thereby making the most deadly type of attacks less likely. Though much more needs to be done, improved homeland security is possible.

Given that a determined attacker will be able to penetrate homeland defenses to some degree, it is clear that consequence management programs must be strengthened. However, preventive activities tend to lower the overall level of risk, even without advance knowledge of what the targets are, and should rank high on any policymaker's list of priorities. Thus, efforts to extend the nation's safety perimeter outward by improved border controls and cooperative agreements with other nations on land- and sea-based trade deserve support and funding.

Similarly, the United States should take advantage of its considerable competitive advantages in information technology by linking together its numerous public and private databases for data-mining and analysis.

In terms of specific vulnerabilities to concentrate on, those representing the greatest threats in terms of potential casualties, economic losses and the U.S. way of life are **mass transit, maritime security, radiological threats, bioterrorism,** and **attacks against chemical plants.** Policymakers and Congress should put measures to prevent such attacks at the top of their agenda with regards to new security measures and spending.

## Endnotes

1 Eunice Moscoso, "Small Planes Posing Big Terrorism Threat: Security Lax at Thousands of Airfields," *The Atlanta Journal Constitution*, June 2, 2002, p. B8; and Greg Schneider, "Private Plane Charters: One Way Around Air Security," *The Washington Post*, June 2, 2002, p. 1.

2 In regard to the vulnerability of the pipeline and terminus facility see "FBI Practices Protection of Oil Pipeline," *Fairbanks Daily News-Miner*, June 6, 2002. <http://www.news-miner.com/Stories/0,1413,113~7249~656677,00.html>

3 James L. Ford, *Radiological Dispersal Devices: Assessing the Transnational Threat*, Strategic Forum No. 136, March 1998, Institute for National Strategic Studies, National Defense University. <http://www.ndu.edu/inss/strforum/forum136.html>

Almost any radioactive material can be used to construct a radiological dispersal device, including fission products, spent fuel from nuclear reactors, and relatively low-level materials, such as medical, industrial and research waste. Weapons-grade materials (highly enriched uranium or plutonium) are not needed, although they could be used. A radiological dispersal device is designed to scatter radioactive debris over a wide area, thereby contaminating it and possibly causing casualties through radiation sickness, as well as denying its use to military forces or others for some period of time. The radiological dispersal device threat is threefold: the blast and fragmentation effects from the conventional explosive, the radiation exposure from the radioactive material used, and the fear and panic that its use would spread among the target group or population.

4 See White House News Release, "President to Propose Department of Homeland Security," June 6, 2002. <http://www.whitehouse.gov/news/releases/2002/06/20020606.html>. For detail see Department of Homeland Security portal page.

5 For detail on these recommendations see *Securing Nuclear Weapons and Materials*.

## ACRONYMS

| | |
|---|---|
| **BWC** | Biological and Toxic Weapons Convention |
| **CBO** | Congressional Budget Office |
| **CDC** | Centers for Disease Control and Prevention |
| **DoD** | Department of Defense |
| **EPA** | Environmental Protection Agency |
| **FAA** | Federal Aviation Administration |
| **FCC** | Federal Communications Commission |
| **FDA** | Food and Drug Administration |
| **FEMA** | Federal Emergency Management Agency |
| **HHS** | Health and Human Services Department |
| **ICBM(s)** | intercontinental ballistic missile(s) |
| **IMO** | International Maritime Organization |
| **INS** | Immigration and Naturalization Service |
| **MTCR** | Missile Technology Control Regime |
| **NORTHCOM** | Northern Command |
| **NRC** | Nuclear Regulatory Commission |
| **NSC** | National Security Council |
| **OHS** | Office of Homeland Security |
| **PDD** | Presidential Decision Directives |
| **TSA** | Transportation Security Administration |
| **WMD** | weapons of mass destruction |

CENTER FOR DEFENSE INFORMATION
1779 Massachusetts Avenue, NW
Washington, DC 20036
202.332.0600 · Fax 202.462.4559
www.cdi.org