107th Congress
1st Session

COMMITTEE PRINT

S. PRT.
107–43

STRATEGIES FOR HOMELAND DEFENSE

A COMPILATION

BY THE

COMMITTEE ON FOREIGN RELATIONS
UNITED STATES SENATE

Joseph R. Biden, Jr., Chairman

SEPTEMBER 26, 2001

Available via the World Wide Web: http://www.access.gpo.gov/congress/senate

Printed for the use of the Committee on Foreign Relations

U.S. GOVERNMENT PRINTING OFFICE
75–249 CC WASHINGTON : 2001

CONTENTS

LETTER OF TRANSMITTAL

UNITED STATES SENATE,
COMMITTEE ON FOREIGN RELATIONS,
Washington, DC, September 26, 2001.

DEAR COLLEAGUE:

The tragic and unconscionable attacks of September 11 have awakened all Americans to the very real threat posed by international terrorism. As Congress works to ensure that the awful events of September 11th will never be repeated, it is instructive for us to review several recent studies of the issue. In recent years, a number of major commissions and distinguished witnesses before Congress have highlighted the emergence of both nation-states and sub-national groups with the desire and the capability to employ asymmetric means, including weapons of mass destruction, to strike at the United States homeland. Their reports and statements have underscored the real vulnerability of the United States in responding to such attacks and mitigating their consequences.

The Committee on Foreign Relations has reprinted the executive summaries and key excerpts from some of the leading reports on emerging threats to U.S. national security. For your benefit, I include a brief summary of each of the six reports included in this Committee reprint:

I. THE NATIONAL COMMISSION ON TERRORISM (JUNE 2000)

The final report of the National Commission on Terrorism, chaired by L. Paul Bremer III, declares in no uncertain terms, "Today's terrorists seek to *inflict mass casualties,* and they are attempting to do so both overseas and on American soil. They are less dependent on state sponsorship and are, instead, forming loose, transnational affiliations based on religious or ideological affinity and a common hatred of the United States."

The National Commission urged the U.S. intelligence and law enforcement communities to use the full scope of their authorities to collect information regarding terrorist plans and attack. Some of the specific measures suggested, including loosened restrictions on CIA recruitment methods and expanded electronic surveillance capabilities, are now being considered in the current environment. It encouraged the United States to firmly target all states that support terrorists through diplomatic, financial, economic, and military means, including the imposition of sanctions on states not fully cooperative with counter-terrorism efforts.

II. THE U.S. COMMISSION ON NATIONAL SECURITY/21ST CENTURY: EXCERPT ON HOMELAND DEFENSE (FEBRUARY 2001)

This commission, known as "Hart-Rudman" after its co-chairs, former Senators Gary Hart and Warren Rudman, concluded that "attacks against American citizens, possibly causing heavy casualties, are likely over the next quarter century." Citing a growing diffusion of technology and an abundance of actors with grievances against the United States, the Hart-Rudman commission urged making the security of the American homeland *the primary national security mission of the U.S. government.*

To begin carrying out this mission, the commission recommends creation of a *National Homeland Security Agency* to coordinate all U.S. government activities on homeland defense. The commission urges the United States to rely on three main instruments in deterring and defending against threats to the homeland: (1) diplomacy, (2) the overseas U.S. diplomatic, intelligence, and military presence, and (3) vigilant border security and surveillance.

III. A REPORT CARD ON THE DEPARTMENT OF ENERGY'S NON-PROLIFERATION PROGRAMS WITH RUSSIA ("BAKER-CUTLER TASK FORCE") (JANUARY 2001)

This bipartisan task force called on the President to quickly formulate a strategic plan to secure and/or neutralize in the next eight to ten years *all nuclear weapons-usable material located in Russia.* To carry out this goal, the task force suggested that the U.S. government set aside approximately *$30 billion* over the next eight to ten years.

Co-chaired by former U.S. Senator Howard Baker and former White House Counsel Lloyd Cutler, the task force declared that *the most urgent threat facing the United States* is the danger that weapons of mass destruction or weapons-usable material, i.e., plutonium and highly enriched uranium, could be stolen and sold to terrorists or hostile nation-states. The task force concluded that current U.S. government efforts, including the Nunn-Lugar programs and the Department of Energy nuclear non-proliferation programs, were on the right track but were insufficient to meet the enormity of this threat.

IV. STATEMENTS BY FORMER SENATOR SAM NUNN AND DR. D.A. HENDERSON BEFORE THE SENATE COMMITTEE ON FOREIGN RELATIONS ON "THE THREAT OF BIOTERRORISM AND THE NATURAL SPREAD OF INFECTIOUS DISEASES" (SEPTEMBER 2001)

According to Senator Nunn, "*Biological terrorism is one of our greatest national security threats,* and one that cannot be addressed by Department of Defense standard operating procedures." Both he and Dr. D.A. Henderson, an architect of the global campaign to eradicate smallpox more than twenty years ago, testified before the Committee on Foreign Relations earlier this month on their participation in "Dark Winter," a recent exercise simulating the U.S. government's response to a smallpox attack on three American cities.

Senator Nunn and Dr. Henderson drew a number of lessons from the Dark Winter exercise. First, the measures we can take to deter or prevent bioterrorism are cost effective measures in countering natural epidemics. Second, the United States must recognize the central role of public health and medicine and seek to recapitalize our medical infrastructure. These efforts should include an adequate surge capability to handle emergencies and a strong surveillance and monitoring network, both domestic and international, to detect, track, and contain epidemics and provide evidence of biological weapons attacks. Third, we should build our national pharmaceutical stockpile to capacity, including extra production capability for drugs and vaccines, and increase funding for biomedical research to develop new medicines and diagnostic tests.

V. Crowe Report on Embassy Security (January 1999)

The Crowe Report called for the appropriation of $1.4 billion per year over ten years to fund capital building programs, security operations, and personnel to ensure maximum security at U.S. embassies around the world. The final report of the Department of State Accountability Review Boards, better known as the Crowe Report after the former Chairman of the Joint Chiefs of Staff William J. Crowe, examined the August 1998 bombings of the U.S. Embassies in Kenya and Tanzania. It criticized the State Department for an "institutional failure" in not fully recognizing the threat posed by transnational terrorism and the particular use of large car bombs.

VI. The Gilmore Commission: Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (December 1999 and December 2000)

The so-called "Gilmore Commission," named for its chair, Virginia Governor James Gilmore III, recognized terrorism employing weapons of mass destruction as a *serious threat to homeland defense and focused on the need to improve domestic capabilities in responding to such attacks.* The Gilmore Commission called upon the U.S. government to develop a viable strategy on national domestic preparedness plans to combat terrorism. To carry out this national strategy, the Commission recommends that the President should establish a National Office for Combating Terrorism in the Executive Office of the President. The director of this office, a Senate-confirmed appointee, would exercise program and budget authority over all federal efforts to fight terrorism.

Certainly, we should not rush to adopt all of these recommendations; some of these proposals, under closer scrutiny, may not advance our objectives in the war on terrorism. But it is my hope that these reports will help frame our debate on comprehensive legislation to counter terrorism and other emerging threats to U.S. national security in coming weeks and months. I welcome the chance to speak in further detail with each of you on these critical issues.

Sincerely,

Joseph R. Biden, Jr., *Chairman.*

COUNTERING THE CHANGING THREAT OF INTERNATIONAL TERRORISM

REPORT OF THE NATIONAL COMMISSION ON TERRORISM

JUNE 5, 2000

COMMISSION MEMBERS AND STAFF

COMMISSIONERS

L. Paul Bremer III, Chairman, is the Managing Director of Kissinger Associates. During a 23-year career in the American diplomatic service, Ambassador Bremer served in Asia, Africa, Europe and Washington, D.C. He was Ambassador to the Netherlands from 1983 to 1986. From 1986-1989, he served as Ambassador-at-large for Counter-Terrorism, where he was responsible for developing and implementing America's global polices to combat terrorism.

Maurice Sonnenberg, Vice Chairman, is the senior international advisor to the investment banking firm of Bear, Stearns & Co. Inc. and the senior international advisor to the law firm of Manatt, Phelps & Phillips, LLP. He is a member of the President's Foreign Intelligence Advisory Board. He recently served as a member of the U.S. Commission on Reducing and Protecting Government Secrecy and as the senior advisor to the U.S. Commission on the Roles and Capabilities of the U.S. Intelligence Community.

Richard K. Betts is Leo A. Shifrin Professor of War and Peace Studies in the political science department, Director of the Institute of War and Peace Studies, and Director of the International Security Policy program in the School of International and Public Affairs at Columbia University. He is also Director of National Security Studies and Senior Fellow at the Council on Foreign Relations, and author of *Surprise Attack: Lesson for Defense Planning.*

Wayne A. Downing, General, U.S. Army, retired in 1996 after a 34-year career, where he served in a variety of command assignments in infantry, armored, special operations and joint units culminating in his appointment as the Commander-in-Chtef of the U.S. Special Operations Command. Since retirement, he was appointed to assess the 1996 terrorist attack on the U.S. base at Khobar Towers, Saudi Arabia, and to make recommendations to protect people and facilities world wide from terrorist attack. General Downing serves on several boards and panels in both the private and government sectors.

Jane Harmon just completed a year as Regents Professor at U.C.L.A. where she taught at the Department of Political Science and Center for International Relations. Harmon represented California's 36th Congressional District from 1992-1998 where she served on the National Security, Science and Intelligence Committees. Prior government experience includes

Senate Counsel, White House Deputy Cabinet Secretary and DoD Special Counsel. Harmon is currently seeking election to her former seat.

Fred C. Iklé is a Distinguished Scholar, Center for Strategic and International Studies. Dr. Iklé is Chairman of the Board of Telos Corporation and a Director of the Zurich-American Insurance Companies and of CMC Energy Services. Prior to joining the Center, Dr. Iklé served as Undersecretary of Defense for Policy and Director for the U.S. Arms Control and Disarmament Agency.

Juliette N. Kayyem is an Associate of the Executive Session on Domestic Preparedness, John F. Kennedy School of Government, Harvard University. She writes and teaches courses on counter-terrorism policy and the law. Ms. Kayyem has most recently served as a legal advisor to the Attorney General at the U.S. Department of Justice and as Counsel to the Assistant Attorney General for Civil Rights.

John F. Lewis, Jr. is Director of Global Security for Goldman, Sachs & Co., New York. Previously, he was Assistant Director-in-Charge of the National Security Division of the Federal Bureau of Investigation. Mr. Lewis managed the FBI's national counterintelligence and counterterrorism programs. Mr. Lewis has held a variety of positions, including an appointment as Director of Intelligence and CI Programs, National Security Staff and previous Chairman of the International Association of Chiefs of Police Committee on Terrorism.

Gardner Peckham is Managing Director of the government relations firm of Block, Kelly, Scruggs & Healey with a practice focused on international trade, defense and foreign policy issues. Prior to joining the firm, Mr. Peckham served as Senior Policy Advisor to the Speaker of the United States House of Representatives. He also held several other senior positions in Congress and during the Bush Administration served as Deputy Assistant Secretary for Legislative Affairs at the U.S. Department of State and Director for Legislative Affairs at the National Security Council Staff.

R. James Woolsey is a partner at the law firm of Shea & Gardner with a practice in the fields of civil litigation, alternative dispute resolution, and corporate transactions; he also serves on several corporate boards. Previous to returning to the firm, Mr. Woolsey served as Director of Central Intelligence. His U.S. Government service includes Ambassador to the Negotiations on CFE, Under Secretary of the Navy, and General Counsel of the U.S. Senate Committee on Armed Services. He has served on many Presidential and Congressional delegations, boards, and commissions.

EXECUTIVE SUMMARY

International terrorism poses an increasingly dangerous and difficult threat to America. This was underscored by the December 1999 arrests in Jordan and at the U.S./Canadian border of foreign nationals who were allgedly planning to attack crowded millennium celebrations. Today's terrorists seek to inflict mass casualties, and they are attempting to do so both overseas and on American soil. They are less dependent on state sponsorship and are, instead, forming loose, transnational affiliations based on religious or ideological affinity and a common hatred of the United States. This makes terrorist attacks more difficult to detect and prevent.

Countering the growing danger of the terrorist threat requires significantly stepping up U.S. efforts. The government must immediately take steps to reinvigorate the collection of intelligence about terrorists' plans, use all available legal avenues to disrupt and prosecute terrorist activities and private sources of support, convince other nations to cease all support for terrorists, and ensure that federal, state, and local officials are prepared for attacks that may result in mass casualties. The Commission has made a number of recommendations to accomplish these objectives:

Priority one is to prevent terrorist attacks. U.S. intelligence and law enforcement communities must use the full scope of their authority to collect intelligence regarding terrorist plans and methods.

- CIA guidelines adopted in 1995 restricting recruitment of unsavory sources should not apply when recruiting counterterrorism sources.
- The Attorney General should ensure that FBI is exercising fully its authority for investigating suspected terrorist groups or individuals, including authority for electronic surveillance.
- Funding for counterterrorism efforts by CIA, NSA, and FBI must be given higher priority to ensure continuation of important operational activity and to close the technology gap that threatens their ability to collect and exploit terrorist communications.
- FBI should establish a cadre of reports officers to distill and disseminate terrorism-related information once it is collected.

U.S. policies must firmly target all states that support terrorists.

- Iran and Syria should be kept on the list of state sponsors until they stop supporting terrorists.
- Afghanistan should be designated a sponsor of terrorism and subjected to all the sanctions applicable to state sponsors.
- The President should impose sanctions on countries that,

while not direct sponsors of terrorism, are nevertheless not cooperating fully on counterterrorism. Candidates for consideration include Pakistan ond Greece.

Private sources of financial and logistical support for terrorists must be subjected to the full force and sweep of U.S. and international laws.

- All relevant agencies should use every available means, including the full array of criminal, civil, and administrative sanctions to block or disrupt nongovernmental sources of support for international terrorism.
- Congress should promptly ratify and implement the International Convention for the Suppression of the Financing of Terrorism to enhance international cooperative efforts.
- Where criminal prosecution is not possible, the Attorney General should vigorously pursue the expulsion of terrorists from the United States through proceedings which protect both the national security interest in safeguarding classified evidence and the right of the accused to challenge that evidence.

A terrorist attack involving a biological agent, deadly chemicals, or nuclear or radiological material, even if it succeeds only partially, could profoundly affect the entire nation. The government must do more to prepare for such an event.

- The President should direct the preparation of a manual to guide the implementation of existing legal authority in the event of a catastrophic terrorist threat or attack. The President and Congress should determine whether additional legal authority is needed to deal with catastrophic terrorism.
- The Department of Defense must have detailed plans for its role in the event of a catastrophic terrorist attack, including criteria for decisions on transfer of command authority to DoD in extraordinary circumstances.
- Senior officials of all government agencies involved in responding to a catastrophic terrorism threat or crisis should be required to participate in national exercises every year to test capabilities and coordination.
- Congress should make it illegal for anyone not properly certified to possess certain critical pathogens and should enact laws to control the transfer of equipment critical to the development or use of biological agents.
- The President should establish a comprehensive and coordinated long-term research and development program for catastrophic terrorism.
- The Secretary of State should press for an international convention to improve multilateral cooperation on preventing or responding to cyber attacks by terrorists.

The President and Congress should reform the system for reviewing and funding departmental counterterrorism programs to ensure that the activities and programs of various agencies are part of a comprehensive plan.

- The executive branch official responsible for coordinating counterterrorism efforts across the government should be given a stronger hand in the budget process.

- Congress should develop mechanisms for a comprehensive review of the President's counterterrorism policy and budget.

THE INTERNATIONAL TERRORISM THREAT IS CHANGING

- Who are the international terrorists?
- What are their motives and how do they get their support?
- How can we stop them?

The answers to these questions have changed significantly over the last 25 years. There are dramatically fewer international terrorist incidents than in the mid-eighties. Many of the groups that targeted America's interests, friends, and allies have disappeared. The Soviet bloc, which once provided support to terrorist groups, no longer exists. Countries that once excused terrorism now condemn it. This changed international attitude has led to 12 United Nations conventions targeting terrorist activity and, more importantly, growing, practical international cooperation.

However, if most of the world's countries are firmer in opposing terrorism, some still support terrorists or use terrorism as an element of state policy. Iran is the clearest case. The Revolutionary Guard Corps and the Ministry of Intelligence and Security carry out terrorist activities and give direction and support to other terrorists. The regimes of Syria, Sudan, and Afghanistan provide funding, refuge, training bases, and weapons to terrorists. Libya continues to provide support to some Palestinian terrorist groups and to harass expatriate dissidents, and North Korea may still provide weapons to terrorists. Cuba provides safehaven to a number of terrorists. Other states allow terrorist groups to operate on their soil or provide support which, while falling short of state sponsorship, nonetheless gives terrorists important assistance.

The terrorist threat is also changing in ways that make it more dangerous and difficult to counter.

International terrorism once threatened Americans only when they were outside the country. Today international terrorists attack us on our own soil. Just before the millennium, an alert U.S. Customs Service official stopped Ahmad Ressam as he attempted to enter the United States from Canada—apparently to conduct a terrorist attack. This fortuitous arrest should not inspire complacency, however. On an average day, over one million people enter the United States legally and thousands more enter illegally. As the World Trade Center bombing demonstrated, we cannot rely solely on existing border controls and procedures to keep foreign terrorists out of the United States.

Terrorist attacks are becoming more lethal. Most terrorist organizations active in the 1970s and 1980s had clear political objectives. They tried to calibrate their attacks to produce just enough bloodshed to get attention for their cause, but not so much as to alienate public support. Groups like the Irish Republican Army and the Palestine Liberation Organization often sought specific political concessions.

Now, a growing percentage of terrorist attacks are designed to kill as many people as possible. In the 1990s a terrorist incident was almost 20 percent more likely to result in death or injury than an incident two decades ago. The World Trade Center bombing in

New York killed six and wounded about 1,000, but the terrorists' goal was to topple the twin towers, killing tens of thousands of people. The thwarted attacks against New York City's infrastructure in 1993—which included plans to bomb the Lincoln and Holland tunnels—also were intended to cause mass casualties. In 1995, Philippine authorities uncovered a terrorist plot to bring down 11 U.S. airliners in Asia. The circumstances surrounding the millennium border arrests of foreign nationals suggest that the suspects planned to target a large group assembled for a New Year's celebration. Overseas attacks against the United States in recent years have followed the same trend. The bombs that destroyed the military barracks in Saudi Arabia and two U.S. Embassies in Africa inflicted 6,059 casualties. Those arrested in Jordan in late December had also planned attacks designed to kill large numbers.

The trend toward higher casualties reflects, in part, the changing motivation of today's terrorists. Religiously motivated terrorist groups, such as Usama bin Ladin's group, al-Qaida, which is believed to have bombed the U.S. Embassies in Africa, represent a growing trend toward hatred of the United States. Other terrorist groups are driven by visions of a post-apocalyptic future or by ethnic hatred. Such groups may lack a concrete political goal other than to punish their enemies by killing as many of them as possible, seemingly without concern about alienating sympathizers. Increasingly, attacks are less likely to be followed by claims of responsibility or lists of political demands.

The shift in terrorist motives has contributed to a change in the way some international terrorist groups are structured, Because groups based on ideological or religious motives may lack a specific political or nationalistic agenda, they have less need for a hierarchical structure. Instead, they can rely on loose affiliations with like-minded groups from a variety of countries to support their common cause against the United States.

Al-Qaida is the best-known transnational terrorist organization. In addition to pursuing its own terrorist campaign, it calls on numerous militant groups that share some of its ideological beliefs to support its violent campaign against the United States, But neither al-Qaida's extremist politico-religious beliefs nor its leader, Usama bin Ladin, is unique. If al-Qaida and Usama bin Ladin were to disappear tomorrow, the United States would still face potential terrorist threats from a growing number of groups opposed to perceived American hegemony. Moreover, new terrorist threats can suddenly emerge from isolated conspiracies or obscure cults with no previous history of violence.

These more loosely affiliated, transnational terrorist networks are difficult to predict, track, and penetrate. They rely on a variety of sources for funding and logistical support, including self-financing criminal activities such as kidnapping, narcotics, and petty crimes. Their networks of support include both front organizations and legitimate business and nongovernment organizations. They use the Internet as an effective communications channel.

Guns and conventional explosives have so far remained the weapons of choice for most terrorists. Such weapons can cause many casualties and are relatively easy to acquire and use. But some terrorist groups now show interest in acquiring the capability

to use chemical, biological, radiological, or nuclear (CBRN) materials. It is difficult to predict the likelihood of a CBRN attack, but most experts agree that today's terrorists are seeking the ability to use such agents in order to cause mass casualties.

Still, these kinds of weapons and materials confront a non-state sponsored terrorist group with significant technical challenges. While lethal chemicals are easy to come by, getting large quantities and weaponizing them for mass casualties is difficult, and only nation states have succeeded in doing so. Biological agents can be acquired in nature or from medical supply houses, but important aspects of handling and dispersion are daunting. To date, only nation states have demonstrated the capability to build radiological and nuclear weapons.

The 1995 release of a chemical agent in the Tokyo subway by the apocalyptic Aum Shinrikyo group demonstrated the difficulties that terrorists face in attempting to use CBRN weapons to produce mass casualties. The group used scores of highly skilled technicians and spent tens of millions of dollars developing a chemical attack that killed fewer people than conventional explosives could have. The same group failed totally in a separate attempt to launch an anthrax attack in Tokyo.

However, if the terrorists' goal is to challenge significantly Americans' sense of safety and confidence, even a small CBRN attack could be successful.

Moreover, terrorists could acquire more deadly CBRN capabilities from a state. Five of the seven nations the United States identifies as state sponsors of terrorism have programs to develop weapons of mass destruction. A state that knowingly provides agents of mass destruction or technology to a terrorist group should worry about losing control of the terrorists' activities and, if the weaoons could be traced back to that state, the near certainty of massive retaliation. However, it is always difficult and sometimes dangerous to attempt to predict the actions of a state. Moreover, a state in chaos, or elements within such a state, might run these risks, especially if the United States were engaged in military conflict with that state or if the United States were distracted by a major conflict in another area of the world.

The Commission was particularly concerned about the persistent lack of adequate security and safeguards for the nuclear material in the former Soviet Union (FSU). A Center for Strategic International Studies panel chaired by former Senator Sam Nunn concluded that, despite a decade of effort, the risk of "loose nukes" is greater than ever. Another ominous warning was given in 1995 when Chechen rebels, many of whom fight side-by-side with Islamic terrorists from bin Ladin's camps sympathetic to the Chechen cause, placed radioactive material in a Moscow park.

Cyber attacks are often considered in the same context with CBRN. Respectable experts have published sobering scenarios about the potential impact of a successful cyber attack on the United States. Already, hackers and criminals have exploited some of our vulnerabilities.

Certainly, terrorists are making extensive use of the new information technologies, and a conventional terrorist attack along with a coordinated cyber attack could exponentially compound the dam-

age. While the Commission considers cyber security a matter of grave importance, it also notes that the measures needed to protect the United States from cyber attack by terrorists are largely identical to those necessary to protect us from such an attack by a hostile foreign country, criminals, or vandals.

Not all terrorists are the same, but the groups most dangerous to the United States share some characteristics not seen 10 or 20 years ago:

- They operate in the United States as well as abroad.
- Their funding and logistical networks cross borders, are less dependent on state sponsors, and are harder to disrupt with economic sanctions.
- They make use of widely available technologies to communicate quickly and securely.
- Their objectives are more deadly.

This changing nature of the terrorist threat raises the stakes in getting American counterterrorist policies and practices right.

GOOD INTELLIGENCE IS THE BEST WEAPON AGAINST INTERNATIONAL TERRORISM

Obtaining information about the identity, goals, plans, and vulnerabilities of terrorists is extremely difficult. Yet, no other single policy effort is more important for preventing, preemepting, and responding to attacks.

The Commission has identified significant obstacles to the collection and distribution of reliable information on terroriswm to analysts and policymakers. These obstacles must be removed.

In addition, this information, often collected at great risk to agents and officers in the field, must be safeguarded. Leaks of intelligence and law enforcement information reduce its value, endanger sources, alienate friendly nations and inhibit their cooperation, and jeopardize the U.S. Government's ability to obtain further information.

ELIMINATE BARRIERS TO AGGRESSIVE COLLECTION OF INFORMATION ON TERRORISTS

Complex bureaucratic procedures now in place send an unmistakable message to Central Intelligence Agency (CIA) officers in the field that recruiting clandestine sources of terrorist information is encouraged in theory but discouraged in practice.

PURSUE A MORE AGGRESSIVE STRATEGY AGAINST TERRORISM

Since the 1980s, the United States has based its counterterrorism policy on four pillars:

- Make no consessions to terrorists and strike no deals:
- Bring terrorists to justice for their crimes:
- Isolate and apply pressure on states that sponsor terrorism to force them to cange their behavior; and
- Bolster the counterterrorism capabilities of countries that work with the United States and require assistance.

The government uses multiple tools to pursue this strategy. Diplomacy is an important instrument, both in gaining the assistance

of other nations in particular cases and convincing the international community to condemn and outlaw egregious terrorist practices. Law enforcement is often invaluable in the investigation and apprehension of terrorists. Military force and covert action can often preempt or disrupt terrorist attacks. But meeting the changing terrorist threat requires more aggressive use of these tools and the development of new policies and practices.

PREPARE TO PREVENT OR RESPOND TO CATASTROPHIC TERRORIST ATTACKS

A terrorist attack in the United States using a biological agent, deadly chemicals, or nuclear or radiological material, even if only partially successful, would profoundly affect the entire nation, as would a series of conventional attacks or a single bombing that caused thousands of deaths. Given the trend toward more deadly terrorist attacks and indications that mass casualties are an objective of many of today's terrorists, it is essential that America be fully prepared to prevent and respond to this kind of catastrophic terrorism.

Over the past few years, the U.S. Government has taken a number of positive steps. Several Presidential Directives have effected major changes in organizational responsibilities and improved cooperation. The Department of Health and Human Services' Strategic Plan, the Attorney General's Five-Year Plan, the establishment of a military Joint Task Force for Civil Support, and improvement in first responders' capabilities are valuable efforts, but there is still more to do.

There is a risk that, in preventing or responding to a catastrophic terrorist attack, officials may hesitate or act improperly because they do not fully understand their legal authority or because there are gaps in that authority.

There is some statutory authority that does not now exist that should be considered for catastrophic conditions. For example:

- Federal quarantine authority cannot be used in a situation that is confined to a single state.
- Not all cities or states have their own quarantine authority.
- There is no clear federal authority with regard to compelling vaccinations, or rationing scarce vaccinations, or requiring autopsies when necessary for a terrorism investigation.

The Constitution permits extraordinary measures in the face of extraordinary threats, To prevent or respond to catastrophic terrorism, law enforcement and public health officials have the authority to conduct investigations and implement measures that temporarily exceed measures applicable under non-emergency conditions. These may include cordoning off of areas, vehicle searches, certain medical measures, and sweep searches through areas believed to contain weapons or terrorists.

Determining whether a particular measure is reasonable requires balancing privacy and other rights against the public interest in coping with a terrorist threat which may lead to massive casualties. Advance preparation is the best way to deal successfully with a terrorist incident without jeopardizing individuals' Constitutional rights.

Recommendations:

- The President should direct the preparation of a manual on the implementation of existing legal authority necessary to address effectively a catastrophic terrorist threat or attack. The manual should be distributed to the appropriate federal, state, and local officials and be used in training, exercises, and educational programs.
- The President should determine whether any additional legal authority is needed to deal with catastrophic terrorism and make recommendations to Congress if necessary.

The U.S. Government's plans for a catastrophic terrorist attack on the United States do not employ the full range of the Department of Defense's (DoD's) capabilities for managing large operations. Additionally the interagency coordination and cooperation required to integrate the DoD properly into counterterrorism planning has not been accomplished.

The Department of Defense's ability to command and control vast resources for dangerous, unstructured situations is unmatched by any other department or agency. According to current plans, DoD involvement is limited to supporting the agencies that are currently designated as having the lead in a terrorism crisis, the FBI and the Federal Emergency Management Agency (FEMA). But, in extraordinary circumstances, when a catastrophe is beyond the capabilities of local, state, and other federal agencies, or is directly related to an armed conflict overseas, the President may want to designate DoD as a lead federal agency. This may become a critical operational consideration in planning for future conflicts. Current plans and exercises do not consider this possibility.

An expanded role for the DoD in a catastrophic terrorist attack will have policy and legal implications. Other federal agencies, the states, and local communities will have major concerns. In preparing for such a contingency, there will also be internal DoD issues on resources and possible conflicts with traditional military contingency plans. These issues should be addressed beforehand.

Effective preparation also requires effective organization. The DoD is not optimally organized to respond to the wide range of missions that would likely arise from the threat of a catastrophic terrorist attack. For example, within DoD several offices, departments, Unified Commands, the Army, and the National Guard have overlapping responsibilities to plan and execute operations in case of a catastrophic terrorist attack. These operations will require an unprecedented degree of interagency coordination and communication in order to be successful.

There are neither plans for the DoD to assume a lead agency role nor exercises rehearsing this capability. Hence, these demanding tasks would have to be accomplished on an ad hoc basis by the military.

Recommendations:

- The President should direct the Assistant to the President for National Security Affairs, in coordination with the Secretary of Defense and the Attorney General, to develope and adopt detailed contingency plans that would transfer lead federal agen-

cy authority to the Department of Defense if necessary during a catastrophic terrorist attack or prior to an imminent attack.
- The Secretary of Defense should establish a unified command structure that would integrate all catastrophic terrorism capabilities and conduct detailed planning and exercises with relevant federal, state, and local authorities.

The interagency program and plan for exercising the government's preparedness to respond to a catastrophic terrorist attack is inadequate.

In addition to DoD exercises, a realistic interagency exercise program, with full participation by all relevant federal agencies and their leaders, is essential for national preparedness to counter a catastrophic terrorist attack. In June 1995, the President established an interagency counterterrorist Exercise Subgroup and program which included preparation for a catastrophic terrorist attack. However, not all federal agencies have participated in or budgeted for these exercises.

Additionally, in September 1998, Congress funded and mandated the Department of Justice and the Federal Emergency Management Agency to conduct a counterterrorism and consequence management exercise, called TOPOFF, involving relevant federal agencies and their senior leadership, with select state and local governments participating, to evaluate the U.S. Government's preparedness for a catastrophic terrorist incident. However, sufficient funding was not provided and there is no requirement to exercise on a regular schedule.

Recommendation:

- The President should direct (1) the Exercise Subgroup, under the direction of the national coordinator for counterterrorism, to exercise annually the government's responses to a catastrophic terrorism crisis, including consequence management; and (2) all relevant federal agencies to plan, budget and participate in counterterrorism and consequence management exercises coordinated by the Exercise Subgroup and ensure senior officer level participation, particularly in the annual exercises.

Given the urgency of near-term needs, long-term research and development (R&D) projects on technologies useful to fighting terrorism will be short-changed unless Congress and the President can agree on special procedures and institutional arrangements to work on research that is risky and has more distant payoffs.

Research and Development spending for new technologies to cope with catastrophic terrorism has significantly increased over the past three years. Most of the funds, however, are targeted on near-term improvements to meet immediate needs for better detectors, more vaccines, and requirements of first responders.

To prevent or cope with terrorist attacks in the future, in particular attacks using CBRN agents, the U.S. Government must make greater use of America's dominance in science and technology. No other country, much less any subnational organization, can match U.S. scientific and technological prowess in biotechnology and pharmaceutical production and quality control, elec-

tronics, computer science and other domains that could help overcome and defeat the technologies used by future terrorists. But this kind of R&D requires time—five to ten years or more—to develop new ideas, test hypotheses, craft preliminary applications, and test them. Developing mass production for successful applications further delays getting products into the hands of users.

The following list illustrates, but by no means exhausts, the type of projects that could constitute a long-term R&D program.

- New sensors to detect nuclear weapons in transit (e.g., gamma-ray imaging systems, including stimulation to elicit detectable emissions).
- High power ultraviolet beams to destroy BW agents and to clean up contaminated areas.
- New types of "tripwires" suitable for many different entry-points (e.g., expolsive-sniffers, body-scanners, and their prototyping for mass-production.
- Advanced development of anti-virals for smallpox.

The Commission considered several institutional arrangements to manage long-term R&D. One option is establishing a large program at one of the Department of Energy (DoE) or other national laboratories to conduct in-house research, contract for external research, initiate prototyping for production, and involve qualified outside experts. This last task is particularly important in the fields of biotechnology and pharmaceutical production techniques. The goal would be to attract talented biotechnology and pharmaceutical industry scientists and engineers to work with the government for one or two years on high priority projects.

Recommendation:

- The President should establish a comprehensive and coordinated long-term Research and Development program to counter catastrophic terrorism.

Current controls on transfers of pathogens that could be used in biological terrorism are inadequate and controls on related equipment are nonexistent. In addition, current programs of the Department of Health and Human Services are not adequate to ensure physical security of pathogens or to monitor disease outbreaks overseas.

Terrorists, without serious risk of detection, could obtain pathogens from domestic natural sources, steal them, or import them into the United States. Most pathogens in the United States are tightly controlled, but regulation of laboratories as well as of dangerous agents during transport are designed to prevent accidents, not theft. Moreover, these controls are not as rigorous as controls over nuclear material.

Creating pathogens small and sturdy enough to disperse broadly over a target population for an effective period of time remains, fortunately, a complex process. Thus, regulating the sophisticated equipment required to turn pathogens into weapons could hamper terrorist efforts to acquire this capability.

However, no regulatory scheme is foolproof. Moreover, contagious diseases do not require sophisticated dispersion devices. Thus, it is important to have the ability to detect outbreaks of infectious dis-

eases and to distinguish bioterrorist attacks from natural outbreaks. Some detection and analytical systems are in place domestically, but the international community's ability to distinguish natural disease from terrorism lags far behind even these modest U.S. efforts.

Recommendations:

- The Secretary of Health and Human Services should strengthen physical security standards applicable to the storage, creation, and transport of pathogens in research laboratories and other certified facilities in order to protect against theft or diversion. These standards should be as rigorous as the physical protection and security measures applicable to critical nuclear materials.
- The Congress should:
  —Make possession of designated critical pathagens illegal for anyone who is not properly certified.
  —Control domestic sale and transfer of equipment critical to the development or use of biological agents by certifying legitimate users of critical equipment and prohibiting sales of such equipment to non-certified entities.
  —Require tagging of critical equipment to enable law enforcement to identify its location.
- The Secretary of Health and Human Services, working with the Department of State, should develop an international monitoring program to provide early warning of infectious disease outbreaks and possible terrorist experimentation with biological substances.

ROAD MAP FOR NATIONAL SECURITY: IMPERATIVE FOR CHANGE

THE PHASE III REPORT OF THE U.S. COMMISSION ON NATIONAL SECURITY/21ST CENTURY

EXCERPT ON "SECURING THE NATIONAL HOMELAND"

FEBRUARY 15, 2001

U.S. COMMISSION ON NATIONAL SECURITY/21ST CENTURY [1]

GARY HART
Co-Chair

WARREN B. RUDMAN
Co-Chair

ANNE ARMSTRONG
Commissioner

NORMAN R. AUGUSTINE
Commissioner

JOHN DANCY
Commissioner

JOHN R. GALVIN
Commissioner

LESLIE H. GELB
Commissioner

NEWT GINGRICH
Commissioner

LEE H. HAMILTON
Commissioner

LIONEL H. OLMER
Commissioner

DONALD B. RICE
Commissioner

JAMES SCHLESINGER
Commissioner

HARRY D. TRAIN
Commissioner

ANDREW YOUNG
Commissioner

CHARLES G. BOYD, *Executive Director*

[1] Disclaimer: This Commission has striven successfully to achieve consensus on all major issues, and each Commissioner stands by all the major recommendations made in this report. However, as is to be expected when discussing complex issues, not every Commissioner agrees completely with every statement in the text that follows.

I. SECURING THE NATIONAL HOMELAND

One of this Commission's most important conclusions in its Phase I report was that attacks against American citizens on American soil, possibly causing heavy casualties, are likely over the next quarter century.[7] This is because both the technical means for such attacks, and the array of actors who might use such means, are proliferating despite the best efforts of American diplomacy.

These attacks may involve weapons of mass destruction and weapons of mass disruption. As porous as U.S. physical borders are in an age of burgeoning trade and travel, its "cyber borders" are even more porous—and the critical infrastructure upon which so much of the U.S. economy depends *can* now be targeted by non-state and state actors alike. America's present global predominance does not render it immune from these dangers. To the contrary, U.S. preeminence makes the American homeland more appealing as a target, while America's openness and freedoms make it more vulnerable.

Notwithstanding a growing consensus on the seriousness of the threat to the homeland posed by weapons of mass destruction and disruption, the U.S. government *has not* adopted homeland security as a primary national security mission. Its structures and strategies are fragmented and inadequate. The President must therefore both develop a comprehensive strategy and propose new organizational structures to prevent and protect against attacks on the homeland, and to respond to such attacks if prevention and protection should fail.

Any reorganization must be mindful of the scale of the scenarios we envision and the enormity of their consequences. We need orders-of-magnitude improvements in planning, coordination, and exercise. The govemment must also be prepared to use effectively—albeit with all proper safeguards—the extensive resources of the Department of Defense. This will necessitate new priorities for the U.S. armed forces and particularly, in our view, for the National Guard.

The United States *is today very poorly organized to design and implement any comprehensive strategy to protect the homeland.* The assets and organizations that now exist for homeland security are scattered across more than two dozen departments and agencies, and all fifty states. The Executive Branch, with the full participation of Congress, needs to realign, refine, and rationalize these as-

[7] See *New World Coming,* p. 4, and the Report of the National Defense Panel, *Transforming Defense: National Security in the 21st Century* (Washington, DC: December 1997), p. 17.

sets into a coherent whole, or even the best strategy will lack an adequate vehicle for implementation.

This Commission believes that the security of the American homeland from the threats of the new century should be *the* primary national security mission of the U.S. government. While the Executive Branch must take the lead in dealing with the many policy and structural issues involved, Congress is a partner of critical importance in this effort. It must find ways to address homeland security issues that bridge current gaps in organization, oversight, and authority, and that resolve conflicting claims to jurisdiction within both the Senate and the House of Representatives and also between them.

Congress is crucial, as well, for guaranteeing that homeland security is *achieved within a framework of law that protects the civil liberties and privacy of American citizens.* We are confident that the U.S. government can enhance national security without compromising established Constitutional principles. But in order to guarantee this, we must plan ahead. In a major attack involving contagious biological agents, for example, citizen cooperation with government authorities will depend on public confidence that those authorities can manage the emergency. If that confidence is lacking, panic and disorder could lead to insistent demands for the temporary suspension of some civil liberties. That is why preparing for the worst is essential to protecting individual freedoms during a national crisis.

Legislative guidance for planning among federal agencies and state and local authorities must take particular cognizance of the role of the Defense Department. *Its subordination to civil authority needs to be clearly defined in advance.*

In short, advances in technology have created new dimensions to our nation's economic and physical security. While some new threats can be met with traditional responses, others cannot. More needs to be done in three areas to prevent the territory and infrastructure of the United States from becoming easy and tempting targets: in strategy, in organizational realignment, and in Executive-Legislative cooperation. We take these areas in turn.

A. THE STRATEGIC FRAMEWORK

A homeland security strategy to minimize the threat of intimidation and loss of life is an essential support for an international leadership role for the United States. Homeland security is not peripheral to U.S. national security strategy but central to it. At this point, national leaders have not agreed on a clear strategy for homeland security, a condition this Commission finds dangerous and intolerable. We therefore recommend the following:

• 1: The President should develop a comprehensive strategy to heighten America's ability to prevent and protect against all forms of attack on the homeland, and to respond to such attacks if prevention and protection fail.

In our view, the President should:

- Give new priority in his overall national security strategy to homeland security, and make it a central concern for incoming

officials in all Executive Branch departments, particularly the intelligence and law enforcement communities;
- Calmly prepare the American people for prospective threats, and increase their awareness of what federal and state governments are doing to prevent attacks and to protect them if prevention fails;
- Put in place new government organizations and processes, eliminating where possible staff duplication and mission overlap; and
- Encourage Congress to establish new mechanisms to facilitate closer cooperation between the Executive and Legislative Branches of government on this vital issue.

We believe that homeland security can best be assured through a strategy of *layered defense* that focuses first on prevention, second on protection, and third on response.

Prevention.—Preventing a potential attack comes first. Since the occurrence of even one event that causes catastrophic loss of life would represent an unacceptable failure of policy, U.S. strategy should therefore act as far forward as possible to prevent attacks on the homeland. This strategy has at its disposal three essential instruments.

Most broadly, the first instrument is U.S. diplomacy. U.S. foreign policy should strive to shape an international system in which just grievances can be addressed without violence. Diplomatic efforts to develop friendly and trusting relations with foreign governments and their people can significantly multiply America's chances of gaining early warning of potential attack and of doing something about impending threats. Intelligence-sharing with foreign governments is crucial to help identify individuals and groups who might be considering attacks on the United States or its allies. Cooperative foreign law enforcement agencies can detain, arrest, and prosecute terrorists on their own soil. Diplomatic success in resolving overseas conflicts that spawn terrorist activities will help in the long run.

Meanwhile, verifiable arms control and nonproliferation efforts must remain a top priority. These policies can help persuade states and terrorists to abjure weapons of mass destruction and to prevent the export of fissile materials and dangerous dual-use technologies. But such measures cannot by themselves prevent proliferation. So other measures are needed, including the possibility of punitive measures and defenses. The United States should take a lead role in strengthening multilateral organizations such as the International Atomic Energy Agency.

In addition, increased vigilance against international crime syndicates is also important because many terrorist organizations gain resources and other assets through criminal activity that they then use to mount terrorist operations. Dealing with international organized crime requires not only better cooperation with other countries, but also among agencies of the federal government. While progress has been made on this front in recent years, more remains to be done.[8]

---

[8] See *International Crime Threat Assessment* (Washington, DC: The White House, December 2000).

The second instrument of homeland security consists of the U.S. diplomatic, intelligence, and military presence overseas. Knowing the who, where, and how of a potential physical or cyber attack is the key to stopping a strike before it can be delivered. Diplomatic, intelligence, and military agencies overseas, as well as law enforcement agencies working abroad, are America's primary eyes and ears on the ground. But increased public-private efforts to enhance security processes within the international transportation and logistics networks that bring people and goods to America are also of critical and growing importance.

Vigilant systems of border security and surveillance are a third instrument that can prevent those agents of attack who are not detected and stopped overseas from actually entering the United States. Agencies such as the U.S. Customs Service and U.S. Coast Guard have a critical prevention role to play. Terrorists and criminals are finding that the difficulty of policing the rising daily volume and velocities of people and goods that cross U.S. borders makes it easier for them to smuggle weapons and contraband, and to move their operatives into and out of the United States. Improving the capacity of border control agencies to identify and intercept potential threats without creating barriers to efficient trade and travel requires a sub-strategy also with three elements.

First is the development of new transportation security procedures and practices designed to reduce the risk that importers, exporters, freight forwarders, and transportation carriers will serve as unwitting conduits for criminal or terrorist activities. *Second* is bolstering the intelligence gathering, data management, and information sharing capabilities of border control agencies to improve their ability to target high-risk goods and people for inspection. *Third* is strengthening the capabilities of border control agencies to arrest terrorists or interdict dangerous shipments *before* they arrive on U.S. soil.

These three measures, which place a premium on public-private partnerships, will pay for themselves in short order. They will allow for the more efficient allocation of limited enforcement resources along U.S. borders. There will be fewer disruptive inspections at ports of entry for legitimate businesses and travelers. They will lead to reduced theft and insurance costs, as well. Most important, the underlying philosophy of this approach is one that balances prudence, on the one hand, with American values of openness and free trade on the other.[9] To shield America from the world out of fear of terrorism is, in large part, to do the terrorists' work for them. To continue business as usual, however, is irresponsible.

The same may be said for our growing cyber problems. Protecting our nation's critical infrastructure depends on greater public awareness and improvements in our tools to detect and diagnose intrusions. This will require better information sharing among all federal, state, and local governments as well as with private sector owners and operators. The federal government has these specific tasks:

---

[9] Note in this regard Stephen B. Flynn, "Beyond Border Control," *Foreign Affairs* (November/December 2000).

- To serve as a model for the private sector by improving its own security practices;
- To address known government security problems on a system-wide basis;
- To identify and map network interdependencies so that harmful cascading effects among systems can be prevented;
- To sponsor vulnerability assessments within both the federal government and the private sector; and
- To design and carry out simulations and exercises that test information system security across the nation's entire infrastructure.

Preventing attacks on the American homeland also requires that the United States maintain long-range strike capabilities. The United States must bolster deterrence by making clear its determination to use military force in a preemptive fashion if necessary. Even the most hostile state sponsors of terrorism, or terrorists themselves, will think twice about harming Americans and American allies and interests if they fear direct and severe U.S. attack after—*or before*—the fact. Such capabilities will strengthen deterrence even if they never have to be used.

Protection.—The Defense Department undertakes many different activities that serve to protect the American homeland, and these should be integrated into an overall surveillance system, buttressed with additional resources. A ballistic missile defense system would be a useful addition and should be developed to the extent technically feasible, fiscally prudent, and politically sustainable. Defenses should also be pursued against cruise missiles and other sophisticated atmospheric weapon technologies as they become more widely deployed. While both active duty and reserve forces are involved in these activities, the Commission believes that more can and should be done by the National Guard, as is discussed in more detail below.

Protecting the nation's critical infrastructure and providing cyber-security must also include:

- Advanced indication, warning, and attack assessments;
- A warning system that includes voluntary, immediate private-sector reporting of potential attacks to enable other private-sector targets (and the U.S. government) better to take protective action; and
- Advanced systems for halting attacks, establishing backups, and restoring service.

Response.—Managing the consequences of a catastrophic attack on the U.S. homeland would be a complex and difficult process. The first priority should be to build up and augment state and local response capabilities. Adequate equipment must be available to first responders in local communities. Procedures and guidelines need to be defined and disseminated and then practiced through simulations and exercises. Interoperable, robust, and redundant communications capabilities are a must in recovering from any disaster. Continuity of government and critical services must be ensured as well. Demonstrating effective responses to natural and manmade disasters will also help to build mutual confidence and relation-

ships among those with roles in dealing with a major terrorist attack.

All of this puts a premium on making sure that the disparate organizations involved with homeland security—on various levels of government and in the private sector—can work together effectively. We are frankly skeptical that the U.S. government, as it exists today, can respond effectively to the scale of danger and damage that may come upon us during the next quarter century. This leads us, then, to our second task: that of organizational realignment.

B. ORGANIZATIONAL REALIGNMENT

Responsibility for homeland security resides at all levels of the U.S. government—local, state, and federal. Within the federal government, almost every agency and department is involved in some aspect of homeland security. None have been organized to focus on the scale of the contemporary threat to the homeland, however. This Commission urges an organizational realignment that:

- Designates a single person, accountable to the President, to be responsible for coordinating and overseeing various U.S. government activities related to homeland security;
- Consolidates certain homeland security activities to improve their effectiveness and coherence;
- Establishes planning mechanisms to define clearly specific responses to specific types of threats; and
- Ensure that the appropriate resources and capabilities are available.

Therefore, this Commission strongly recommends the following:

• 2: The President should propose, and Congress should agree to create, a National Homeland Security Agency (NHSA) with responsibility for planning, coordinating, and integrating various U.S. government activities involved in homeland security. The Federal Emergency Management Agency (FEMA) should be a key building block in this effort.

Given the multiplicity of agencies and activities involved in these homeland security tasks, someone needs to be responsible and accountable to the President not only to coordinate the making of policy, but also to oversee its implementation. This argues against assigning the role to a senior person on the National Security Council (NSC) staff and for the creation of a separate agency. This agency would give priority to overall planning while relying primarily on others to carry out those plans. To give this agency sufficient stature within the government, its director would be a member of the Cabinet and a statutory advisor to the National Security Council. The position would require Senate confirmation.

Notwithstanding NHSA's responsibilities, the National Security Council would still play a strategic role in planning and coordinating all homeland security activities. This would include those of NHSA as well as those that remain separate, whether they involve other NSC members or other agencies, such as the Centers for Disease Control within the Department of Health and Human Services.

We propose building the National Homeland Security Agency upon the capabilities of the Federal Emergency Management Agency (FEMA), an existing federal agency that has performed well in recent years, especially in responding to natural disasters. NHSA would be legislatively chartered to provide a focal point for all natural and manmade crisis and emergency planning scenarios. It would retain and strengthen FEMA's ten existing regional offices as a core element of its organizational structure.

While FEMA is the necessary core of the National Homeland Security Agency, it is not sufficient to do what NHSA needs to do. In particular, patrolling U.S. borders, and policing the flows of peoples and goods through the hundreds of ports of entry, must receive higher priority. These activities need to be better integrated, but efforts toward that end are hindered by the fact that the three organizations on the front line of border security are spread across three different U.S. Cabinet departments. The Coast Guard works under the Secretary of Transportation, the Customs Service is located in the Department of the Treasury, and the, Immigration and Naturalization Service oversees the Border Patrol in the Department of Justice. In each case, the border defense agency is far from the mainstream of its parent department's agenda and consequently receives limited attention from the department's senior officials. We therefore recommend the following:

• 3: The President should propose to Congress the transfer of the Customs Service, the Border Patrol, and Coast Guard to the National Homeland Security Agency, while preserving them as distinct entities.

Bringing these organizations together under one agency will create important synergies. Their individual capabilities will be molded into a stronger and more effective system, and this realignment will help ensure that sufficient resources are devoted to tasks crucial to both public safety and U.S. trade and economic interests. Consolidating overhead, training programs, and maintenance of the aircraft, boats, and helicopters that these three agencies employ will save money, and further efficiencies could be realized with regard to other resources such as information technology, communications equipment, and dedicated sensors. Bringing these separate, but complementary, activities together will also facilitate more effective Executive and Legislative oversight, and help rationalize the process of budget preparation, analysis, and presentation.

Steps must be also taken to strengthen these three individual organizations themselves. The Customs Service, the Border Patrol, and the Coast Guard are all on the verge of being overwhelmed by the mismatch between their growing duties and their mostly static resources.

The Customs Service, for example, is charged with preventing contraband from entering the United States. It is also responsible for preventing terrorists from using the commercial or private transportation venues of international trade for smuggling explosives or weapons of mass destruction into or out of the United States. The Customs Service, however, retains only a modest air, land, and marine interdiction force, and its investigative component, supported by its own intelligence branch, is similarly modest.

The high volume of conveyances, cargo, and passengers arriving in the United States each year already overwhelms the Customs Service's capabilities. Over $8.8 billion worth of goods, over 1.3 million people, over 340,000 vehicles, and over 58,000 shipments are processed *daily* at entry points. Of this volume, Customs can inspect only *one to two percent* of all inbound shipments. The volume of U.S. international trade, measured in terms of dollars and containers, has doubled since 1995, and it may well double again between now and 2005.

Therefore, this Commission believes that *an improved computer information capability and tracking system—as well as upgraded equipment that can detect both conventional and nuclear explosives, and chemical and biological agents—would be a wise short-term investment with important long-term benefits.* It would also raise the risk for criminals seeking to target or exploit importers and cargo carriers for illicit gains.[10]

The Border Patrol is the uniformed arm of the Immigration and Naturalization Service. Its mission is the detection and prevention of illegal entry into the United States. It works primarily between ports of entry and patrols the borders by various means. There has been a debate for many years about whether the dual functions of the Immigration and Naturalization Service—border control and enforcement on the one side, and immigration facilitation on the other—should be joined under the same roof. The U.S. Commission on Immigration Reform concluded that they should not be joined.[11] We agree: the Border Patrol should become part of the NHSA.

The U.S. Coast Guard is a highly disciplined force with multiple missions and a natural role to play in homeland security. It performs maritime search and rescue missions, manages vessel traffic, enforces U.S. environmental and fishery laws, and interdicts and searches vessels suspected of carrying illegal aliens, drugs, and other contraband. En a time of war, it also works with the Navy to protect U.S. ports from attack.

Indeed, in many respects, the Coast Guard is a model homeland security agency given its unique blend of law enforcement, regulatory, and military authorities that allow it to operate within, across, and beyond U.S. borders. It accomplishes its many missions by routinely working with numerous local, regional, national, and international agencies, and by forging and maintaining constructive relationships with a diverse group of private, non-governmental, and public marine-related organizations. As the fifth armed service, in peace and war, it has national defense missions that include port security, overseeing the defense of coastal waters, and supporting and integrating its forces with those of the Navy and the other services.

The case for preserving and enhancing the Coast Guard's multimission capabilities is compelling. But its crucial role in protecting national interests close to home has not been adequately appreciated, and this has resulted in serious and growing readiness concerns. U.S. Coast Guard ships and aircraft are aging and technologically obsolete; indeed; the Coast Guard cutter fleet is older than

[10] See the *Report of the Interagency Commission on Crime and Security in U.S. Seaports* (Washington, DC: Fall 2000).

[11] See the *Report of the U.S. Commission on Immigration Reform* (Washington, DC: 1997).

39 of the world's 41 major naval fleets. As a result, the Coast Guard fleet generates excessive operating and maintenance costs, and lacks essential capabilities in speed, sensors, and interoperability. To fulfill all of its missions, the Coast Guard requires updated platforms with the staying power, in hazardous weather, to remain offshore and fully operational throughout U.S. maritime economic zones,[12]

The Commission recommends strongly that Congress recapitalize the Customs Service, the Border Patrol, and the Coast Guard so that they can confidently perform key homeland security roles.

NHSA's planning, coordinating, and overseeing activities would be undertaken through three staff Directorates. The Directorate of Prevention would oversee and coordinate the various border security activities, as discussed above. A Directorate of Critical Infrastructure Protection (CIP) would handle the growing cyber threat. FEMA's emergency preparedness and response activities would be strengthened in a third directorate to cover both natural and manmade disasters. A Science and Technology office would advise the NHSA Director on research and development efforts and priorities for all three directorates.

Relatively small permanent staffs would man the directorates. NHSA will employ FEMA's principle of working effectively with state and local governments, as well as with other federal organizations, stressing interagency coordination. Much of NHSA's daily work will take place directly supporting state officials in its regional offices around the country. Its organizational infrastructure *will not be heavily centered* in the Washington, DC area.

NHSA would also house a National Crisis Action Center (NCAC), which would become the nation's focal point for monitoring emergencies and for coordinating federal support in a crisis to state and local governments, as well as to the private sector. We envision the center to be an interagency operation, directed by a two-star National Guard general, with full-time representation from the other federal agencies involved in homeland security.

NHSA will require a particularly close working relationship with the Department of Defense. It will need also to create and maintain strong mechanisms for the sharing of information and intelligence with U.S. domestic and international intelligence entities. We suggest that NHSA have liaison officers in the counter-terrorism centers of both the FBI and the CIA. Additionally, the sharing of information with business and industry on threats to critical infrastructures requires further expansion.

NHSA will also assume responsibility for overseeing the protection of the nation's critical infrastructure. Considerable progress has been made in implementing the recommendations of the President's Commission on Critical Infrastructure Protection (PCCIP) and Presidential Decision Directive 63 (PDD-63). But more needs to be done, for the United States has real and growing problems in this area.

U.S. dependence on increasingly sophisticated and more concentrated critical infrastructures has increased dramatically over

[12] See Report of the Interagency Task Force on U.S. Coast Guard Roles and Missions, *A Coast Guard for the Twenty First-Century* (Washington, DC: December 1999).

the past decade. Electrical utilities, water and sewage systems, transportation networks, and communications and energy systems now depend on computers to provide safe, efficient, and reliable service. The banking and finance sector, too, keeps track of millions of transactions through increasingly robust computer capabilities.

The overwhelming majority of these computer systems are privately owned, and many operate at or very near capacity *with little or no provision for manual back-ups in an emergency.*

Moreover, the computerized information networks that link systems together are themselves vulnerable to unwanted intrusion and disruption. An attack on any one of several highly interdependent networks can cause collateral damage to other networks and the systems they connect. Some forms of disruption will lead merely to nuisance and economic loss, but other forms will jeopardize lives. One need only note the dependence of hospitals, air-traffic control systems, and the food processing industry on computer controls to appreciate the point.

The bulk of unclassified military communications, too, relies on systems almost entirely owned and operated by the private sector. Yet little has been done to assure the security and reliability of those communications in crisis. Current efforts to prevent attacks, protect against theft most damaging effects, and prepare for prompt response are uneven at best, and this is dangerous because a determined adversary is most likely to employ a weapon of mass disruption during a homeland security or foreign policy crisis.

As noted above, a Directorate for Critical Infrastructure Protection would be an integral part of the National Homeland Security Agency. This directorate would have two vital responsibilities. First would be to oversee the physical assets and information networks that make up the U.S. critical infrastructure. It should ensure the maintenance of a nucleus of cyber security expertise within the government, as well. There is now an alarming shortage of government cyber security experts due in large part to the financial attraction of private-sector employment that the government cannot match under present personnel procedures.[13] The director's second responsibility would be as the Critical Information Technology, Assurance, and Security Office (CITASO). This office would coordinate efforts to address the nation's vulnerability to electronic or physical attacks on critical infrastructure.

Several critical activities that are currently spread among various government agencies and the private sector *should be brought together for this purpose.* These include:

- Information Sharing and Analysis Centers (ISACs), which are government-sponsored committees of private-sector participants who work to share information, plans, and procedures for information security in their fields;
- The Critical Infrastructure Assurance Office (CIAO), currently housed in the Commerce Department, which develops outreach and awareness programs with the private sector;
- The National Infrastructure Protection Center (NIPC), currently housed in the FBI, which gathers information and provides warnings of cyber attacks; and

[13] We return to this problem below in Section IV.13

- The Institute for Information Infrastructure Protection (I3P), also in the Commerce Department, which is designed to coordinate and support research and development projects on cyber security.

In partnership with the private sector where most cyber assets are developed and owned, the Critical Infrastructure Protection Directorate would be responsible for enhancing information sharing on cyber and physical security, tracking vulnerabilities and proposing improved risk management policies, and delineating the roles of various government agencies in preventing, defending, and recovering from attacks. To do this, the government needs to institutionalize better its private-sector liaison across the board—with the owners and operators of critical infrastructures, hardware and software developers, server/service providers, manufacturers/producers, and applied technology developers.

The Critical Infrastructure Protection Directorate's work with the private sector must include a strong advocacy of greater government and corporate investment in information assurance and security. The CITASO would be the focal point for coordinating with the Federal Communications Commission (FCC) in helping to establish cyber policy, standards, and enforcement mechanisms. Working closely with the Office of Management and Budget (OMB) and its Chief Information Officer Council (CIO Council), the CITASO needs to speak for those interests in government councils.[14] The CITASO must also provide incentives for private-sector participation in Information Sharing and Analysis Centers to share information on threats, vulnerabilities, and individual incidents, to identify interdependencies, and to map the potential cascading effects of outages in various sectors.

The directorate also needs to help coordinate cyber security issues internationally. At present, the FCC handles international cyber issues for the U.S. government through the International Telecommunications Union, As this is one of many related international issues, it would be unwise to remove this responsibility from the FCC. Nevertheless, the CIP Directorate should work closely with the FCC on cyber issues in international bodies.

The mission of the NHSA must include specific planning and operational tasks to be staffed through the Directorate for Emergency Preparedness and Response. These include:

- Setting training and equipment standards, providing resource grants, and encouraging intelligence and information sharing among state emergency management officials, local fast responders, the Defense Department, and the FBI;
- Integrating the various activities of the Defense Department, the National Guard, and other federal agencies into the Federal Response Plan; and
- Pulling together private sector activities, including those of the medical community, on recovery, consequence management, and planning for continuity of services.

[14] The Chief Information Officer Council is a government organization consisting of all the statutory Chief Information Officers in the government. It is located within OMB under the Deputy Director for Management.

Working with state officials, the emergency management community, and the law enforcement community, the job of NHSA's third directorate will be to rationalize and refine the nation's incident response system. The current distinction between crisis management and consequence management is neither sustainable nor wise. The duplicative command arrangements that have been fostered by this division are prone to confusion and delay. NHSA should develop and manage a single response system for national incidents, in close coordination with the Department of Justice (DoJ) and the FBI. This would require that the current policy, which specifies initial DoJ control in terrorist incidents on U.S. territory, be amended once Congress creates NHSA. We believe that this arrangement would in no way contradict or diminish the FBI's traditional role with respect to law enforcement.

The Emergency Preparedness and Response Directorate should also assume a major resource and budget role. WIth the help of the Office of Management and Budget, the directorate's first task will be to figure out what is being spent on homeland security in the various departments and agencies. Only with such an overview can the nation identify the shortfalls between capabilities and requirements. Such a mission budget should be included in the President's overall budget submission to Congress. The Emergency Preparedness and Response Directorate will also maintain federal asset databases and encourage and support up-to-date state and local databases.

FEMA has adapted well to new circumstances over the past few years and has gained a well-deserved reputation for responsiveness to both natural and manmade disasters. While taking on homeland security responsibilities, the proposed NHSA would strengthen FEMA's ability to respond to such disasters. It would streamline the federal apparatus and provide greater support to the state and local officials who, as the nation's first responders, possess enormous expertise. To the greatest extent possible, federal programs should build upon the expertise and existing programs of state emergency preparedness systems and help promote regional compacts to share resources and capabilities.

To help simplify federal support mechanisms, *we recommend transferring the National Domestic Preparedness Office (NDPO), currently housed at the FBI, to the National Homeland Security Agency.* The Commission believes that this transfer to FEMA should be done at first opportunity, even before NHSA is up and running.

The NDPO would be tasked with organizing the training of local responders and providing local and state authorities with equipment for detection, protection, and decontamination in a V/MD emergency. NUSA would develop the policies, requirements, and priorities as part of its planning tasks as well as oversee the various federal, state, and local training and exercise programs. In this way, a single staff would provide federal assistance for any emergency, whether it is caused by flood, earthquake, hurricane, disease, or terrorist bomb.

A WMD incident on American soil is likely to overwhelm local fire and rescue squads, medical facilities, and government services. Attacks may contaminate water, food, and air; large-scale evacu-

ations may be necessary and casualties could be extensive. Since getting prompt help to those who need it would be a complex and massive operation requiring federal support, such operations must be extensively planned in advance. Responsibilities need to be assigned and procedures put in place for these responsibilities to evolve if the situation worsens.

As we envision it, state officials will take the initial lead in responding to a crisis. NHSA will normally use its Regional Directors to coordinate federal assistance, while the National Crisis Action Center will monitor ongoing operations and requirements. Should a crisis overwhelm local assets, state officials will turn to NHSA for additional federal assistance. In major crises, upon the recommendation of the civilian Director of NHSA, the President will designate a senior figure—a Federal Coordinating Officer—to assume direction of all federal activities on the scene. If the situation warrants, a state governor can ask that active military forces reinforce National Guard units already on the scene. Once the President federalizes National Guard forces, or if he decides to use Reserve forces, the Joint Forces Command will assume responsibility for all military operations, acting through designated task force commanders. At the same time, the Secretary of Defense would appoint a Defense Coordinating Officer to provide civilian oversight and ensure prompt civil support. This person would work for the Federal Coordinating Officer.

To be capable of carrying out its responsibilities under extreme circumstances, NHSA will need to undertake robust exercise programs and regular training to gain experience and to establish effective command and control procedures. It will be essential to update regularly the Federal Response Plan. It will be especially critical for NHSA officials to undertake detailed planning and exercises for the *full range* of potential contingencies, *including ones that require the substantial involvement ofmililary assets in support.*

NHSA will provide the overarching structure for homeland security, but other government agencies will retain specific homeland security tasks. We take the necessary obligations of the major ones in turn.

Intelligence Community. Good intelligence is the key to preventing attacks on the homeland and homeland security should become one of the intelligence community's most important missions.[15] Better human intelligence must supplement technical intelligence, especially on terrorist groups covertly supported by states. As noted above, fuller cooperation and more extensive information-sharing with friendly governments will also improve the chances that would-be perpetrators will be detained, arrested, and prosecuted before they ever reach U.S. borders.

The intelligence community also needs to embrace cyber threats as a legitimate mission and to incorporate intelligence gathering on potential strategic threats from abroad into its activities.

To advance these ends, we offer the following recommendation:

[15] We return to this issue in our discussion of the Intelligence Community in Section IlI.F., particularly in recommendation 37.

• 4: The President should ensure that the National Intelligence Council: include homeland security and asymmetric threats as an area of analysis; assign that portfolio to a National Intelligence Officer; and produce National Intelligence Estimates on these threats.

Department of State. U.S. embassies overseas are the American people's first line of defense. U.S. Ambassadors must make homeland security a top priority for all embassy staff, and Ambassadors need the requisite authority to ensure that information is shared in a way that maximizes advance warning overseas of direct threats to the United States.

Ambassadors should also ensure that the gathering of information, and particularly from open sources, takes full advantage of all U.S. government resources abroad, including diplomats, consular officers, military officers, and reptesentatives of the various other departments and agencies. The State Department should also strengthen its efforts to acquire information from Americans living or travelling abroad in private capacities.

The State Department has made good progress in its overseas efforts to reduce terrorism, but we now need to extend this effort into the Information Age. Working with NHSA's CIP Directorate, the State Department should expand cooperation on critical infrastructure protection with other states and international organizations. Private sector initiatives, particularly in the banking community, provide examples of international cooperation on legal issues, standards, and practices. Working with the CIP Directorate and the FCC, the State Department should also encourage other governments to criminalize hacking and electronic intrusions and to help track hackers, computer virus proliferators, and cyber terrorists.

Department of Defense. The Defense Department, which has placed its highest priority on preparing for major theater war, should pay far more attention to the homeland security mission. Organizationally, DoD responses are widely dispersed. An Assistant to the Secretary of Defense for Civil Support has responsibility for WMD incidents, while the Department of the Army's Director of Military Support is responsible for non-WMD contingencies. Such an arrangement does not provide clear lines of authority and responsibility or ensure political accountability. The Commission therefore recommends the following:

• 5: The President should propose to Congress the establishment of an Assistant Secretary of Defense for Homeland Security within the Office of the Secretary of Defense, reporting directly to the Secretary.

A new Assistant Secretary of Defense for Homeland Security would provide policy oversight for the various DoD activities within the homeland security mission and ensure that mechanisms are in place for coordinating military support in major emergencies. He or she would work to integrate homeland security into Defense Department planning, and ensure that adequate resources are forthcoming. This Assistant Secretary would also represent the Secretary in the NSC interagency process on homeland security issues.

Along similar lines and for similar reasons, we also recommend that *the Defense Department broaden and strengthen the existing*

Joint Forces Command/Joint Task Force-Civil Support (JTF-CS) to coordinate military planning, doctrine and command and control for military support for all hazards and disasters.

This task force should be directed by a senior National Guard general with additional headquarters personnel. JTF-CS should contain several rapid reaction task forces, composed largely of rapidly mobilizable National Guard units. The task force should have command and control capabilities for multiple incidents. Joint Forces Command should work with the Assistant Secretary of Defense for Homeland Security to ensure the provision of adequate resources and appropriate force allocations, training, and equipment for civil support.

On the prevention side, maintaining strong nuclear and conventional forces is as high a priority for homeland security as it is for other missions. Shaping a peaceful international environment and deterring hostile military actors remain sound military goals. But deterrent forces may have little effect on non-state groups secretly supported by states, or on individuals with grievances real or imagined. In cases of clear and imminent danger, the military must be able to take preemptive action overseas in circumstances where local authorities are unable or unwilling to act. For this purpose, as noted above, the United States needs to be prepared to use its rapid, long-range precision strike capabilities. A decision to act would obviously rest in civilian hands, and would depend on intelligence information and assessments of diplomatic consequences. But even if a decision to strike preemptively is never taken or needed, the capability should be available nonetheless, for knowledge of it can contribute to deterrence.

We also suggest that the Defense Department broaden its mission of protecting air, sea, and land approaches to the United States, consistent with emerging threats such as the potential proliferation of cruise missiles. The department should examine alternative means of monitoring approaches to the territorial United States. Modern information technology and sophisticated sensors can help monitor the high volumes of traffic to and from the United States. Given the volume of legitimate activities near and on the border, even modern infonnation technology and remote sensors cannot filter the good from the bad as a matter of routine. It is neither wise nor possible to create a surveillance umbrella over the United States. But Defense Department assets can be used to support detection, monitoring, and even interception operations when intelligence indicates a specific threat.

Finally, a better division of labor and understanding of responsibilities is essential in dealing with the connectivity and interdependence of U.S. critical infrastructure systems. This includes addressing the nature of a national transportation network or cyber emergency and the Defense Department's role in prevention, detection, or protection of the national critical infrastructure. The department's sealift and airlift plans are premised on largely unquestioned assumptions that domestic transportation systems will be fully available to support mobilization requirements. The department also is paying insufficient attention to the vulnerability of its information networks. Currently, the department's computer network defense task force (JTF-Computer Network Defense) is un-

derfunded and understaffed for the task of managing an actual strategic information warfare attack. It should be given the resources to carry out its current mission and is a logical source of advice to the proposed NHSA Critical Information Technology, Assurance, and Security Office.

National Guard. The National Guard, whose origins are to be found in the state militias authorized by the U.S. Constitution, should play a central role in the response component of a layered defense strategy for homeland security. We therefore recommend the following:

• 6: The Secretary of Defense, at the President's direction, should make homeland security a primary mission of the National Guard, and the Guard should be organized, properly trained, and adequately equipped to undertake that mission.

At present, the Army National Guard is primarily organized and equipped to conduct sustained combat overseas. In this the Guard fulfills a strategic reserve role, augmenting the active military during overseas contingencies. At the same time, the Guard carries out many state-level missions for disaster and humanitarian relief, as well as consequence management. For these, it relies upon the discipline, equipment, and leadership of its combat forces. The National Guard should redistribute resources currently allocated predominantly to preparing for conventional wars overseas to provide greater support to civil authorities in preparing for and responding to disasters, especially emergencies involving weapons of mass destruction.

Such a redistribution should flow from a detailed assessment of force requirements for both theater war and homeland tecurity contingencies. The Department of Defense should conduct such an assessment, with the participation of the state governors and the NHSA Director. In setting requirements, the department should minimize forces with dual missions or reliance on active forces detailed for major theater war. This is because the United States will need to maintain a heightened deterrent and defensive posture against homeland attacks during regional contingencies abroad. The most likely timing of a major terrorist incident will be while the United States is involved in a conflict overseas.[16]

The National Guard is designated as the primary Department of Defense agency for disaster relief. In many cases, the National Guard will respond as a state asset under the control of state governors. While it is appropriate for the National Guard to play the lead military role in managing the consequences of a WMD attack, its capabilities to do so are uneven and in some cases its forces are not adequately structured or equipped. Twenty-two WMD Civil Support Teams, made up of trained and equipped full-time National Guard personnel, will be ready to deploy rapidly, assist local first responders, provide technical advice, and pave the way for additional military help. These teams fill a vital need, but more effort is required.

This Commission recommends that the National Guard be directed to fulfill its historic and Constitutional mission of homeland

[16] See the *Report of the National Defense University Quadrennial Defense Review 2001 Working Group* (Washington, DC: Institute for National Strategic Studies, November 2000), p. 60.

security. It should provide a mobilization base with strong local ties and support. It is already "forward deployed" to achieve this mission and should:

- Participate in and initiate, where necessary, state, local, and regional planning for responding to a WMD incident;
- Train and help organize local first responders;
- Maintain up-to-date inventories of military resources and equipment available in the area on short notice;
- Plan for rapid inter-state support and reinforcement; and
- Develop an overseas capability for international humanitarian assistance and disaster relief.

In this way, the National Guard will become a critical asset for homeland security.

Medical Community. The medical community has critical roles to play in homeland security. Catastrophic acts of terrorism or violence could cause casualties far beyond any imagined heretofore. Most of the American medical system is privately owned and now operates at close to capacity. An incident involving WMD will quickly overwhelm the capacities of local hospitals and emergency management professionals.

In response, the National Security Council, FEMA, and the Department of Health and Human Services have already begun a reassessment of their programs. Research to develop better diagnostic equipment and immune-enhancing drugs is underway, and resources to reinvigorate U.S. epidemiological surveillance capacity have been allocated. Programs to amass and regionally distribute inventories of antibiotics and vaccines have started, and arrangements for mass production of selected pharmaceuticals have been made. The Centers for Disease Control has rapid-response investigative units prepared to deploy and respond to incidents.

These programs will enhance the capacities of the medical community, but the momentum and resources for this effort must be extended. *We recommend that the NHSA Directorate for Emergency Preparedness and Response assess local and federal medical resources to deal with a WMD emergency. It should then specify those medical programs needed to deal with a major national emergency beyond the means of the private sector, and Congress should fund those needs.*

C. EXECUTIVE-LEGISLATIVE COOPERATION

Solving the homeland security challenge is not just an Executive Branch problem. Congress should be an active participant in the development of homeland security programs, as well. Its hearings can help develop the best ideas and solutions. Individual members should develop expertise in homeland security policy and its implementation so that they can fill in policy gaps and provide needed oversight and advice in times of crisis. Most important, using its power of the purse, Congress should ensure that government agencies have sufficient resources and that their programs are coordinated, efficient, and effective.

Congress has already taken important steps. A bipartisan Congressional initiative produced the U.S. effort to deal with the possibility that weapons of mass destruction could "leak" out of a dis-

integrating Soviet Union.[17] It was also a Congressional initiative that established the Domestic Preparedness Program and launched a 120-city program to enhance the capability of federal, state, and local first responders to react effectively in a WMD emergency.[18] Members of Congress from both parties have pushed the Executive Branch to identify and manage the problem more effectively. Congress has also proposed and funded studies and commissions on various aspects of the homeland security problem.[19] But it must do more.

A sound homeland security strategy requires the overhaul of much of the legislative framework for preparedness, response, and national defense programs. Congress designed many of the authorities that support national security and emergency preparedness programs principally for a Cold War environment. The new threat environment—from biological and terrorist attacks to cyber attacks on critical systems—poses vastly different challenges. *We therefore recommend that Congress refurbish the legal foundation for homeland security in response to the new threat environment.*

In particular, Congress should amend, as necessary, key legislative authorities such as the Defense Production Act of 1950 and the Communications Act of 1934, which facilitate homeland security functions and activities.[20] Congress should also encourage the sharing of threat, vulnerability, and incident data between the public and private sectors—including federal agencies, state governments, first responders, and industry.[21] In addition, Congress should monitor and support current efforts to update the international legal framework for communications security issues.[22]

---

[17] Sponsored by Senators Sam Nunn and Richard Luger.

[18] Public Law 104-201, *National Defense Authorization Act for FY 1997: Defense Against Weapons of Mass Destruction.* This legislation, known as the Nunn-Lugar-Domenici Amendment, was passed in July 1996.

[19] We note: the Rumsfeld Commission [*Report of the Commission to Assess the Ballistic Missile Threat to the United States* (Washington, DC: July 15, 1998)]; the Deutch Commission [*Combating Proliferation of Weapons of Mass Destruction* (Washington. DC: July 14, 1999)]; Judge William Webster's Commission [*Report on the Advancement of Federal Law Enforcement* (Washington, DC: January 2000)]; the Bremer Commission [Report of the National Commission on Terrorism, *Countering the Changing Threat of International Terrorism* (Washington, DC: June 2000)]; and an advisory panel led by Virginia Governor James Gilmore [*First Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (Washington, DC: December 15, 1999)].

[20] The Defense Production Act was developed during the Korean War when shortages of critical natural resources such as coal, oil, and gas were prioritized for national defense purposes. [See Defense Production Act of 1950, codified at 50 USC App. § 2061 et seq. Tide I includes delegations to prioritize and allocate goods and services based on national defense needs.] Executive Order 12919, *National Defense Industrial Resources Preparedness,* June 6, 1994, implements Title I of the Defense Production Act. Congressional review should focus on the applicability of the Defense Production Act to homeland security needs, ranging from prevention to restoration activities. Section 706 of the Communications Act of 1934 also needs revision so that it includes the electronic media that have developed in the past two decades. [See 48 Stat. 1104, 47 USC § 606, as amended.] Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* April 3, 1984, followed the breakup of AT&T and attempted to specify anew the prerogatives of the Executive Branch in accordance with the 1934 Act in directing national communications media during a national security emergency. It came before the Internet, however, and does not clearly apply to it.

[21] For more than four years, multiple institutions have called on national leadership to support laws and policies promoting security cooperation through public-private partnerships. See, for example, the President's Commission on Critical Infrastructure Protection, *Critical Foundations, Protecting America's Infrastructures* (Washington, DC: October 1997), pp. 86-88 and *Report of the Defense Science Board Task Force on Information Warfare* (Washington, DC: November 1996).

[22] This includes substantial efforts in multiple forums, such as the Council of Europe and the G8, to fight transnationsl organized crime. See *Communiqué* on principles to fight transnational organized crime, Meeting of the Justice and Interior Ministers of the Eight, December 9-10, 1997.

Beyond that, Congress has some organizational work of its own to do. As things stand today, so many federal agencies are involved with homeland security that it is exceedingly difficult to present federal programs and their resource requirements to the Congress in a coherent way. It is largely because the budget is broken up into so many pieces, for example, that counter-terrorism and information security issues involve nearly *two* dozen Congressional committees and subcommittees. The creation of the National Security Homeland Agency will redress this problem to some extent, but because of its growing urgency and complexity, homeland security will still require a stronger working relationship between the Executive and Legislative Branches. Congress should therefore find ways to address homeland security issues that bridge current jurisdictional boundaries and that create more innovative oversight mechanisms.

There are several ways of achieving this. The Senate's Arms Control Observer Group and its more recent NATO Enlargement Group were two successful examples of more informal Executive-Legislative cooperation on key multi-dimensional issues. Specifically, in the near term, this Commission recommends the following:

• 7: Congress should establish a special body to deal with homeland security issues, as has been done effectively with intelligence oversight. Members should be chosen for their expertise in foreign policy, defense, intelligence, law enforcement, and appropriations. This body should also include members of all relevant Congressional committees as well as ex-officio members from the leadership of both Houses of Congress.

This body should develop a comprehensive understanding of the problem of homeland security, exchange information and viewpoints with the Executive Branch on effective policies and plans, and work with standing committees to develop integrated legislative responses and guidance. Meetings would often be held in closed session so that Members could have access to interagency deliberations and diverging viewpoints, as well as to classified assessments. Such a body would have neither a legislative nor an oversight mandate, and it would not eclipse the authority of any standing committee.

At the same time, Congress needs to systematically review and restructure its committee system, as will be proposod in recommendation 48. A single, select committee in each house of Congress should be given authorization, appropriations, and oversight responsibility for all homeland security activities. When established, these committees would replace the function of the oversight body described in recommendation 7.

In sum, the federal government must address the challenge of homeland security with greater urgency. The United States is not immune to threats posed by weapons of mass destruction or disruption, but neither is it entirely defenseless against them. Much has been done to prevent and defend against such attacks, but these efforts must be incorporated into the nation's overall security strategy, and clear direction must be provided to all departments and agencies. Non-traditional national security agencies that how have greater relevance than they did in the past must be reinvigorated.

Accountability, authority, and responsibility must be more closely aligned within government agencies. An Executive-Legislative consensus is required, as well, to convert strategy and resources into programs and capabilities, and to do so in a way that preserves fundamental freedoms and individual rights.

Most of all, however, the government must reorganize itself for the challenges of this new era, and make the necessary investments to allow an improved organizational structure to work. Through the Commission's proposal for a National Homeland Security Agency, the U.S. government will be able to improve the planning and coordination of federal support to state and local agencies, to rationalize the allocation of resources, to enhance readiness in order to prevent attacks, and to facilitate recovery if prevention fails. Most important, this proposal integrates the problem of homeland security within the broader framework of U.S. national security strategy. In this respect, it differs significantly from issue-specific approaches to the problem, which tend to isolate homeland security away from the larger strategic perspective of which it must be a part.

We are mindful that erecting the operational side of this strategy will take time to achieve. Meanwhile, the threat grows ever more serious. That is all the more reason to start right away on implementing the recommendations put forth here.

A REPORT CARD ON THE DEPARTMENT OF ENERGY'S NONPROLIFERATION PROGRAMS WITH RUSSIA

HOWARD BAKER AND LLOYD CUTLER, CO-CHAIRS, RUSSIA TASK FORCE

THE SECRETARY OF ENERGY ADVISORY BOARD

JANUARY 10, 2001

TASK FORCE MEMBERS

HOWARD BAKER (CO-CHAIR), Baker, Donelson, Bearman & Caldwell, Former United States Senator

LLOYD CUTLER (Co-Chair), Wilmer Cutler & Pickering, Former White House Counsel

GRAHAM T. ALLISON, Director, The Belfer Center, Kennedy School of Government, Harvard University

ANDREW ATHY, Chairman, Secretary of Energy Advisory Board, Partner, O'Neill, Athy & Casey PC

J. BRIAN ATWOOD, Executive Vice President, Citizens Energy, Former Administrator, USAID

DAVID BOREN, President, University of Oklahoma, Former United States Senator from Oklahoma

LYNN DAVIS, Senior Fellow, RAND Corporation

BUTLER DERRICK, Partner, Powell, Goldstein, Frazer & Murphy, LLP, Former Member of Congress from South Carolina

SUSAN EISENHOWER, President, The Eisenhower Institute, Founder, Center for Political and Strategic Studies

LEE HAMILTON, Director, Woodrow Wilson Center, Former Member of Congress from Indiana

ROBERT I. HANFLING, Senior Advisor, Putnam, Hayes and Bartlett

GARY HART,[1] Of Counsel, Coudert Brothers, Former United States Senator from Colorado

DANIEL MAYERS, Of Counsel, Wilmer, Cutler, & Pickering

JIM MCCLURE, McClure, Gerard & Neuenschwander, Inc., Former United States Senator from Idaho

SAM NUNN, Senior Partner, King & Spalding, Former United States Senator from Georgia

ALAN SIMPSON, Director, Institute of Politics, Harvard University, Former United States Senator from Wyoming

[1] Senator Hart has been prevented from full participation in the Task Force's deliberations by other government service.

DAVID SKAGGS, Executive Director, Democracy and Citizenship Program, The Aspen Institute, Former Member of Congress from Colorado

JOHN TUCK, Senior Advisor, Baker, Donelson, Bearman & Caldwell, Former Under Secretary of Energy

A Report Card on the Department of Energy's Nonproliferation Programs with Russia

Executive Summary

INTRODUCTION

Since the breakup of the Soviet Union, we have witnessed the dissolution of an empire having over 40,000 nuclear weapons, over a thousand metric tons of nuclear materials, vast quantities of chemical and biological weapons materials, and thousands of missiles. This Cold War arsenal is spread across 11 time zones and lacks the Cold War infrastructure that provided the control and financing necessary to assure that chains of command remain intact and nuclear weapons and materials remain securely beyond the reach of terrorists and weapons-proliferating states. This problem is compounded by the existence of thousands of weapons scientists who, not always having the resources necessary to adequately care for their families, may be tempted to sell their expertise to countries of proliferation concern.

In order to assess the Department of Energy's part of current U.S. efforts to deal with this critical situation, in February 2000 Secretary of Energy Bill Richardson asked former Senate Majority Leader Howard Baker and former White House Counsel Lloyd Cutler to co-chair a bipartisan task force to review and assess DOE's nonproliferation programs in Russia and to make recommendations for their improvement. After nine months of careful examination of current DOE programs and consideration of related nonproliferation policies and programs of the U.S. Government, the Task Force reached the following conclusions and recommendations.

1. *The most urgent unmet national security threat to the United States today is the danger that weapons of mass destruction or weapons-usable material in Russia could be stolen and sold to terrorists or hostile nation states and used against American troops abroad or citizens at home.*

This threat is a clear and present danger to the international community as well as to American lives and liberties.

2. *Current nonproliferation programs in the Department of Energy the Department of Defense, and related agencies have achieved impressive results thus far, but their limited mandate and funding fall short of what is required to address adequately the threat.*

The Task Force applauds and commends Secretary Richardson, his predecessors and colleagues for their dedication, commitment and hard work in seeking to address this issue. The cooperation of the Russian Federation has also been a critical and significant factor in the work carried out to date.

But the Task Force concludes that the current budget levels are inadequate and the current management of the U.S. Government's response is too diffuse. The Task Force believes that the existing scope and management of the U.S. programs addressing this threat leave an unacceptable risk of failure and the potential for catastrophic consequences.

3. *The new President and leaders of the 107th Congress face the urgent national security challenge of devising an enhanced response proportionate to the threat.*

The enhanced response should include: a net assessment of the threat; a clear achievable mission statement; the development of a strategy with specific goals and measurable objectives; a more centralized command of the financial and human resources required to do the job; and an identification of criteria for measuring the benefits for Russia, the United States, and the entire world.

The Task Force offers one major recommendation to the President and the Congress. The President, in consultation with Congress and in cooperation with the Russian Federation, should quickly formulate a strategic plan to secure and/or neutralize in the next eight to ten years all nuclear weapons-usable material located in Russia and to prevent the outflow from Russia of scientific expertise that could be used for nuclear or other weapons of mass destruction. Accomplishing this task will be regarded by future generations as one of the greatest contributions the United States and Russia can make to their long-term security and that of the entire world.

While emphasizing that enhanced efforts are needed from the U.S., the Task Force underscores that enhanced efforts are also required from Russia. Ultimately, Russia will be responsible for securing its remaining nuclear arsenal. If this program is conceived in full cooperation with the Russian Federation, is adequately financed, and is implemented as part of a growing, open and transparent partnership, then the Task Force believes that Russia should be positioned to take over any work remaining at the end of the eight to ten year period. If Russia is not prepared for such a partnership, then full success will not be achieved.

Bearing this in mind, the Task Force report outlines an enhanced national security program as described above. This program could be carried out for less than one percent of the U.S. defense budget, or up to a total of $30 billion over the next eight to ten years.[1] The Russian Government would, of course, be expected to make a significant contribution commensurate with its own financial ability. The national security benefits to U.S. citizens from securing and/or neutralizing the equivalent of more than 80,000 nuclear weapons and potential nuclear weapons[2] would constitute the

[1] This plan is based on the assumption that both countries will maintain a core nuclear weapons program sufficient to meet defense needs and to provide for naval fuel requirements. A detailed budget for this program would be developed on the basis of the strategic plan called for above. The Task Force believes a budget of approximately $3 billion annually would be appropriate, recognizing that it would not be possible to ramp up to that level immediately. A suggestive outline is attached as Appendix A.

[2] Assuming approximately 4 kg of plutonium or 20 kg of highly enriched uranium per weapon. David Albright, Frans Berkhout and William Walker. "Plutonium and Highly Enriched Uranium 1996: World Inventories, Capabilities and Policies." SIPRI (Oxford Press: 1997), page 8.

highest return on investment in any current U.S. national security and defense program. The new President should press other major powers such as the European Union, Japan and Canada to assume a fair share of the costs of these efforts designed also to enhance the security of these countries. Contributions from other countries could significantly reduce U.S. costs.

BACKGROUND

As two former adversaries adapting to the end of the Cold War, the United States and Russia both have a responsibility to examine and address the dangers posed by the massive nuclear arsenal built up over the past five decades. In Russia, this review must examine the many dangers and challenges posed by the more than 40,000 nuclear weapons produced by the former Soviet Union and the large quantities of highly enriched uranium (HEU) and plutonium that could be used to make more than 40,000 additional nuclear weapons.

Important steps have already been taken with many ambitious milestones being met over the past decade. Former President Bush negotiated and President Clinton implemented what some have called the "contract of the century" with President Yeltsin. Under this agreement, the U.S. is purchasing 500 metric tons of HEU removed from former Soviet nuclear weapons, and this material is being converted to low enriched uranium fuel that is then used in civilian power reactors. To date, more than 110 metric tons of HEU, enough to build some 5,000 nuclear weapons, have been blended down and rendered impotent for nuclear weapons use. In its blended-down form, this material has been delivered to the international market to fuel civilian power reactors. Through close cooperation among the U.S., Russia, and other countries of the former Soviet Union, we have also succeeded in eliminating strategic nuclear arsenals left in Ukraine, Kazakhstan, and Belarus—preventing the potential emergence of three major new nuclear weapon states. The elimination of these arsenals has greatly increased U.S. and international security, particularly since these nuclear weapons were mounted on strategic intercontinental ballistic missiles aimed at the United States.

Since the Nunn-Lugar legislative initiative of 1991,[3] the U.S. Government has established an array of threat reduction programs in both the Departments of Defense and Energy to assist in dismantling Russian nuclear and other weapons of mass destruction and to improve significantly the security of such weapons and materials. Together, these programs have helped to protect, secure, and begin disposition of strategic weapons delivery systems as well as hundreds of metric tons of nuclear weapons-usable material—preventing the emergence of a virtual "Home Depot" for would-be proliferators. Additional work, under the aegis of the Department of State, has addressed what is known as the "brain drain problem" both in Russia and other countries of the former Soviet Union through programs such as the International Science and Technology Center (ISTC) Program. This program, together with DOE's

[3] The Soviet Nuclear Threar Reduction Act of 1991 was created under Public Law Number 102-228.

Initiatives for Proliferation Prevention and its Nuclear Cities Initiative, has helped to redirect weapons scientists and engineers from defense work to civilian employment.

These U.S. programs have reduced the threat of diversion of nuclear weapons materials. To the best of our knowledge, no nuclear weapons or quantity of nuclear weapons-usable material have been successfully stolen and exported, while many efforts to steal weapons-usable material have been intercepted by Russian and international police operations.

Much more remains to be done, however. The Task Force observes that while we know a good deal about the size and state of the Russian weapons complex, there is still much that we do not know. More than 1,000 metric tons of HEU and at least 150 metric tons of weapons-grade plutonium exist in the Russian weapons complex. Most of the cases involving the successful seizure and recovery of stolen nuclear weapons-usable material have occurred on the western border of Russia. The southern border is less secure. Materials may be diverted through centuries old trade routes along Russia's mountainous border. In addition, many of the Russian nuclear sites remain vulnerable to insiders determined to steal enough existing material to make several nuclear weapons and to transport these materials to Iran, Iraq, or Afghanistan. At some sites, one well-placed insider would be enough. The Task Force was advised that buyers from Iraq, Iran and other countries have actively sought nuclear weapons-usable material from Russian sites.

In a worst-case scenario, a nuclear engineer graduate with a grapefruit-sized lump of HEU or an orange-sized lump of plutonium, together with material otherwise readily, available in commercial markets, could fashion a nuclear device that would fit in a van like the one the terrorist Yosif parked in the World Trade Center in 1993. The explosive effects of such a device would destroy every building in the Wall Street financial area and would level lower Manhattan.

In confronting this danger, the Russian Government has recognized that theft of nuclear weapons or nuclear weapons-usable material threatens Moscow or St. Petersburg as surely as it threatens Washington, DC or New York. Chechen terrorists have already threatened to spread radioactive material around Moscow; if they were armed with a nuclear device, the situation would be much worse. Success in countering this threat to both nations rests on a bedrock of shared vital interests.

THE THREAT TODAY

Russia today wrestles with a weakened ability to protect and secure its Cold War legacy. A number of factors have come together to present an immediate risk of theft of potential weapons of mass destruction: delays in payments to guards at nuclear facilities; breakdowns in command structures, including units that control weapons or guard weapons-usable material; and inadequate budgets for protection of stockpiles and laboratories housing thousands of potential nuclear weapons. Such threats are not hypothetical. Consider the following:

- In late 1998, conspirators at a Ministry of Atomic Energy (MinAtom) facility in Chelyabinsk were caught attempting to

steal fissile material of a quantity just short of that needed for one nuclear device. The head of MinAtom's nuclear material accounting confirmed the attempted theft and warned that, had the attempt been successful, it would have caused "significant damage to the Russian State."

- Early in 1998, the mayor of Krasnoyarsk-45, a closed Russian "nuclear city" that stores enough HEU for hundreds of nuclear weapons, wrote to Krasnoyarsk Governor Alexander Lebed warning that a social explosion in his city was unavoidable unless urgent action was taken. Nuclear scientists and other workers in the city remained unpaid for several months, and basic medical supplies could not be purchased. General Lebed, a former National Security Advisor to President Yeltsin, had earlier proposed to Moscow that his region take responsibility for the nuclear forces and facilities on its territory, pay salaries for these military officers and atomic workers, and take command of the structures. The Russian Government has never agreed to the proposal.
- In December 1998, an employee at Russia's premier nuclear weapons laboratory in Sarov (formerly Arzamas-16) was arrested for espionage and charged with attempting to sell documents on nuclear weapons designs to agents of Iraq and Afghanistan for $3 million. The regional head of the Federal Security Bureau, when reporting the case, confirmed that this was not the first case of nuclear theft at Sarov and explained that such thefts were the result of the "very difficult financial position" of workers at such defense enterprises.
- In January 2000, Federal Security Bureau agents arrested four sailors at the nuclear submarine base in Vilyuchinsk-3 on the Kamchatka Peninsula with a stash of precious metals and radioactive material they had stolen from an armored safe in their nuclear submarine. After the sailors' arrest, investigators discovered at their homes additional stashes of stolen radioactive material and submarine components containing gold, platinum, silver, and palladium.

These are a sample of dozens of actual incidents. Imagine if such material were successfully stolen and sold to a terrorist like Osama bin Laden, who reportedly masterminded the bombings of the U.S. embassies in Kenya and Tanzania and is the chief suspect in the recent attack on the U.S. destroyer *Cole.*

Democracies like ours are inherently messy, frequently distracted, and often bogged down in partisanship. Our government historically finds it difficult to mobilize without the catalyst of an actual incident. The new President and leaders of the 107th Congress face no larger challenge than to mobilize the nation to precautionary action before a major disaster strikes.

ASSESSING CURRENT DOE NONPROLIFERATION PROGRAMS

The Task Force had the benefit of briefings by both government and non-government experts and reviews of written materials. Members of the Task Force also visited seven sites in Russia in July 2000, reviewing DOE programs and meeting with 13 organizations over the course of a week. The Task Force was able to visit only a few sites of the vast nuclear complex, and it recognizes that

those sites were probably in better economic and physical condition than others in the complex. The dire state of those sites gave the Task Force members cause for grave concern about the overall condition of the Russian nuclear complex.

The Task Force applauds the accomplishments of current DOE programs and related programs of other U.S. Government agencies. The Task Force commends in particular the dedication to duty exhibited by the hundreds of DOE and national laboratory employees involved in these programs. The Task Force was also impressed by the high quality of cooperation extended by most of DOE's Russian counterparts during the course of its vist to Russia. Both MinAtom and the Russian Navy provided access to all of the facilities requested, as well as some additional sites that were thought to be inaccessible. Despite difficulties in the overall implementation of the DOE programs, the Task Force found Russia's cooperation to be a significant and positive factor. The United States and the Soviet Union competed in creating nuclear weapons of mass destruction; now the U.S. and Russia are cooperating to dismantle them. The Task Force believes that the record of progress demonstrates it is far better for the United States to be on the inside working with Russia than on the outside with no capability to affect Russia's actions.

However, the Task Force finds very disturbing the ongoing Russian trade with Iran in dual-use nuclear technology and missile technology and Russia's apparent intention to supply new conventional weapons systems to Iran. Despite the fact that these issues have been raised with Russia at the highest levels of both governments, the problem has not yet been resolved. The Task Force views the failure to resolve these issues as very serious and believes the lack of satisfactory resolution will increase the difficulties inherent in continued cooperation with Russia and in carrying out the Task Force's recommendations. While the Task Force affirms that the DOE nonproliferation programs are unequivocally in the U.S. national security interest, the Task Force is particularly concerned that if Russian cooperation with Iran continues in a way that compromises nuclear nonproliferation norms, it will inevitably have a major adverse effect on continued cooperation in a wide range of other ongoing nonproliferation programs. Among other consequences, there will be little support in Congress and the Executive Branch for the major new initiatives the Task Force is recommending.

Unquestionably, much has been accomplished by the array of programs now being operated by DOE and other U.S. Government agencies. Nonetheless, the Task Force believes it is time for the U.S. Government to perform a risk assessment based on input from all relevant agencies to estimate the total magnitude of the threat posed to U.S. national secutity. The Task Force also believes there is a strong need to create greater synergies among the existing nonproliferation programs, hence its call for government-wide coordination of the current programs and direct White House involvement.

THE TASK FORCE SPECIFICALLY FINDS

1. By and large, current DOE programs are having a significant and positive effect. The strategic plan recommended by the Task Force should review the needs of each of these programs and, where appropriate, provide for a substantial increase in funding. Expansions of program scope and increases in funding, however, must take careful account of the pace at which funds can usefully be expended in each individual program.

2. The strategic plan and the associated budgets should identify specific goals and measurable objectives for each program, as well as provide criteria for success and an exit strategy. These should be factored into the five-year budget plan currently being developed for the National Nuclear Security Administration.[4]

3. A major obstacle to further expansion and success of current programs is the continuation of differences between the U.S. and Russia over transparency and access. As a condition for a substantially expanded program, the U.S. and Russia should agree at a high level on the degree of transparency needed to assure that U.S.-funded activity has measurable impacts on program objectives and that U.S. taxpayer dollars are being spent as intended.

4. Given the gravity of the existing situation and the nature of the challenge before us, it is imperative that the President establish a high-level leadership position in the White House with responsibility for policy and budget coordination for threat reduction and nonproliferation programs across the U.S. Government. The President should appoint a person of stature who commands the respect and attention of relevant Cabinet officers and Congressional leaders to lead this program.

5. The U.S. administration of these programs should seek to eliminate any unnecessary and overly restrictive controls that hamper swift and efficient action. To overcome potential impediments that often arise from "business as usual" practices within the Russian and U.S. bureaucracies, DOE and related agencies should take practical steps, including further enlargement of the DOE team working with the U.S. Ambassador in Moscow, to ensure the most efficient on-the-ground implementation of the programs in Russia.

6. It is imperative to mobilize the sustained interest and concern of the Congress. The Task Force urges the Congress to consider the creation of a joint committee on weapons of mass destruction, nuclear safety and nonproliferation, modeled after the former Joint Committee on Atomic Energy. Creation of such a committee would ensure that the issues receive adequate high-level attention and that Member and staff expertise is developed and preserved.

ACCOMPLISHING THE TASK

The major recommendation of the Task Force is that one of the first national security initiatives of the new President be the formulation of a comprehensive, integrated strategic plan, done in co-

[4] On March 1, 2000, in accordance with Public Law 106-65, the National Nuclear Security Administration was formally established as a semi-autonomous entity within the Department of Energy. The NNSA is comprised of four preexisting component organizations: defense programs, nuclear nonproliferation, fissile materials disposition, and naval reactors. With the establishment of the NNSA, the Office of Nonproliferation and National Security became Defense Nuclear Nonproliferation and incorporated the Office of Fissile Materials Disposition.

operation with the Russian Federation, to secure and/or neutralize in the next eight to ten years all nuclear weapons-usable material located in Russia and to prevent the outflow from Russia of scientific expertise that could be used for nuclear or other weapons of mass destruction. The Task Force's vision is a world in which all such weapons-usable materials are safe, secure, and accounted for, with transparency sufficient to assure the world that this is the case. The path toward this vision begins by securing all existing nuclear weapons-usable material and eliminating excess stockpiles of uranium and plutonium in Russia.

The Task Force has reviewed many promising proposals but does not claim to have a complete grasp of the universe of good solutions to this set of problems. While it recognizes that the new President will wish to consider other options, the Task Force proposes a strategic plan with specific goals and measurable objectives to eliminate the danger of inadequate controls over weapons of mass destruction and weapons-usable materials. The Task Force recognizes that the quantities of excess material in Russia are so large that they cannot be completely eliminated even within an eight to ten year period. This is especially true of the plutonium stockpile, elimination of which is directly linked to the progress of U.S. efforts to eliminate its own excess plutonium. This plan is designed to bring the material under effective control, to reduce drastically the threat posed by such materials, and to reach a position where Russia can take over any remaining work at the end of the eight to ten year period. Consultation and collaboration with Russia will be critical to success. The proposed strategic plan follows.

1. *Secure Russian nuclear weapons and material* by:

- drastically shrinking the number of sites where the material is held;
- accelerating security upgrades for the remaining buildings in use;
- assisting the Russians as they identify, tag, and seal all their warheads and materials as part of a reliable accounting system;
- securing the return of HEU from Soviet-built research reactors, primarily in Eastern Europe, to Russia for downblending and disposition; and
- developing a plan, after a joint U.S.-Russian examination of the extent of the threat, to be implemented by DOE and DOD, to minimize potential proliferation threats posed by decommissioned Russian general-purpose submarines and their fuel.

2. *Eliminate excess Russian HEU* by:

- demilitarizing all remaining excess Russian HEU through the development of art expanded capacity for downblending in Russia; and
- accelerating the purchase of the approximately 400 metric tons of HEU remaining to be downblended under the current HEU agreement, while ensuring that the material not flood and depress the world market. This could require the Russian or U.S. Government to hold the material for an indefinite period of time.

3. *Manage excess Russian plutonium,* accelerating existing disposition commitments and emphasizing safe and secure storage, by:
   - storing up to 100 metric tons of plutonium at Mayak if additional storage wings are built there, or at other highly secure sites;
   - eliminating up to 100 metric tons of excess Russian plutonium by blending fuel as mixed oxide fuel and burning it in civilian reactors, building on what the U.S. and Russia have agreed to do for an initial 34 metric tons;
   - reinvigorating verifiable efforts to halt additional Russian production of plutonium; and
   - preparing an inventory of the total Russian stockpile.
4. *Downsize the nuclear complex,* building on existing Russian plans and accomplishments, by:
   - facilitating Russian efforts to accelerate the shutdown of its weapons facilities, ensuring the identification of the highest-value targets for cooperation;
   - funding "contract research" by Russian nuclear scientists to develop efficient, low-cost environmental technologies of benefit to the U.S., while simultaneously preventing the outflow of scientific expertise from Russia that could be used for nuclear or other weapons of mass destruction;
   - working with Russia to ensure that nuclear weapons scientists and workers are provided financial incentives for early retirement from the weapons complex;
   - overhauling foreign and domestic lending practices to new businesses in the nuclear cities; and
   - enhancing communication between the municipalities and the weapons institutes or facilities that are co-located with them to increase efficiency in the expenditure of resources.
5. *Plan for Russian financing of sustainable security* by
   - seeking specific commitments from Russia to fund adequate levels of security and accounting for its nuclear material and a slimmed-down nuclear complex;
   - exploring, in consultation with Russian officials, an array of concepts fur developing new revenue streams for financing projects in an accountable and transparent manner; and
   - working with Russian officials to begin detailed planning for the transition away from U.S. financial support.

The Task Force believes it is quite feasible that the Russian Federation and the United States could together carry out an intensive, well-conceived and well-funded strategic plan as outlined above over the next eight to ten years.

U.S. SENATE COMMITTEE ON FOREIGN RELATIONS

HEARING ON

THE THREAT OF BIOTERRORISM AND THE NATURAL SPREAD OF INFECTIOUS DISEASES

SEPTEMBER 5, 2001

Former U.S. Senator Sam Nunn, the former Chair of the Senate Armed Services Committee, continues to play an active role in national security and non-proliferation affairs as the co-chair of the Nuclear Threat Initiative. Senator Nunn recently carried out the duties of the President of the United States in an exercise titled "Dark Winter," which simulated a smallpox attack carried out against three U.S. cities.

Dr. D.A. Henderson, one of the leading experts in the world on bioterrorism, served for 20 years with the Centers for Disease Control, including assignments as Chief of Surveillance and Chief of the Epidemic Intelligence Service; 11 years with the World Health Organization as Director of the successful Smallpox Eradication Program; and 16 years as Chairman of the Pan-American Health Organization's Technical Advisory Group which advised on the design and development of the polio eradication program. Dr. Henderson is now the director of the Johns Hopkins Center for Civilian Biodefense Studies. Dr. Henderson's data formed the technical basis for the "Dark Winter" scenario exercise in which Senator Nunn participated.

PREPARED STATEMENT OF HON. SAM NUNN, FORMER U.S. SENATOR, CO-CHAIRMAN OF THE NUCLEAR THREAT INITIATIVE

Chairman Biden and members of the Committee, it is a privilege and honor for me to come back to the United States Senate where I spent so much of my life. I thank you for dedicating the first of these hearings to the threats of bioterrorism and the spread of infectious diseases. Biological terrorism is one of our greatest national security threats, and one that cannot be addressed by Department of Defense standard operating procedures. The specter of a biological weapons attack—and the parallel peacetime threat of a naturally occurring infectious disease outbreak—are unique, and they deserve the time and focus you are devoting to them today.

Mr. Chairman and members of the Committee, as you may know, this past June at Andrews Air Force Base, I was a participant in the exercise *Dark Winter*—which simulated a biological weapons attack on the United States. It's a lucky thing for the United States that this was just a test and not a real emergency. But, Mr. Chairman and members of the Committee, our lack of preparation *is* a real emergency.

During my 24 years on the Senate Armed Services Committee, I saw scenarios and satellite photos and Pentagon plans for most any category of threat you can imagine. But a biological weapons attack on the United States fits no existing category of security threats. Psychologist Abraham Maslow once wrote: "When all you have is a hammer, everything starts to look like a nail." This is not a nail; it's different from other security threats; and to fight it, we need a different set of tools than the ones we've been using.

Our exercise involved an intentional release of smallpox. Experts today believe that a single case of smallpox anywhere in the world would constitute a global medical emergency. As Members of this committee know, a wave of smallpox was touched off in Yugoslavia in 1972 by a single infected individual. The epidemic was stopped in its fourth wave by quarantines, aggressive police and military measures, and 18 million emergency vaccinations to protect a population of 21 million that was already highly vaccinated.

Mr. Chairman, we have effectively only 12 million doses of vaccine in America to protect a highly vulnerable population of 275 million that is essentially not vaccinated. The Yugoslavia crisis mushroomed from one case; our *Dark Winter* exercise began with 20 confirmed cases in Oklahoma City, 30 suspected cases spread out in Oklahoma, Georgia, and Pennsylvania, and countless more cases of individuals who were infected but didn't know it. We did not know the time, place or size of the release, so we had no way of judging the magnitude of the crisis. All we knew was that we had a big problem and a small range of responses. One certainty was that it would get worse before it would get better. Our medical experts told us that we had only two strategies for effective small-

pox containment: (1) isolating those who are sick, and (2) vaccinating those who have been exposed. Isolation is difficult when you're not sure who has it; vaccination cannot stop the spread if you don't have enough of it.

DARK WINTER OVERVIEW

Dark Winter simulated a series of National Security Council (NSC) meetings dealing with a terrorist attack involving the covert release of smallpox in three American cities. The exercise was conducted by the Center for Strategic and International Studies, the Johns Hopkins Center for Civilian Biodefense Studies, and the ANSER Institute for Homeland Defense, under the leadership of John Hamre, Tara O'Toole and Randy Larsen, respectively. Many of the participants in *Dark Winter* had served previous Presidents in cabinet or sub-cabinet positions. Most knew how the NSC worked, and they were all individuals with considerable expertise and perspective in the security, law enforcement and health fields.

I will not take the Committee's time with a complete replay of the events, but will share with you the highlights.

In the opening minutes of *Dark Winter,* we learned from the Secretary of Health and Human Services that cases of smallpox had just been diagnosed by the Centers for Disease Control. Given the infectious nature of the disease, we were facing the start of a smallpox epidemic—an event with devastating, if not catastrophic, potential.

Like all of you, I received a smallpox vaccination when I was a child, but I had forgotten the honor of the disease. In the 20th century, more than 300 million people died from smallpox—more than those killed in all wars of the century combined. Thanks to a massive and highly collaborative international campaign, smallpox as a naturally occurring disease was eradicated. But once eradicated, the consequences of a smallpox outbreak has become more dangerous with each passing year as new generations of unvaccinated citizens are born and the potency of the previous vaccinations diminishes with time. Unfortunately, we know that smallpox was made into a weapon by the Soviet Union; we do not know if any other nations or groups have successfully pursued a similar goal, and this should be a matter of keen intelligence forces.

Over a 24-hour period at Andrews Air Force Base, our NSC "war gamers" dealt with three weeks of simulated shock, stress and horror. I was given the role of President of the United States, and Jim Woolsey was the Director of the Central Intelligence Agency.

We learned that on December 9, 2002, some dozen patients reported to the Oklahoma City Hospital with a strange illness confirmed quickly by the CDC to be smallpox. While we only knew about the Oklahoma cases the first day, we later learned the scope of the initial infections and the sites of three simultaneous attacks in shopping centers in Oklahoma, Georgia and Pennsylvania. The initial infection quickly spread to five states and 3,000 victims although most infected individuals had not displayed symptoms or gone to the hospital in the first few days so we did not know who they were or where they were.

We quickly learned that we had only two tools available to deal with a smallpox attack—vaccination and isolation, and we had only enough vaccine for one out of every 23 Americans.

I denied the Secretary of Defense's demand that all 2.3 million of U.S. military personnel be immediately vaccinated wherever they were in the world. Instead, we administered vaccine to U.S. military, including the National Guard, and security and medical service personnel who were on the front lines locally and also those who were in areas of the world where a smallpox attack was more likely to occur. Our initial decision was to use our limited vaccine supply to protect health care workers, local police and fire officials, National Guard on the scene and local, state and federal officials in the line of fire. We also devised a strategy to try and put a firewall around the infections that were being reported, but that strategy was largely ineffective because of the rapid spread of the disease and our limited supply of vaccine.

So, on the first night of decision-making, we designed a vaccination strategy, and we ordered accelerated production of new stock. We asked the Secretary of State to try to find surplus stock from other countries. I will skip the agonizing details and get to the conclusions.

On Day Six of the crisis, we had very little vaccine left. We quickly faced the only alternative—forced isolation with large numbers of exposed citizens whose locations and identities remained guesswork. We were down to the really tough questions. Do we force whole communities and cities to stay in their homes? How? With force? Do we physically prevent citizens in high-risk areas from fleeing their communities when they themselves may already be infected? Who provides food and care for those in forced isolation, particularly when we can no longer provide vaccine to essential providers?

On Day Twelve, when our war game ended and my brief tenure as President concluded, we were beginning the next stage of the epidemic—those who caught smallpox from the original 3,000 people who were infected in the initial terrorist attack. Our health experts told us that every two to three weeks the number of cases would increase ten-fold. To give you a glimpse of how the exercise ended, here are a few highlights from a simulated CNN broadcast:

> On Day Twelve of the worst public health crisis in America's history, demonstrations for more vaccine in hard-hit communities disintegrated into riots and looting around the nation. Interstate commerce has stopped in several regions of the nation. A suspension of trading on America's stock exchanges takes effect tomorrow. International commerce with the U.S. has virtually ceased.
>
> The Centers for Disease Control reports that efforts to stem the smallpox epidemic have depleted America's inventory of smallpox vaccine. While the CDC may be out of vaccine, at least 45 Internet websites are offering what they claim are safe, effective vaccines from previously forgotten stocks. These claims have not—repeat not—been independently verified, and authorities urge caution.
>
> At least 25 more states and 10 foreign countries are reporting smallpox infections. At the United Nations, China

has sponsored a resolution to censure the U.S., blaming America for reintroducing smallpox to the world. It is demanding that the U.S. supply the world with vaccine.

In summary, Mr. Chairman, I determined from our war game that public health has become a national security issue, but that we are unprepared. We were out of vaccine. We were discussing martial law. Interstate commerce was eroding rapidly. The members of our simulated NSC, as well as state and local officials, were desperate. We came to realize too late that our country:

- *Had not produced* sufficient vaccine.
- *Had not prepared* top officials to cope with this new type of security crisis.
- *Had not invested* adequately in the planning and exercises absolutely necessary for coordinated response.
- *Had not ensured* that the public health infrastructure was adequate, with built in surge capacity.
- *Had not educated* the American people, or developed strategies to constructively engage the media in educating the public, about what was happening and what to do.
- *Had not practiced* what few plans there were in place.
- *Had not ranked* biological terrorism or infectious diseases as high national priorities.

DILEMMAS AND INSIGHTS

Most participants in our exercise would have been much more in their element if we had been dealing with a terrorist bombing. The effects of a bomb are bounded in time and place. After the explosion, the nation's leadership knows the geography and the extent of the damage. You know where to start, and how much it will take to respond and rebuild. Smallpox, on the other hand, is a silent, ongoing, invisible attack. It is highly contagious, and spreads in a flash—each smallpox victim can infect ten to twenty others. It incubates for two weeks before physically appearing—it comes in waves.

The most insidious effect of a biological weapons attack is that it can turn Americans against Americans. Once smallpox is released, it is not the terrorists anymore who are the threat; our neighbors and family members can become the threat. If they've been exposed, they can kill you by talking to you. The scene could match the horror of the Biblical description in Zechariah (8:10): "Neither was there any peace to him that went out or came in . . . for I set all men every one against his neighbour."

A biological weapons attack cuts across categories and mocks old strategies. For more than two thousand years the most important rule of war has been to know your enemy.

In military language, this means that when you face a battlefield scenario, you draw up an order of battle—you estimate the number of enemy tanks and planes and troops, their intelligence and logistics capabilities, and other resources. A biological weapon, however, is an invisible killer. An attack may go unrecognized for days, only becoming evident after large numbers of people become sick. In the case of a contagious disease, our own people would become the en-

emy's weapons as they transmit the disease to others, creating ever-widening circles of exposure.

Even after you know there has been an attack, there still are few reliable numbers—because you don't know who initially released it, how much more they have, or where they are. And the usual responses to an attack are impossible: "Engage the enemy; open fire; stop their advance; bring out the wounded." You can hardly know who is wounded.

For the participants, this exercise was filled with many such horrible dilemmas and unpleasant insights.

Number one: We have a fragmented and under-funded public health system—at the local, state, and federal levels—that does not allow us to effectively detect and track disease outbreaks in real time.

Two: Lab facilities needed to diagnose the disease are inadequately supported and laboring with outdated technology.

Three: There is insufficient partnership and communication across federal agencies and among local, state, and federal governments.

Four: The only way to deal with smallpox is with isolation and vaccination, but we don't have enough vaccines, and we don't have enough dedicated facilities, resources, or information for effective isolation.

Five: A biological weapons attack will be a local event with national implications, and that guarantees tension between local, state and national interests. In our exercise, Governor Keating of Oklahoma asked for vaccine for every one of his citizens—as he had to in the interests of his state. The President said no, as he had to in the interests of the nation. Naturally, this demands a high degree of advanced planning and coordination, because of the diverging interests, and because key players and partners are answerable to different leaders.

Six: Most hospitals run at or near full capacity all the time: a surge in patients from smallpox, combined with the inevitable infections of hospital personnel, and the flight of some fearful health care professionals, would create a catastrophic overload.

Seven: There will be a dearth of information on this kind of event. My staff and cabinet could not tell me ten percent of what I wanted to know: "How many cases are there right now? How many more cases can we expect? Will there be more attacks? When and where did the first infections take place? Who released it? What's the worst-case scenario? Is our vaccine supply secure and safe for use? Will other countries loan us emergency vaccine to keep the disease from spreading all over the world?

And there are many tradeoffs. One of the biggest: We have 12 million vaccines; that's enough for *one* out of every 23 Americans. How do we decide whom to vaccinate?

Do we take power from the Governors and federalize the National Guard? Do we seize hotels and convert them into hospitals? Do we close borders and block all travel? What level of force do we use to keep someone sick with smallpox in isolation? Do we keep people known or thought to be exposed quarantined in their homes? Do we guarantee 2.3 million doses of vaccine to the military; or do we first cover all health care providers? Do we take

strong measures that protect health, but could undermine public support or destroy the economy?

Finally: How do you talk to the public in a way that is candid, yet prevents panic—knowing that panic itself can be a weapon of mass destruction? My staff had two responses: "We don't know" and "You're late for your press conference."

I told people in the exercise: "I would never go before the press with this little information," and Governor Keating—who knows about dealing with disaster, said: "You have no choice." And I went, even though I did not have answers for the public's most urgent questions: "How do you plan to protect our families?" "How rapidly and how far will it spread?" And "Why isn't there enough vaccine?"

Naturally, there are some skeptics anytime you describe a dire threat to the United States. I want to tell the Committee: I am convinced the threat of a biological weapons attack on the United States is as urgent as it is real. As Secretary Rumsfeld said in his confirmation hearings: "I would rank bioterrorism quite high in terms of threats . . . It does not take a genius to create agents that are enormously powerful, and they can be done in mobile facilities, in small facilities." An experiment some years ago showed that a scientist whose specialty was in another field was able to weaponize anthrax on his first attempt for less than $250,000.

Hundreds of labs and repositories around the world sell biological agents for legitimate research—and the same substances used in legitimate research can be turned into weapons research. In addition, the massive biological weapons program of the former Soviet Union remains a threat, at least to the extent that materials and know-how could flow to hostile forces. At its peak, the program employed 70,000 scientists and technicians and made twenty tons of smallpox. One Russian official was quoted some years ago in *The New Yorker* saying: "There were plenty of opportunities for staff members to walk away with an ampule." There still are.

According to a very prominent press report, former Soviet biological weapons scientists have been aggressively—and in some eases successfully—recruited by Iran. And Ambassador Rolf Ekeus, who headed the United Nations special commission that investigated Iraq's arsenal after the Gulf War, and who we are lucky to have on the Board of Directors of NTI, had testified before Congress that in 1991 Iraq had 300 biological bombs.

So the ability of people to acquire or create biological weapons should be clear beyond any doubt. And no one should doubt how lethal biological weapons could be. In 1979, a small amount of anthrax escaped from a Soviet biological weapons lab in Sverdlovsk. Seventy-seven cases of human anthrax occurred in the city surrounding the lab. Sixty-six died, and new cases were appearing as late as 47 days after the leak. All this resulted from only a tiny amount of anthrax being released—on the order of ounces. It doesn't take much imagination to envision the catastrophe that would result if someone deliberately released a much larger quantity.

It is important not to overstate this threat. But it is not an overstatement to say it is real, it is dangerous, and if it occurred today, it would catch us unprepared.

Michael Osterholm and John Schwartz, in their book *Living Terrors,* told about the experience of one doctor who knew his state was one of the best-trained areas of the country for a biological weapons attack. One day he conducted some unscientific research. He discovered that the total city stockpile for dealing with an anthrax attack would not cover even 600 patients. He found that a doctor trained in biological weapons failed to diagnose anthrax when the classic symptoms were described; a doctor in the radiology department failed to recognize inhalation anthrax when shown an X-ray; and a voice mail message describing a bioterrorism concern went unreturned by the state health department for three days.

NEXT STEPS

In fairness, we are making progress. The Clinton Administration deserves credit for recognizing that a biological weapons attack is different from warfare or other terrorist threats and for targeting funds to address it. That initiative includes strengthening the public health infrastructure, creating a pharmaceutical stockpile for civilian use, a contract to develop and produce a new smallpox vaccine, research to develop new and improved diagnostics, drugs and vaccines, programs to train first responders (police and fire departments as well as public health and medical professionals) across the United States, and investments in new technologies to help detect biological agents.

Under the Bush Administration, these efforts are continuing and in some eases, funding is increasing. It is also heartening that Secretary Thompson has named a senior advisor on bioterrorism who previously directed the program on bioterrorism at the Centers for Disease Control and Prevention. These are positive steps. Still, we have to do more—and quickly.

Before detailing the issues that I believe deserve the greatest attention, we should keep in mind that the results of biological attacks would vary according to the specific agent used. Technology and training for early recognition of the type of pathogen are essential. This exercise gave us valuable lessons about a possible *smallpox* attack. The circumstances would be very different in the case of an anthrax attack, for example. In the event of an attack using anthrax, vaccination and isolation would be irrelevant, but antibiotics would need to be administered on the scene immediately.

For the participants, the *Dark Winter* exercise instilled in all of us that there is much work to be done:

Number one: Clearly, measures that will deter or prevent bioterrorism are the most cost effective means to counter threats to public health and social order. We need to prevent the proliferation of biological weapons, in part by strengthening intelligence gathering against such threats, but also by providing peaceful research options to scientists in the former Soviet Union. Efforts to fight proliferation require a global approach, including finding a way to strengthen and enforce the Biological Weapons Convention.

Two: We need to focus more attention, concern and resources on the specific threat of bioterrorism—understanding that it is different from other threats we face. Biological weapons must be countered with new protocols for securing dangerous pathogens,

with increased vigilance and surveillance, as well as with increased supplies of medicines and vaccines and significantly increased training.

Three: We need to recognize the central role of public health and medicine in this effort and engage these professionals fully as partners on the national security team. We must act on the understanding that public health is an important pillar in our national security framework. In the event of a biological weapons attack—millions of lives will depend on how quickly doctors diagnose the illness, communicate their findings, and bring forth a fast and effective response at the local and federal level. This means, clearly, that public health and medical professionals must be part of the national security team. Planning for an event like this is not the exclusive purview of the Department of Defense, the National Security Council, the CIA and the Department of Energy. The Department of Health and Human Services (CDC, FDA, NIH, etc.) must also be included.

This may seem obvious enough. But several years ago, when Administration officials were meeting to discuss supplemental funding legislation for defense against biological weapons—the presiding official from the Office of Management and Budget greeted the officials from the NSC, and FBI and CIA and DOD, then saw the Assistant Secretary from Health and Human Services at the table, did a double-take and said: "What are you doing here?" Health officials should not need to be given directions to the White House Situation Room in an emergency.

Four: We need to identify and put into practice the mechanisms by which all levels of government will interact and work together. It is critical that we understand our differing roles, responsibilities, capabilities, and authorities, and plan on how we will work together before an act of terrorism occurs.

Five: We need to reexamine and modernize the legal framework for epidemic control measures and the appropriate balance with civil liberties—the laws that would apply if we were to find ourselves managing the crisis that would come with a biological weapons attack. These laws vary from state to state and many are antiquated. We need to make sure that they are up-to-date, consistent with our current social values and priorities, and we need to reacquaint high-level officials in all areas of response with the specific authorities these laws provide, and how they can implement them.

Six: There should be a clear plan for providing the news media with timely and accurate information to help save lives and prevent panic.

Seven: We need to increase the core capacities of our public health system to detect, track and contain epidemics, by providing resources for effective surveillance systems, diagnostic laboratory facilities, and communication links to other elements of the response effort.

Eight: The national pharmaceutical stockpile should be built to capacity, including extra production capability for drugs and vaccines, with heightened security at the various dispersal sites. We must not fall victim to a twin attack that releases a bio-agent and simultaneously destroys our drugs and vaccines.

Nine: We need to develop plans for a surge of patients in the nation's hospitals to make the best use of existing resources in the event of an emergency. This will require careful advance planning, including how to utilize ancillary facilities such as gymnasiums or armories, since most hospitals are operating at or near capacity right now.

Ten: We need to increase funding for biomedical research to develop new vaccines, new therapeutic drugs, and new rapid diagnostic tests for bioweapon agents.

Eleven: We need to encourage the scientific community to confront the sinister potential of modern biological research, and help them devise systems and practices that ensure the safe, secure storage of, and access to, dangerous pathogens.

Twelve: Officials at the highest levels of the federal, state, and local government need to participate in exercises like *Dark Winter* to understand the importance of advance preparation. Plans must be exercised, evaluated, and understood by decision-makers if they are to prove useful in a time of crisis.

I know how difficult it is to find funding for new initiatives, and public health is often left behind. We need to think about supporting public health activities in the same way we think about our national defense. Congress and the public should understand that expanding disease surveillance, creating additional lab capacity and enhancing vaccine production capabilities will benefit the United States not only in responding to a biological weapons attack, but also by improving our responses to natural disease outbreaks. We have a chance to defend the nation against its adversaries and improve the public health system with the same steps.

THE NUCLEAR THREAT INITIATIVE—A NEW FOUNDATION

Mr. Chairman and members of the Committee, encouraging and helping our government to deter, prevent, and defend against biological terrorism is a central part of our mission at the Nuclear Threat Initiative (NTI)—the organization founded by Ted Turner and guided by an experienced board that Ted and I co-chair. We are dedicated to reducing the global threat from biological, nuclear, and chemical weapons by increasing public awareness, encouraging dialogue, catalyzing action, and promoting new thinking about these dangers in this country and abroad.

We fully recognize that only our government can provide the leadership and resources to achieve our security and health priorities. But within that context, NTI is:

- Seeking ways to reduce the threat from biological weapons and their consequences.
- Exploring ways to increase education, awareness and communication among public health experts, medical professionals, and scientists, as well as among policy makers and elected officials—to make sure more and more people understand the nature and scope of the biological weapons threat.
- Considering ways to improve infectious disease surveillance around the globe—including rapid and effective detection, investigation, and response. This is a fundamental defense against any infectious disease threat, whether it occurs naturally or is released deliberately.

- Stimulating and supporting the scientific community in its efforts to limit inappropriate access to dangerous pathogens and to establish standards that will help prevent the development and spread of biological agents as weapons.
- And finally, NTI is searching for ways to help our government and the Russian government to facilitate the conversion of Russian bioweapons facilities and know-how to peaceful purposes, to secure biomaterials for legitimate use or destruction, and to improve security of dangerous pathogens worldwide.

CONCLUDING REMARKS

Mr. Chairman, enemies don't normally attack us where we are strong; they target us where we are weak. Enemies of the United States are not eager to engage us militarily; they saw what happened in Desert Storm. They will attack us where they believe we are vulnerable. Today, we are vulnerable to biological terrorism and those who perpetuate such an act are not likely to be quickly identified or leave a return address. It is critical that we prepare with all possible speed, because if an attack occurs, and succeeds, there will be others. Preparing is deterring.

Our first priority must be prevention. Whether the enemy achieves its objectives in an attack depends, to a large extent, on how the American people respond. Panic is as great a danger as disease. Some will respond like saints—doing whatever they can, exhibiting brave and selfless patriotism—to meet the needs of family and community. Others will respond with panic, perhaps even using violence to obtain vaccines or drugs, or try to protect themselves or their loved ones from exposure. The distance between these two is broad. How most of our citizens will respond will depend largely on what they hear from the President and their elected leaders, and how they see our government respond. This means we must be prepared.

When America faced possible financial panic in March of 1933, President Roosevelt did three things immediately upon taking office: he ordered the banks to close temporarily, he proposed emergency banking legislation, and he explained his plan to the public in the first of his regular national radio broadcasts.

If he had not talked reassuringly to the American people, his plan might not have worked. But if he had talked, and had no plan, his talk would not have been reassuring. In the event of a biological weapons attack, no President, no matter how great his natural gifts, will be able to reassure the public and prevent panic unless we are better prepared than we are right now.

If we are well prepared—with the ability to detect the disease quickly, report it swiftly, and implement the appropriate infection control measures, including the provision of necessary drugs or vaccines for all those who came in contact with it—then the President of the United States will address the American people with knowledge, with courage, and with confidence, and the people will respond in kind. Whether this or a future President will exert this essential leadership will depend in large part on how we all address this issue now.

I commend the Committee for tackling such a difficult but important matter. Our country's protection and safety depend on your leadership. Thank you.

PREPARED STATEMENT OF DR. DONALD A. HENDERSON, MD, MPH

Mr. Chairman, distinguished Members of the Committee, thank you for the opportunity to appear before you today to discuss the realities of the threat posed by biological weapons, our capabilities to secure an early warning of an attack, our potential for response and, finally, measures that might be taken nationally and internationally to lessen the probability of an attack.

It is generally agreed that the 21st century brings with it a new era in the biological sciences with advances in molecular biology and biotechnology that promise longer, healthier lives and the effective control, perhaps elimination of a host of acute and chronic diseases. The prospects are bright but there is a dark side—the possibility that infectious agents might be developed and produced as offensive weapons; that new or emergent infections, like HIV/AIDS, might overwhelm available preventive and therapeutic measures or that laboratory scientists, perhaps inadvertently, might create and release a new and lethal agent. These concerns are as relevant to Europe, to Africa, to Asia as they are to America, In today's world of rapid travel and large migrant populations, epidemic disease, wherever it occurs and of whatever origin, threatens the security of all nations. We are, today, ill-prepared to deal with these challenges.

Throughout the 45 years of my professional career, my principal concern has been the control of infectious diseases both in the United States and abroad. My experience has included 20 years with the Centers for Disease Control, including assignments as Chief of Surveillance and Chief of the Epidemic Intelligence Serve; 11 years with WHO as Director of the Smallpox Eradication Program; and 16 years as Chairman of the Pan-American Health Organization's Technical Advisory Group which counseled PAHO experts on the design and development of the polio eradication program. Enormous strides in epidemic disease control have been made over the past quarter century and more is promised. Four years ago, however, it became apparent to me that these accomplishments and more were jeopardized by the growing threat of biological weapons as well as by new and emergent infections. This led to our founding three years ago of the Hopkins Center for Civilian Biodefense Studies. Our energies are directed ultimately toward preventing biological disasters that potentially could become global in scope, such as epidemic smallpox could readily be and which AIDS is rapidly becoming.

THE THREAT FROM BIOLOGICAL WEAPONS

Nothing in the realm of natural catastrophes or man-made disasters rivals the complex problems of response that would follow a bioweapons attack against a civilian population. The consequence of such an attack would be an epidemic and, in this country, we

have had little experience in coping with epidemics. In fact, no city has had to deal with a truly serious epidemic accompanied by large numbers of cases and deaths since the 1918 influenza epidemic, more than two generations ago.

Senators Hart and Rudman, chairs of the United States Commission on National Security in the Twenty-first Century, singled out bioweapons as perhaps the greatest threat that the U.S. might face in the next century. Admiral Stansfield Turner pointed out that, besides nuclear weapons, the only other weapons with the capacity to take the nation past the "point of non-recovery" are the biological ones.

The Dark Winter scenario dramatizes the catastrophic potential of smallpox as a weapon. It is, of course, not the only possible organism that might be used. In 1993, the Office of Technology Assessment estimated that 100 grams of anthrax released upwind of a large American city—the model being Washington, DC—could cause between 130,000 and 3 million deaths, depending on the weather and other variables. This degree of carnage is in the same range as that forecast for a hydrogen bomb. Although there is legitimate concern as well about the possible use of chemical weapons, they are far less effective pound for pound and extremely difficult to deploy over large areas. Ten grams of anthrax can produce as many casualties as a ton of a chemical nerve agent.

The insidious manner by which a biological attack would unfold is itself alarming. The fact of an attack using an explosive or chemical weapon would be recognized immediately and resources summoned quickly to deal with the consequences and to begin to remediate the situation. A biological agent would, in all probability, be released clandestinely as an aerosol spray, odorless and invisible, which would drift slowly throughout a building or across a city. Not until days to weeks later would people begin to fall ill; new cases would continue to occur over a period of one to several weeks. Some of those exposed, in all likelihood, would be hundreds of miles away when they develop symptoms—in other cities, in other countries. Thus, the consequence of the attack would extend well beyond the immediate area of release.

Biological weapons have not been used since WWII but this is not because of concern that they might not work. The U.S. program was abandoned in 1969 not for technical but for political reasons. As Gradon Carter has pointed out, the utility of bioweapons had been demonstrated by all possible means short of war. By the 1960s, the U.S. knew how to grow and process many microorganisms in a form usable for mass casualty biological weapons. Trials that modeled dispersion of simulant agents as aerosols were conducted in many cities and scores of tests with live biological agents using animals as targets were performed at the Johnson Atoll from 1963 to 1969. There is now no doubt and there was then no doubt, of the capacity of these weapons to cause widespread casualties. A World Health Organization (WHO) analysis, now 30 years old, supported the belief that biological weapons are strategic, population-destroying weapons. Since then, the technology needed to create and disperse these weapons has advanced significantly.

The year 1972 was a significant one in the history of bioweapons. That year, the Biological Weapons Convention was agreed upon,

calling for all signatory countries to cease research on biological weapons and to destroy existing stocks. The Soviet Union and Iraq were both parties to the Convention. The Soviet Union, however, began immediately to greatly expand and modernize its existing biological weapons program and to develop genetically engineered pathogens and other organisms that could serve as strategic weapons. A new organization was created called Biopreparat. Ostensibly a civilian operation, it recruited some of the most capable of Russian biologists. At its peak, it employed over 30,000 persons. There was also a military program of at least 15,000 people and an agricultural program making crop pathogens that employed 10,000 people. The overall complement of staff was equivalent in size to that of its nuclear program. Biopreparat's agenda included the manipulation of viruses and micro-organisms to render them capable of surviving delivery on missile warheads; the development of particularly virulent strains of organisms that are resistant to vaccines and antibiotics; the creation of peptides that could alter moods and heart biorhythms; and the manufacture of tons of anthrax, as well as smallpox virus and antibiotic-resistant strains of plague.

Although the Soviet program was of prodigious size and sophistication, the infrastructure that is actually necessary to make a biological weapon is, in fact, comparatively simple and inexpensive, especially compared to that required to make a nuclear weapon. To make one kilogram of plutonium requires 100 tons of uranium ore; a substantial quantity of specialized equipment; and an enormous facility readily visible from the air. A biological weapon can be produced with the same equipment one uses to produce an ordinary vaccine; it can be readily housed in a building the size of a two-ear garage; nothing on the exterior would identify its use. Moreover, the room and the equipment could be sufficiently cleansed within 24 hours so that no one, on inspection, would be able to determine whether it had been used to make vaccines or biological weapons.

The intelligence agencies have estimated that at least a dozen states possess or are actively seeking an offensive biological weapons capacity. Most of these states are those named by the State Department as sponsors of terrorism. Expertise for operating these facilities is readily available from now poorly funded laboratories of the Russian biological weapons complex. For these countries, biological weapons have a special appeal. They are inexpensive, they occupy little volume, they are readily transportable from place to place and they are capable of being disseminated covertly so that attribution may be impossible.

It is also important to appreciate that the technologies needed to build biological weapons are available in the open literature and on the Internet. This is not knowledge that is limited to a few hundred scientists isolated in a laboratory in the western desert. There are many scientists who have this knowledge and are capable of putting together a biological weapon. Some have argued that preparing a biological weapon is complicated and have been mistakenly reassured by the failure of Aum Shinrikyo's efforts to aerosolize anthrax throughout Tokyo. In fact, although the sect did include some with experience in microbiology, those who actually

worked on the project were not well-trained microbiologists. Nonetheless, they came very close to succeeding.

IMPLICATIONS OF ADVANCES IN BIOTECHNOLOGY

A key reason for being concerned about biological weapons is the remarkable progress now being made in biotechnology and genomics research. Bioscience is moving at a much faster pace than did physics in the 1950s, partly because of computers and the more ready accessibility of knowledge, and partly because of the money that is being invested by large corporations in the biological sciences. In 1998, the U.S. biotechnology industry employed 150,000 people and had a market capitalization of $97 billion with product sales of $13.4 billion. Last April, the Harvard Business Review predicted that the ability to manipulate the genetic codes of living things will dwarf the business transformation propelled by the Internet. Indeed, it is generally acknowledged that the life sciences will be the most important technology of this century.

But, as the understanding of molecular biology increases and as we develop the ability to manipulate cellular processes, we are also creating the tools and knowledge for building more powerful and more diverse weapons. When we discover why a particular virus or bacteria is especially virulent or why it has become resistant to antibiotics, we create an opening for building a new drug or a new vaccine. At the same time, we facilitate the creation of tools needed to build more virulent weapons.

THE EFFECTS OF A BIOLOGICAL WEAPONS ATTACK

The consequences of a biological weapon attack would be an epidemic, most likely following an unannounced attack. In all probability, we would know that something had happened only when people started appearing in the emergency rooms and doctors' offices with strange maladies. Depending on the biological agent and its incubation period, it could be days or weeks after release of the organism before people first became ill. Identification of the cause could be problematical. American physicians today are not trained to diagnose illnesses due to the pathogens thought to be the ones most likely to be used as bioweapons. Few physicians have ever seen cases of anthrax or smallpox or pneumonic plague.

It is difficult to imagine how the public might respond in today's world to a fast-moving lethal epidemic. In recent decades, there have been few such epidemics in industrialized cities. One of the more recent occurred in India in 1994. Plague broke out in the diamond-polishing district of Surat. It was reported by the media as a deadly, mysterious fever, possibly plague. Within hours, panic reigned. People began streaming from the city. Many in the medical community were among the first to leave. Eventually half a million fled, leaving the city a ghost town. It is estimated that India lost some two billion dollars in lost trade, embargoes, and production as a consequence of this outbreak. How many actually died of plague is still not clear but the total was not more than 50.

Epidemics have the potential to spread internationally as we have observed with the HIV/AIDS epidemic. The disease is contagious but it is not easily transmitted from one person to another. Nevertheless, it spread across the globe and is changing the popu-

lation demographics in some African countries to a degree comparable to that caused by the Black Death of the 1300s, which killed a third of the European population.

ADDRESSING THE BIOLOGICAL WEAPONS THREAT

The status of national preparations to deal with bioterrorism is difficult to summarize. The diverse initiatives taken by different agencies of government are not well coordinated, even within the agencies themselves and many have been designed with little comprehension of what is implied for the civilian population when a biological weapon is used. Beginning in 1995, when the first Presidential Decision Directive was issued, preparations to respond to terrorism focussed almost exclusively on training and equipping "first response" teams to counter the effects of a nuclear or conventional explosive device or a chemical attack. Training programs in 120 cities were targeted to include police, fire and emergency rescue personnel in a "lights and sirens" type of response and special full-time units of the National Guard were constituted whose function is not clear but certainly have little to do with bioterrorism.

Not for several years was there a beginning comprehension that the consequences of use of a biological weapon would be an epidemic and that those first detecting its presence and those primarily responsible for controlling the disease would be public health personnel and physicians. Accordingly, in most cities, public health, medical and hospital personnel were not included either in planning or training. Finally, in FY 99, significant funds began to be made available to the Department of Health and Human Services, primarily the Centers for Disease Control (CDC), whose traditional responsibility, with state and local health departments, has been the surveillance and control of infectious diseases. Some two years ago an Office dealing with Bioterrorism was established at CDC; modest funds began to be made available to the states for development of programs both for response and surveillance; stockpiles of antibiotics were procured; smallpox vaccine was ordered; and a national network of laboratories was established that is capable of diagnosing the organisms of principal concern. Unfortunately, little has yet been done to provide for the training of public health and medical professionals and hospitals remain woefully unprepared.

CURRENT VULNERABILITIES

We are today ill-prepared to deal with an epidemic of any sort. There is, as yet, no comprehensive national plan nor an agreed strategy for dealing with the problem of biological weapons. There is little inter-agency coordination at the federal level and nationally funded programs appear to be as often competitive as cooperative. Particularly serious are the vulnerabilities in our medical health care system and our public health infrastructure.

Hospitals

When Americans are seriously ill, they expect to be cared for in hospitals. If the hospitals became overwhelmed and were paralyzed by chaos, it would have serious implications for public morale and for the potential for containing an epidemic, let alone treating

those who were already sick. The likelihood of public anxiety rising to civil disorder would rise substantially.

Hospitals are under serious pressure today. Of the 5000 hospitals in the U.S., 30% are losing money; over the last decade, 1000 have closed because of financial reasons. They face a host of regulatory issues including those dealing with health insurance portability, safer needles, medical and medication error reduction, limits on medical device reuse, ergonomic standards for employees, requirements for patient restraints and seclusion, and many more. At the same time, the numbers of the uninsured are increasing and the population is aging and in need of more medical services. The hospitals have struggled to become ever more efficient but, in their quest to eliminate inefficiencies, they have basically wiped out their surge capacity. Even minor increases in patient demand, such as that of the 1999 brief and mild flu season strained most hospitals.

This lack of elasticity is also seen in the pharmaceutical field as companies have focussed on just-in-time production and delivery. The result is that reserve supplies are few and temporary problems in production are regularly manifested in country-wide spot shortages of such as antibiotics and other critical drugs.

There is an increasing shortage of emergency rooms what with the loss of a thousand hospitals in the past decade and a desire on the part of hospitals to close ERs, if possible, because of their drain on resources. The amount of time that Baltimore's hospitals have been on "diversion" of ambulances because of over crowding has doubled every year for the past three years. Ventilators to aid respiration are in short supply. Baltimore, home to two major medical centers and medical schools, could not handle an acute situation that produced as many as 50 casualties requiring ventilators. A handful of highly contagious patients would cause havoc, there being in the Baltimore-Washington area, no more than 100 beds in negative pressure rooms that could handle highly contagious patients.

However, the most intractable problem for hospitals is likely to be staffing. As we have been told, only half of all nurses work in hospitals and the average age of a nurse in America is 53. More are now retiring than are being recruited to the field. Hospital administrators report that, even if they had more open beds, they doubt that they would have staff to care for the patients.

The Public Health System

The public health system is in even worse shape. Public health is a long-neglected stepchild to modern medicine. It is a sector that has been understaffed and under funded for several decades.

It is believed that, in most states, there is ample authority for public health officials to respond aggressively and effectively to protect the public health. However, many of the relevant laws were written between the time of the Civil War and the 1930s. A more critical problem is knowing what to do and how to do it. With sharp reductions in the number of cases of the major infectious diseases, processes and knowledge about when and how to use quarantine and isolation procedures, how to organize large scale vac-

cination programs and how to communicate effectively with a concerned public have been lost.

A major problem is that there really is no public health "system" for dealing with infectious diseases in this country, but, rather, a fragmented pattern of activities. The federal system, which for the most part is in the federal Centers for Disease Control and Prevention is itself comprised of a number of Centers and activities that are themselves independent fiefdoms. State and local health departments reflect a similar pattern and there is a major disconnect between the public health and medicine. Doctors rarely communicate with local public health officials and often, when they try to do so, they find no one with needed competence. In New York City, a city with one of the best public health departments in the country, the report of two eases of encephalitis to the health department led to the unraveling of the West Nile epidemic. This was a laudable and important response. However, it was later discovered that at the time the first two cases were reported, there were 20 other patients already hospitalized with encephalitis, a clearly recognizable and legally reportable disease.

In most areas, public health is not treated as an emergency service as are police, fire and utilities. The concept of a 24 hour per day, 7 day per week "hot line" is little known. Yet, public health officials will be the ones who will be obliged to organize a response to an epidemic, to communicate with the public and to orchestrate a city and state's response resources

INCREASING PREPAREDNESS

What can be done to diminish our vulnerability to bioweapons.

First, we have got to better prepare our public health and medical care services to respond to outbreaks and epidemics and to mass casualty situations whatever their origin. They are at the core of any response and yet, only recently have they even begun to be involved in the necessary planning and training activities. Significant resources will be required for this purpose, perhaps one billion dollars per year or more. Although a large sum, this would represent less than 10% of government expenditures for counterterrorist activities. This investment, however, would serve a far broader utility than bioterroism alone.

Second, we need to mount a robust research and development program for bio-defense. It would seem logical for this to be a joint DOD-DHHS effort. We need to engage the genius of the universities, the pharmaceutical firms and the biotechnology companies, few of whom are now involved. The bioscience community does not have a history of engagement with defense projects and, by and large, they have not been eager to work with government in this field. For this to happen will require inventive structures and incentives. Three areas of research and development would be especially important: (1) More definitive, rapid, automated means of diagnosing major pathogens, basically building microchips that could identify specific pathogens by deciphering the molecular genomes. (2) Mechanisms for being able to rapidly develop and produce new antibiotics and antiviral drugs for new and emergent diseases. (3) Mechanisms for enhancing the immune response generally, so as to get beyond the one organism-one drug approach.

Third, public health has to identify those critical capacities that are needed to fight epidemics of contagious disease. These include surveillance and reporting systems, particularly the ability to track an epidemic once it occurs. But what we must do, even in normal times, is to track outbreaks once they arc identified. Communications systems that connect health care providers and the public health system are critical.

Fourth, in cooperation with WHO and other countries, we need to strengthen greatly our intelligence gathering capability. A focus on international surveillance and on scientist-to-scientist communication will be necessary if we are to have an early warning about the possible development and production of biological weapons by rogue nations or groups and, likewise, to have the earliest possible warning and longest possible lead time to develop drugs and vaccines to deal with new or emergent organisms.

Fifth, a concerted effort by the medical, public health and, broadly, the biological sciences community to condemn participation in research or development of biological weapons is clearly indicated. Such a response would provide no certain guarantees that misbehavior would not occur but then, there is as yet no other satisfactory deterrent to deal with these troublesome weapons.

SUMMARY

Biological weapons are a significant threat, and because of the rapidly growing power of biotechnology and biological knowledge, the urgency and the diversity of this threat will only increase. The nature of biological weapons and the epidemics that they could create is such that preventing them will be far more challenging than preventing the catastrophic use of chemical or nuclear weapons. It is going to be hard to detect biological weapons production facilities, it is going to be hard to track the weapons before they are used, and it is going to be very hard to interdict them before they are released.

If we do nothing more than strengthen the public health and medical care systems, we can significantly decrease the suffering and death that would follow a bioweapons attack. By being able to mitigate the consequences of such an attack, we can make ourselves less attractive targets to would-be perpetrators. As important, we could improve the everyday functioning of the health care and the public health system for the general good.

REPORT OF THE ACCOUNTABILITY REVIEW BOARDS ON THE EMBASSY BOMBINGS IN NAIROBI AND DAR ES SALAAM

CHAIRMAN: ADMIRAL WILLIAM CROWE, JR.

JANUARY 1999

Report of the Accountability Review Boards

Board Members

Admiral William J. Crowe, *Chairman*

Nairobi Board

Amb. Michael H. Armacost
Amb. Philip C. Wilcox, Jr.
Dr. Janne E. Nolan
Mr. Arthur W. Donahue
Amb. Richard C. Brown—*Executive Secretary*

Dar Es Salaam Board

Amb. Terence A. Todman
Mr. David Busby
Dr. Lynn E. Davis
Mr. Montgomery L. Rogers
Mr. Kenneth R. McKune—*Executive Secretary*

REPORT OF THE ACCOUNTABILITY REVIEW BOARDS ON THE EMBASSY BOMBINGS IN NAIROBI AND DAR ES SALAAM—JANUARY 1999

EXECUTIVE OVERVIEW

The near simultaneous vehicular bombings of the US Embassies in Nairobi, Kenya. and Dar Es Salaam, Tanzania, on August 7, 1998. were terrorist incidents costing the lives of over 220 persons and wounding more than 4,000 others. Twelve American USG employees and family members, and 32 Kenyan and 8 Tanzanian USO employees, were among those killed. Both chanceries withstood collapse from the bombings, but were rendered unusable, and several adjacent buildings were severely damaged or destroyed. In examining the circumstances of these two bombings, the Accountability Review Boards for Nairobi and Dar Es Salaam determined that:

1. The terrorists intended to destroy the chanceries; to kill or injure US Government employees and others in the chanceries; and to damage US prestige, morale, and diplomacy. Thus, according to P.L. 99–399, the incidents were security related.

2. The security systems and procedures for physical security at the embassies in Nairobi and Dar Es Salaam as a general matter met and, in some cases, exceeded the systems and procedures prescribed by the Department of State for posts designated at the medium or low threat levels. However, these standard requirements had not sufficiently anticipated the threat of large vehicular bomb attacks and were inadequate to protect against such attacks.

The Department of State, in fact, does not apply its security standards fully. For far too many* (*Note: Passages here and elsewhere in this document marked with an asterisk (*) indicate more details can be found in the classified version of the report.*) of its overseas facilities it implements them only "to the maximum extent feasible," applying "risk management." For example, neither the chancery in Nairobi nor in Dar Es Salaam met the Department's standard for a 100 ft. (3Om) setback/standoff zone. Both were "existing office buildings" occupied before this standard was adopted; so a general exception was made. The widespread use of such exceptions worldwide with respect to setback and other non-feasible security standards reflects the reality of not having adequate funds to replace all sub-standard buildings within a short period of time. Thus in the interim before Inman buildings could be constructed, exceptions were granted. In light of the August 7 bombings, these general exceptions to the setback requirement in particular mask a dangerous level of exposure to similar attacks elsewhere.

3. The security systems and procedures relating to actions taken at Embassies Nairobi and Dar Es Salaam were, for the most part, properly implemented. In Nairobi, the suicide bomber failed in his

attempt to penetrate the embassy's outer perimeter, thanks to the refusal of local guards to open the gates. In Dar Es Salaam, the suicide bomber likewise failed to penetrate the perimeter, apparently stopped by guards and blocked by an embassy water truck.

However, neither post's Emergency Action Plan anticipated a car bomb scenario. Nor were there explicit Department requirements for dealing with such contingencies in EAP worldwide guidelines, despite clear Inman Report recommendations. While car bombs are often immediately preceded by some types of as was the case in Nairobi, personnel Side embassies are not trained to react properly, nor do perimeter guards have appropriate equipment

4. There was no credible intelligence that provided immediate or tactical warning of the August 7 bombings.

- A number of earlier intelligence reports cited alleged threats against several U.S. diplomatic and other targets, including the embassies in Nairobi and Dar Es Salaam. All of these reports were disseminated to the intelligence community and to appropriate posts abroad, but were largely discounted because of doubts about the sources. Other reporting—while taken seriously—was imprecise, changing and non-specific as to dates, diminishing its usefulness. Additionally, actions taken by intelligence and law enforcement authorities to confront suspect terrorist groups including the Al-Haramayn non-governmental organization and the Usama Bin Laden (UBL) organization in Nairobi, were believed to have dissipated the alleged threats. Indeed, for eight months prior to the August 7 bombings, no further intelligence was produced to warn the embassies in Nairobi and Dar Es Salaam.*
- The Federal Bureau of Investigation (FBI) investigation of the bombings is still underway but, thus far, has uncovered no information indicating that the earlier intelligence reporting could have predicted the time or place of the attacks. Information from FBI and intelligence sources could yet be developed, however, to implicate some of the individuals or groups cited in the earlier intelligence reporting, or more likely, to further amplify understanding of the UBL organization's role in the bombings.

5. The Boards found that both the intelligence and policy communities relied excessively on tactical intelligence to determine the level of potential terrorist threats to posts worldwide. The Inman Report noted and previous experience indicates that terrorist attacks are often not preceded by warning intelligence. The establishment of the Counter Terrorism Center with an inter-agency team of officers has produced tactical intelligence that has enabled the US to thwart a number of terrorist threats.* But we cannot count on having such intelligence to warn us of such attacks.

6. The Boards did not find reasonable cause to believe that any employee of the United States Government or member of the uniformed services was culpable of dereliction of his or her duties in connection with the August 7 bombings. The Boards did find, however, an institutional failure of the Department of State and embassies under its direction to recognize threats posed by transnational terrorism and vehicle bombs worldwide. Policy-mak-

ers and operational officers were remiss in not preparing more comprehensive procedures to guard against massive truck bombs. This combined with lack of resources for building more secure facilities created the ingredients for a deadly disaster. Responsibility for obtaining adequate resources for security programs is widely dispersed throughout the US government as is decision making for determining security policies and procedures. No one person or office is accountable for decisions on security policies, procedures and resources. Ambassadors who are specifically charged with responsibility for the security of US diplomatic personnel assigned to their posts lack adequate authority and resources to carry out this responsibility.

7. The Boards were especially disturbed by the collective failure of the US government over the past decade to provide adequate resources to reduce the vulnerability of US diplomatic missions to terrorist attacks in most countries around the world. Responsibility for this failure can be attributed to several Administrations and their agencies, including the Department of State, the National Security Council, and the Office of Management and Budget, as well as the US Congress.

8. The US response to the August bombings was resourceful and often heroic. However, in the absence of significant training and contingency planning to deal with mass casualties and major destruction from terrorist bombs, the response was occasionally chaotic and marred by a host of planning and logistical failures, especially in the area of military transportation. The Foreign Emergency Support Teams (FESTs) arrived in Nairobi and Dar Es Salaam about 40 hours after the bombings, having experienced delays of 13 hours. There was disjointed liaison between the State Department, as the lead agency, and the Defense Department, FBI and other agencies. The personnel selection of the FESTs was *ad hoc* and not ideal. Medical and other emergency equipment was not always ready and available for shipment.

9. In the wake of these two terrorist acts, the Department of State and other US government organizations focused quickly on the lessons learned. They immediately reviewed the vulnerabilities of our embassies and missions abroad and took steps to strengthen perimeter security at all posts, to re-prioritize the construction and upgrades necessary to bring our overseas US facilities up to what are referred to as "Inman standards," and Congress appropriated over $1 billion in supplemental funds.

10. This is only the first step in what is required to provide for the security of Americans in embassies overseas. We must undertake a comprehensive and long-term strategy for protecting American officials overseas, including sustained funding for enhanced security measures, for long-term costs for increased security personnel, and for a capital building program based on an assessment of requirements to meet the new range of global terrorist threats. This must include substantial budgetary appropriations of approximately $1.4 billion per year maintained over an approximate ten-year period, in addition to savings from the closure of overseas installations where increased capital and security costs outweigh the magnitude of overall US interests. Additional funds for security

must be obtained without diverting funds from our major foreign affairs programs.

Key Recommendations

The 1986 Omnibus Diplomatic and Anti-Terrorism Act established the legal basis for the Accountability Review Board and specifically requires that acts of terrorism against US diplomatic installations abroad, wherein the loss of life or significant property damage occurs, be investigated with a view, among other factors, toward determining whether security systems and procedures were adequate and were implemented. After addressing these issues in this report, the Boards will propose and elaborate on a number. of recommendations aimed at improving security systems and procedures. We provide a listing of the recommendations below.* The bulk of them are necessitated by the use of large vehicular bombs, a threat that has not been fully appreciated in recent years. The first 15 recommendations deal with adjustments in systems and procedures to enhance security of the work place. The final six recommendations address how to improve crisis management systems and procedures. All are directed toward achieving the objective of saving lives. They are urgent and need to be acted upon immediately. No single measure will accomplish the objective but, taken together, they should substantially improve the security for US personnel serving abroad.

Three additional recommendations deal with intelligence and information availability, matters the Boards are also enjoined to address under the law.* (Details and rationale for all of the recommendations are contained in the classified version of the report.)

I. IMPROVING SECURITY SYSTEMS AND PROCEDURES

A. Work Place Security Enhancements

1. Emergency Action Plans for all posts should be revised to provide a "special alarm signal" for Large exterior bombs and duck-and-cover practice drills in order to reduce casualties from vehicular bombs. Special equipment should be provided to perimeter guards.*

2. Given the worldwide threat of transnational terrorism which uses a wide range of lethal weapons, including vehicle bombs, every post should be treated as a potential target and the Department of State's Physical Security Standards and policies should be revised to reflect this new reality.

3. For those US diplomatic buildings abroad not meeting Inman standards, essential physical security upgrades should be made immediately and should include a number of specific measures involving perimeters and counter-surveillance.*

4. The Secretary of State should personally review the security situation of embassy chanceries and other official premises, closing those which are highly vulnerable and threatened but for which adequate security enhancements cannot be provided, and seek new secure premises for permanent use, or temporary occupancy, pending construction of new buildings.

5. Demarches to all governments with whom we have relations should be made regularly to remind them of their obligation to pro-

vide security support for our embassies. For those governments whose police forces need additional training to enable them to provide more adequate protection, the Department should provide training under the Anti-Terrorism Assistance (ATA) program. The Department should also explore ways to provide any necessary equipment to host governments to upgrade their ability to provide adequate protection. Failure by a host government to honor its obligations should trigger an immediate review of whether a post should be closed.

6. The Department of State should radically reformulate and revise the "Composite Threat List" and, as a part of this effort, should create a category exclusively for terrorism with criteria that places more weight on transnational terrorism. Rating the vulnerability of facilities must include factors relating to the physical security environment, as well as certain host governmental and cultural realities.* These criteria need to be reviewed frequently and all elements of the intelligence community should play an active role in formulating the list. The list's name should be changed to reflect its dual purpose of prioritizing resource allocation and establishing security readiness postures.

7. The Department of State should increase the number of posts with full time Regional Security Officers, seeking coverage of as many chanceries as possible. The Department should also work with the Marine Corps to augment the number of Marine Security Guard Detachments to provide coverage to a larger number of US diplomatic missions.

8. The Department of State should provide all Regional Security Officers comprehensive training on terrorism, terrorist methods of operation, explosive devices, explosive effects, and other terrorist weapons to include weapons of mass destruction such as truck bombs, nuclear devices and chemical/biological weapons.*

9. The Department of State should define the role and functions of each of the US embassies abroad for the coming decade with a view toward exploiting technology more fully, improving their efficiency, ensuring their security, and reducing their overall cost. The Department should look specifically at reducing the number of diplomatic missions by establishing regional embassies located in less threatened and vulnerable countries with Ambassadors accredited to several governments.

10. The physical security standards specified in the State Department's Security Standards and Policy Handbook should be reviewed on a priority basis and revised as necessary in light of the August 7 and other large bombings against US installations.

11. When building new chanceries abroad, all US government agencies, with rare exceptions, should be located in the same compound.

12. The Department of State should work within the Administration and with Congress to obtain sufficient funding for capital building programs and for security operations and personnel over the coming decade (estimated at $1.4 billion per year for the next 10 years), while ensuring that this funding should not come at the expense of other critical foreign affairs programs and operations. A failure to do so will jeopardize the security of US personnel abroad

and inhibit America's ability to protect and promote its interests around the world.

13. First and foremost, the Secretary of State should take a personal and active role in carrying out the responsibility of ensuring the security of US diplomatic personnel abroad. It is essential to convey to the entire Department that security is one of the highest priorities. In the process, the Secretary should reexamine the present organizational structure with the objective of clarifying responsibilities, encouraging better coordination, and assuring that a single high-ranking officer is accountable for all protective security matters and has the authority necessary to coordinate on the Secretary's behalf such activities within the Department of State and with all foreign affairs USG agencies.

14. The Department of State should expand its effort to build public support for increased resources for foreign affairs, and to add emphasis on the need to protect US representatives abroad from terrorism, without sacrificing other important foreign policy programs.

15. The Department of State, in coordination with the intelligence community, should advise all posts concerning potential threats of terrorist attacks from the use of chemical, biological or nuclear materials, should establish means of defending against and minimizing the effect of such attacks through security measures and the revision of EAP procedures and exercises, and should provide appropriate equipment, medical supplies, and first responder training.

B. Better Crisis Management Systems and Procedures

1. Crisis management training for mass casualty and mass destruction incidents should be provided to Department of State personnel in Washington to improve Task Force operations to assure a cadre of crisis managers.

2. A revitalized program for on-site crisis management training at posts abroad should be funded, developed, expanded, and maintained.

3. The FEST should create and exercise a team and equipment package configured to assist in post blast crises involving major casualties and physical damage (while maintaining the package now deployed for differing counter terrorism missions). Such a new configuration should include personnel to assist in medical relief, public affairs, engineering and building safety.

4. A modern, reliable, air-refuelable FEST aircraft with enhanced seating and cargo capacity to respond to a variety of counter terrorism and emergency missions should be acquired urgently for the Department of State. Clearly defined arrangements for a backup aircraft are also needed.

5. The Department of State should work closely with the Department of Defense to improve procedures in mobilizing aircraft and adequate crews to provide more rapid, effective assistance in times of emergency, especially in medical evacuations resulting from mass casualty situations. The Department of State should explore as well, chartering commercial aircraft to transport personnel and equipment to emergency sites, if necessary to supplement Department of Defense aircraft.

6. The Department of State should ensure that all posts have emergency communications equipment, basic excavation tools, medical supplies, emergency documents, next of kin records, and other safety equipment stored at secure off-site locations in anticipation of mass destruction of embassy facilities and heavy US casualties.

II. INTELLIGENCE AND INFORMATION

1. In order to enhance the flow of intelligence that relates to terrorism and security, all such intelligence should normally be disseminated to concerned levels of the policy and analytic community; compartmentalization of such information should be limited to extraordinary situations where there is a clear national security need for limited dissemination;

2. The Department of State should assign a qualified official to the DCI's Counter Terrorism Center; and

3. The FBI and the Department of State should consult on ways to improve information sharing on international terrorism to ensure that all relevant information that might have some bearing on threats against or security for US missions or personnel abroad is made available.*

FIRST AND SECOND ANNUAL REPORTS TO THE PRESIDENT AND THE CONGRESS

OF THE

ADVISORY PANEL TO ASSESS DOMESTIC RESPONSE CAPABILITIES FOR TERRORISM INVOLVING WEAPONS OF MASS DESTRUCTION

I. ASSESSING THE THREAT

DECEMBER 1999

II. TOWARD A NATIONAL STRATEGY FOR COMBATING TERRORISM

DECEMBER 2000

PANEL CHAIR AND MEMBERS

PROJECT DIRECTOR: MIKE WERMUTH

Name and Affiliation	Expertise
The Honorable James S. Gilmore, III, Governor of the Commonwealth of Virginia, Chair	State perspective
James Clapper, Jr. (Lieutenant General, U.S. Air Force, Retired), Private Consultant, and Former Director, Defense Intelligence Agency, Vice Chair	Intelligence
L. Paul Bremer, Private Consultant, and Former Ambassador-at-Large for Counter-Terrorism, U.S. Department of State	Terrorism, counterterrorism
Raymond Downey, Commander, Special Operations, City of New York Fire Department	Emergency response—local
George Foresman, Deputy State Coordinator, Department of Emergency Management, Commonwealth of Virginia	Emergency response—state
William Garrison (Major General, U.S. Army, Retired), Private Consultant, and Former Commander, U.S. Army Special Operations Command's Delta Force	Special operations
Ellen M. Gordon, Administrator, Emergency Management Division, Department of Public Defense, State of Iowa, and President, National Emergency Management Association	Emergency response—state
James Greenleaf, Independent Consultant, and Former Associate Deputy for Administration, Federal Bureau of Investigation	Law enforcement—federal
Dr. William Jenaway, Corporate Executive, and Chief of Fire and Rescue Services, King of Prussia, Pennsylvania	Emergency response—local
William Dallas Jones, Director, Office of Emergency Services, State of California	Emergency response—state
Paul M. Maniscalco, Past President, National Association of Emergency Medical Technicians, and Deputy Chief/Paramedic, City of New York Fire Department, EMSC	Emergency response—local
John O. Marsh, Jr., Attorney at Law, and former Secretary of the Army	Interagency coordination and legal aspects
Kathleen O'Brien, City Coordinator, City of Minneapolis, Minnesota	Local perspective

Name and Affiliation	Expertise
M. Patricia Quinlisk, M.D., Medical Director/State Epidemiologist, Department of Public Health, State of Iowa	Health—state
Patrick Ralston, Executive Director, Indiana State Emergency Management Agency; Executive Director, Department of Fire and Building Services; and Executive Director, Public Safety Training Institute, State of Indiana	Emergency response—state
William Reno (Lieutenant General, U.S. Army, Retired), Former Senior Vice President of Operations, American Red Cross	NGOs
Joseph Samuels, Jr., Chief of Police, Richmond, California	Law enforcement—local, terrorism
Kenneth Shine, M.D., President, Institute of Medicine, National Academy of Sciences	Health—federal
Hubert Williams, President, The Police Foundation	Law enforcement and civil liberties
Ellen Embry, U.S. Department of Defense Representative	

FIRST ANNUAL REPORT TO THE PRESIDENT AND THE CONGRESS—ASSESSING THE THREAT

EXECUTIVE SUMMARY

The possibility that terrorists will use "weapons of mass destruction (WMD)"[6] in this country to kill and injure Americans, including those responsible for protecting and saving lives, presents a genuine threat to the United States. As we stand on the threshold of the twenty-first century, the stark reality is that the face and character of terrorism are changing and that previous beliefs about the restraint on terrorist use of chemical, biological, radiological, and nuclear (CBRN) devices may be disappearing. Beyond the potential loss of life and the infliction of wanton casualties, and the structural or environmental damage that might result from such an attack, our civil liberties, our economy, and indeed our democratic ideals could also be threatened. The challenge for the United States is first to deter and, failing that, to be able to detect and interdict terrorists before they strike. Should an attack occur, we must be confident that local, state, and Federal authorities are well prepared to respond and to address the consequences of the entire spectrum of violent acts.

In recent years, efforts have clearly been focused on more preparations for such attacks. The bombings of the World Trade Center in New York and Alfred P. Murrah Federal Building in Oklahoma City, coupled with the 1995 sarin nerve gas attack in Tokyo and the U.S. embassy bombings this past summer, have heightened American concern and have already prompted an array of responses across all levels of government. At the same time, the country's seeming inability to develop and implement a clear, comprehensive, and truly integrated national domestic preparedness strategy means that we may still remain fundamentally incapable of responding effectively to a serious terrorist attack.

The vast array of CBRN weapons conceivably available to terrorists today can be used against humans, animals, crops, the environment, and physical structures in many different ways. The complexity of these CBRN terrorist threats, and the variety of contingencies and critical responses that they suggest, requires us to ensure that preparedness efforts are carefully planned, implemented, and sustained among all potential responders, with all levels of government operating as partners. These threats, moreover, will require new ways of thinking throughout the entire spectrum of local, state, and Federal agencies. Effecting true change in the cul-

[6] For reasons of clarity and precision, the report uses the term CBRN (chemical, biological, radiological, and nuclear) terrorism, in preference to the more commonly used, yet potentially misleading term, "weapons of mass destruction" or WMD.

ture of a single government agency, much less achieving fundamental changes throughout and among all three, presents formidable hurdles. Nonetheless, the nature of these threats and their potential consequences demands the full commitment of officials at all levels to achieve these goals. Indeed, the need to ensure that a strategic national vision regarding domestic preparedness is in place, so that the country is better able to counter these threats and to respond effectively to the challenges that they present, is among the reasons that this congressionally mandated Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction was established.

The enabling legislation[7] directs the Panel to assess Federal efforts to enhance domestic preparedness, the progress of Federal training programs for local emergency responses, and deficiencies in Federal programs for response to terrorist incidents involving WMD; to recommend strategies for ensuring effective coordination of Federal agency response efforts and for ensuring fully effective local response capabilities for WMD terrorism incidents; and to assess appropriate state and local funding for response to WMD terrorism.[8]

To meet those objectives, the Panel determined that it must first understand the full range of potential CBRN threats from terrorists, based on the belief that without a fundamental understanding of the threats, preparedness efforts by Federal, state, and local entities could be misguided, uncoordinated, and wasteful.

The Panel's analysis of such threats points out that CBRN terrorism has emerged as a U.S. national security concern for several reasons:

- There has been a trend toward increased lethality in terrorism in the past decade.
- There is an increasing focus on the apparent dangers posed by potential CBRN terrorism.
- Terrorists may now feel less constrained to use a CBRN device in an attempt to cause mass casualties, especially following the precedent-setting attack in 1995 by the Aum Shinrikyo.

The reasons terrorists may perpetrate a WMD attack include a desire to kill as many people as possible as a means "to annihilate their enemies," to instill fear and panic to undermine a governmental regime, to create a means of negotiating from a position of unsurpassed strength, or to cause great social and economic impact.

Given any of those potential motives, the report identifies the "most likely terrorists groups" to use CBRN as fundamentalist or apocalyptic religious organizations, cults, and extreme single-issue groups but suggests that such a group may resort to a smaller-scale attack to achieve its goal. The analysis, however, indicates two additional possibilities:

- A terrorist attack against an agricultural base.

---

[7] Section 1405 of the National Defense Authorization Act for Fiscal Year 1999, Public Law 105–261 (HR. 3616. 105th Congress, 2nd Session) (October 17, 1998).

[8] For purposes of the Panel's activities and recommendations, it has included the state level within the scope of its mandate.

- A terrorist use of a CBRN device with the assistance of state sponsorship.

In the latter case, nevertheless, the Panel concludes that several reasons work against state sponsorship, including the prospect of significant reprisals by the United States against the state sponsor, the potential inability of the state sponsor to control its surrogate, and the prospect that the surrogate cannot be trusted, even to the point of using the weapon against its sponsor.

The Panel concludes that the Nation must be prepared for the entire spectrum of potential terrorist threats—both the unprecedented higher-consequence attack, as well as the historically more frequent, lesser-consequence terrorist attack, which the Panel believes is more likely in the near term. Conventional explosives, traditionally a favorite tool of the terrorist, will likely remain the terrorist weapon of choice in the near term as well. Whether smaller-scale CBRN or conventional, any such lower-consequence event—at least in terms of casualties or destruction—could, nevertheless, accomplish one or more terrorist objectives: exhausting response capabilities, instilling fear, undermining government credibility, or provoking an overreaction by the government. With that in mind, the Panel's report urges a more balanced approach, so that not only higher-consequence scenarios will be considered, but that increasing attention must now also be paid to the historically more frequent, more probable, lesser-consequence attack, especially in terms of policy implications for budget priorities or the allocation of other resources, to optimize local response capabilities. A singular focus on preparing for an event potentially affecting thousands or tens of thousands may result in a smaller, but nevertheless lethal attack involving dozens failing to receive an appropriate response in the first critical minutes and hours.

While noting that the technology currently exists that would allow terrorists to produce one of several lethal CBRN weapons, the report also describes the current difficulties in acquiring or developing and in maintaining, handling, testing, transporting, and delivering a device that truly has the capability to cause "mass casualties." Those difficulties include the requirement, in almost all cases, for highly knowledgeable personnel, significant financial resources, obtainable but fairly sophisticated production facilities and equipment, quality control and testing, and special handling. In many cases, the personnel of a terrorist organization run high personal safety risks, in producing, handling, testing, and delivering such a device. Moreover, the report notes, the more sophisticated a device, or the more personnel, equipment, facilities, and the like involved, the greater the risk that the enterprise will expose itself to detection and interdiction by intelligence and law enforcement agencies—particularly in light of the increasing attention focused on terrorism today.

The report explains, with some specificity, the challenges involved in each of the four device or agent topic areas—biological, chemical, nuclear, and radiological—which suggests that some public pronouncements and media depictions about the ease with which terrorists might wreak genuine mass destruction or inflict widespread casualties do not always reflect the significant hurdles currently confronting any nonstate entity seeking to employ such

weapons. The report acknowledges, nevertheless, that the situation now facing a terrorist could change dramatically because of new discoveries, further advances in technology, or other material factors. No matter how difficult or improbable such higher-consequence incidents may be, prudence requires that appropriate steps be taken across the broad spectrum of terrorist threats to deter, prevent, or interdict a terrorist attack before it occurs or failing that, to respond in a way that will—first and foremost—minimize human casualties and also mitigate damage to property and to the environment.

Part of the report focuses on the 1995 Aum Shinrikyo nerve gas attack on the Tokyo subway, which marked the first time that a nonstate group had used a chemical weapon against civilians. The conventional wisdom—that terrorists were not interested in killing, but rather in publicity, or were concerned about a loss of popular support or international recognition—has increasingly been called into question, not only by the Aum event but also by others, such as the World Trade Center and Oklahoma City bombings.

Nevertheless, Chapter Three, which chronicles Aum's attempts to develop a variety of lethal agents or devices, indicates that, despite Aum's considerable resources and the superior technical expertise and state-of-the-art equipment and facilities at its disposal, the group could not effect a truly successful chemical or biological attack. The lesson of Aum is that any nonstate entity faces organizational and significant technological difficulties and other hurdles in attempting to weaponize and deliver chemical and biological weapons, arguably providing a refutation of the suggestion voiced with increasing frequency about the ease with which such weapons can be made and used.

The report contains several conclusions and recommendations, as a result of the threat analysis and other information provided to the Panel and the collective expertise and experience of its members:

- The conclusion that the United States needs to have a viable national strategy to guide the development of clear, comprehensive, and truly integrated national domestic preparedness plans to combat terrorism, one that recognizes that the Federal role will be defined by the nature and severity of the incident but will generally be supportive of state and local authorities, who traditionally have the fundamental responsibility for response, and the recommendation for promulgation of a national-level strategy, with a "bottom-up" perspective—a strategy that clearly delineates and distinguishes Federal, state, and local roles and responsibilities and articulates clear direction for Federal priorities and programs to support local responders;[9] and a comprehensive, parallel public education effort.

[9] The Panel has chosen to use "local responders"—as opposed to "first responders"—to characterize those persons and entities that are most likely to be involved in the early stages following a terrorist attack. That characterization includes not only law enforcement, fire services, emergency medical technicians, emergency management personnel, and others who may be required to respond to the "scene" of an incident, but also other medical and public health personnel who may be required to provide their services in the immediate aftermath of an attack.

- The conclusion that initial and continuing, comprehensive and articulate assessments of potential, credible, terrorist threats within the United States, and the ensuing risk and vulnerability assessments are critical for policymakers and the recommendation that more attention be paid to assessments of the higher-probability/lower-consequence threats—not at the expense of, but in addition to, assessments of the lower-probability/higher-consequence threats.
- The conclusion that the complex nature of current Federal organizations and programs makes it very difficult for state and local authorities to obtain Federal information, assistance, funding, and support; that a Federal focal point and "clearinghouse" for related preparedness information and for directing state and local entities to appropriate Federal agencies, is needed; and that the concept behind the National Domestic Preparedness Office is fundamentally sound.
- The conclusion that congressional decisions for authority and funding to address the issue appear to be uncoordinated, and the recommendation that Congress consider forming an *ad hoc* Joint Special or Select Committee, to provide more efficiency and effectiveness in Federal efforts.
- The conclusion that much more needs to be and can be done to obtain and share information on potential terrorist threats at all levels of government, to provide more effective deterrence, prevention, interdiction, or response, using modern information technology.
- The conclusion that many definitions and terms in this arena are ambiguous or confusing (e.g., "weapons of mass destruction" and "mass casualties"), and the recommendation that there be a revision and codification of universal and easily understood terms.
- The conclusion that national standards for responders at all levels, particularly for planning, training, and equipment, are critical, and the recommendation that more emphasis be placed on research, development, testing, and evaluation in the adoption of such standards.
- The conclusion that, despite recent improvements, too much ambiguity remains about the issue of "who's in charge" if an incident occurs, and the recommendation that efforts be accelerated to develop and to test agreed-on templates for command and control under a wide variety of terrorist threat scenarios.

The report concludes with an overview of the activities of the Panel being undertaken in the current fiscal year:

- A comprehensive review of related Federal programs, placing emphasis on training; communications; equipment; planning requirements; the needs of maritime regions; coordination among the various levels of government; the effectiveness of the structure of military organizations for responses across a broad spectrum of potential threats; and research, development, testing, and evaluation.
- A survey of local and state emergency management and response officials to elicit their views on the efficacy of current Federal programs, particularly in the areas of training, equip-

ment, planning, communications, and Federal agency coordination among the various levels of government.

- Interviews with a number of related Federal, state, and local officials to obtain more detailed information on their views of current Federal programs and activities and their specific proposals or recommendations to improve or enhance Federal efforts.
- Case studies of jurisdictions where such events have occurred or have been threatened, to review and analyze lessons learned from the full range of elements and issues involved in each specific plan or actual response.
- An analysis of the status of existing or the development of appropriate standards in the areas of training for responders at all levels, equipment, notification procedures, communications, and planning.
- Consideration of cyber terrorism issue in the future work of the Panel.

SECOND ANNUAL REPORT TO THE PRESIDENT AND THE CONGRESS—TOWARD A NATIONAL STRATEGY FOR COMBATING TERRORISM

EXECUTIVE SUMMARY

We have been fortunate as a nation. The terrorist incidents in this country—however tragic—have occurred so rarely that the foundations of our society or our form of government have not been threatened. Nevertheless, the potential for terrorist attacks inside the borders of the United States is a serious emerging threat. There is no guarantee that our comparatively secure domestic sanctuary will always remain so. Because the stakes are so high, our nation's leaders must take seriously the possibility of an escalation of terrorist violence against the homeland.

The continuing challenge for the United States is first to deter and, failing that, to detect and interdict terrorists before they strike. Should an attack occur, local, State, and Federal authorities must be prepared to respond and mitigate the consequences of the attack.

To prepare to manage the consequences of such attacks effectively, the United States needs changes in the relationships among all levels of government. Our ability to respond cannot depend on a single level or agency of government. Rather we need a national approach, one that recognizes the unique individual skills that communities, States, and the Federal government possess and that, collectively, will give us the "total package" needed to address all aspects of terrorism.

The Advisory Panel produced a comprehensive assessment, in its first report, of the terrorist threat. The Panel stands by its conclusions from one year ago.

In its second year, the Advisory Panel shifted its emphasis from threat assessment to broad program assessment. The Advisory Panel addressed specific programs for combating terrorism and larger questions of national strategy and Federal organization. While the Advisory Panel found much to commend, it also found problems at all levels of government and in virtually every functional discipline relevant to combating terrorism. The Panel believes these problems are particularly acute at high levels of the Federal Executive Branch. Hence, the present report highlights the related issues of national strategy and Federal organization, and recommends solutions for these and other problems.

Finding 1: The United States has no coherent, functional national strategy for combating terrorism.

The United States needs a functional, coherent national strategy for domestic preparedness against terrorism. The nation has a

loosely coupled set of plans and specific programs that aim, individually, to achieve certain specific preparedness objectives. The Executive Branch portrays as its strategy a compilation of broad policy statements, and various plans and programs already under way. Many programs have resulted from specific Congressional earmarks in various appropriations bills and did not originate in Executive Branch budget requests; they are the initiatives of activist legislators. Although Federal agencies are administering programs assigned to them, the Executive Branch has not articulated a broad functional national strategy that would synchronize the existing programs and identify future program priorities needed to achieve national objectives for domestic preparedness for terrorism. Given the structure of our national government, only the Executive Branch can produce such a national strategy.

Recommendation 1: The next President should develop and present to the Congress a national strategy for combating terrorism within one year of assuming office.

A national strategy is a high-level statement of national objectives coupled logically to a statement of the means that will be used to achieve these objectives. In a coherent strategy, program details are analytically derived from the statement of goals. The next Administration should begin a process of developing a national strategy by a thoughtful articulation of national goals, encompassing deterrence, prevention, preparedness, and response.

Ends. The first step in developing a coherent national strategy is for the Executive Branch to define a meaningful, measurable expression of what it is trying to achieve in combating terrorism. To date, the Federal government's goals have been expressed primarily in terms of program execution. Rather, the national strategy must express goals in terms of the "end state" toward which the program strives. Since there exists no ready-made measure of a country's preparedness for terrorism (especially domestically), the Executive Branch must develop objective measurements for its program to combat terrorism, to track its progress, to determine priorities and appropriate funding levels, and to know when the desired "end state" has been achieved.

Means. With meaningful objectives, logical priorities and appropriate policy prescriptions can be developed. That is the essence of any coherent strategy. Setting priorities is essential and can only be done after specific objectives have been clearly defined. For instance, should the nation seek a higher level of preparedness for its large urban centers than for its rural areas and, if so, how much higher? In the broad area of terrorism preparedness, what should be the relative importance of preparing for conventional terrorism, radiological incidents, chemical weapons, or biological weapons? With respect to biological weapons, which pathogens deserve priority? What priority and commensurate resources need to be devoted to defending against cyber attacks? A proper national strategy will provide a clear answer to these and many other questions. With these answers in hand it will be possible to design and manage an appropriate set of programs. The country is at a disadvantage, of course, in that a large number of programs have already

been established and may have to be reconfigured—an inevitable consequence of their *ad hoc* origins.

ESSENTIAL CHARACTERISTICS OF A COMPREHENSIVE FUNCTIONAL STRATEGY FOR COMBATING TERRORISM

- National in scope, not just Federal.
- Appropriately resourced and based on measurable performance objectives.
- Focused on the full range of deterrence, prevention, preparedness, and response across the spectrum of threats—domestic and international.
- For domestic programs, built on requirements from and fully coordinated with relevant local, State, and Federal authorities.

Finding 2: The organization of the Federal government's programs for combating terrorism is fragmented, uncoordinated, and politically unaccountable.

The lack of a national strategy results in part from the fragmentation of Executive Branch programs for combating terrorism. These programs cross an extraordinary number of jurisdictions and substantive domains: national security, law enforcement, intelligence, emergency management, fire protection, public health, medical care, as well as parts of the private sector.

No one, at any level, is "in charge" of all relevant capabilities, most of which are not dedicated exclusively to combating terrorism. The lack of a national strategy is inextricably linked to the fact that no entity has the authority to direct all of the entities that may be engaged. At the Federal level, no entity has the authority even to direct the coordination of relevant Federal efforts.

Recommendation 2: The next President should establish a National Office for Combating Terrorism in the Executive Office of the President, and should seek a statutory basis for this office.

The office should have a broad and comprehensive scope, with responsibility for the full range of deterring, preventing, preparing for, and responding to international as well as domestic terrorism. The director of this office should be the principal spokesman of the Executive Branch on all matters related to Federal programs for combating terrorism and should be appointed by the President and confirmed by the Senate. The office should have a substantial and professional staff, drawn from existing National Security Council offices and other relevant agencies. It should have at least five major sections, each headed by an Assistant Director:

1. Domestic Preparedness Programs
2. Intelligence
3. Health and Medical Programs
4. Research, Development, Test, and Evaluation (RDT&E), and National Standards
5. Management and Budget

The National Office for Combating Terrorism should exercise program and budget authority over Federal efforts to combat ter-

rorism. It should have the authority to conduct a review of Federal agency programs and budgets to ensure compliance with the priorities established in the national strategy, as well as the elimination of conflicts and unnecessary duplication among agencies. The National Office should administer a budget certification/decertification process with the authority to determine whether an agency's budget complies with the national strategy and to appeal ultimately to the President to resolve disputes.

In addition to developing and overseeing the national strategy, the National Office for Combating Terrorism should oversee terrorism-related intelligence activities. The office should coordinate Federal programs designed to assist response entities at the local and State levels, especially for planning, training, exercises, and equipment. The office should provide direction and priorities for research and development, and related test and evaluation (RDT&E) for combating terrorism, as well as for developing nationally recognized standards for equipment and laboratory protocols and techniques. It should coordinate programs designed to enhance the capabilities of and coordination among the various health and medical entities at all levels.

The National Office for Combating Terrorism should not be an operational entity in the sense of exerting direct control over Federal assets in operations to combat terrorism.

Finally, the director of the National Office should establish an Advisory Board for Domestic Programs to assist in providing broad strategic guidance and to serve as part of the approval process for the domestic portion of strategy, plans, and programs of the National Office for Combating Terrorism. This board should be composed of one or more sitting State governors, mayors of several U.S. cities, the heads of several major professional organizations, and nationally recognized subject matter experts in combating terrorism, in addition to senior representatives of the major Federal entities that have responsibility for combating terrorism. The President and the Congress should each appoint members to this board.

Finding 3: The Congress shares responsibility for the inadequate coordination of programs to combat terrorism.

The Congress's strong interest in, and commitment to, U.S. efforts to combat terrorism is readily apparent. The Congress took the initiative in 1995 to improve the nation's domestic preparedness against terrorism. But the Congress has also contributed to the Executive Branch's problems. Over the past five years, there have been a half-dozen Congressional attempts to reorganize the Executive Branch's efforts to combat terrorism, all of which failed. None enjoyed the support of the Executive Branch. At least 11 full committees in the Senate and 14 full committees in the House—as well as their numerous subcommittees—claim oversight or some responsibility for various U.S. programs for combating terrorism. Earmarks in appropriations bills created many of the Federal government's specific domestic preparedness programs without authorizing legislation or oversight. The rapidly growing U.S. budget for combating terrorism is now laced with such earmarks, which have

proliferated in the absence of an Executive Branch strategy. The Executive Branch cannot successfully coordinate its programs for combating terrorism alone. Congress must better organize itself and exercise much greater discipline.

Recommendation 3: The Congress should consolidate its authority over programs for combating terrorism into a Special Committee for Combating Terrorism—either a joint committee between the Houses or separate committees in each House—and Congressional leadership should instruct all other committees to respect the authority of this new committee and to conform strictly to authorizing legislation.

The creation of a new joint committee or separate committees in each House is necessary to improve the nation's efforts to fight terrorism. The committee should have a substantial standing staff. The new National Office for Combating Terrorism must establish a close working relationship with the committee, and propose comprehensive and coherent programs and budget requests in support of the new national strategy. The new joint or separate committee should have the authority to dispose of the Executive Branch request and to oversee the execution of programs that it authorizes. For this to work, other Congressional authorizing committees with an interest in programs for combating terrorism must recognize the concurrent, consolidated authority of the joint or separate committee; and relevant appropriations committees must exercise restraint and respect the authorizing legislation of the new structure. We recognize that this task is no less daunting than the Executive Branch reorganization that we propose above, but it is no less needed.

Finding 4: The Executive Branch and the Congress have not paid sufficient attention to State and local capabilities for combating terrorism and have not devoted sufficient resources to augment these capabilities to enhance the preparedness of the nation as a whole.

The foundation of the nation's domestic preparedness for terrorism is the network of emergency response capabilities and disaster management systems provided by State and local governments. "Local" response personnel—community and State law enforcement officers, firefighters, emergency medical technicians, hospital emergency personnel, public health officials, and emergency managers—will be the "first responders" to virtually any terrorist attack anywhere in the nation. Federal resources may not arrive for many hours—if not days—after the attack. A disproportionately small amount of the total funds appropriated for combating terrorism is being allocated to provide direct or indirect assistance to State and local response efforts. This level of Federal funding for non-Federal capabilities is not commensurate with the importance that State and local capabilities will have in any operational response to a major terrorist attack inside our borders.

Any coherent national strategy for combating terrorism domestically must recognize the critical need to build on the nation's exist-

ing emergency response and management systems for the pragmatic reasons of viability and cost-effectiveness.

Recommendation 4: The Executive Branch should establish a strong institutional mechanism for ensuring the participation of high-level State and local officials in the development and implementation of a national strategy for terrorism preparedness.

To be consistent with the Federal structure of our government, the President should work in closer partnership with State and local governments as they collectively strive to achieve higher levels of domestic preparedness for terrorism. The domestic portion of a national strategy for combating terrorism should emphasize programs and initiatives that build appropriately on existing State and local capabilities for other emergencies and disasters. The Executive Branch, therefore, should develop the national strategy in close partnership with high-level State and local officials drawn from key professional communities: elected officials, law enforcement, fire protection, emergency medical technicians, public health officials, hospital medical care providers, and emergency managers. State and local officials should, in particular, have substantial responsibility for the detailed design and oversight of the Federal training, equipment, and exercise programs. The Advisory Board for Domestic Programs, proposed earlier, should provide advice for these functions, augmented as necessary by State and local representatives assigned to the National Office for Combating Terrorism.

Finding 5: Federal programs for domestic preparedness to combat terrorism lack clear priorities and are deficient in numerous specific areas.

We have a number of recommendations about selected aspects of current U.S. programs for domestic preparedness to combat terrorism. The lack of clear priorities is an obvious byproduct of the lack of a strategy. Thus, many of our specific recommendations reflect criticisms that are subordinate to our macro-critique that the United States lacks a coherent national strategy. We recognize the problem of offering detailed programmatic recommendations in advance of a national strategy. Through its deliberations, the Advisory Panel has, nevertheless, reached consensus on a number of specific findings and recommendations, summarized below and detailed in the full report.

Specific Functional Recommendations: Our focus continues to be on the needs of local and State response entities. "Local" response entities—law enforcement, fire service, emergency medical technicians, hospital emergency personnel, public health officials, and emergency managers—will *always* be the "first response," and conceivably the only response. When entities at various levels of government are engaged, the responsibilities of all entities and lines of authority must be clear.

1. *Collecting Intelligence, Assessing Threats, and Sharing Information.* The National Office for Combating Terrorism should foster

the development of a consolidated all-source analysis and assessment capability that would provide various response entities as well as policymakers with continuing analysis of potential threats and broad threat assessment input into the development of the annual national strategy. That capability should be augmented by improved human intelligence collection abroad, more effective domestic activities with a thorough review of various Federal guidelines, and reasonable restrictions on acquisition of CBRN precursors or equipment. The National Office should also foster enhancements in measurement and signature intelligence, forensics, and indications and warning capabilities. To promote the broadest possible dissemination of useful, timely (and if necessary, classified) information, the National Office should also oversee the development and implementation of a protected, Internet-based single-source web page system, linking appropriate sources of information and databases on combating terrorism across all relevant functional disciplines.

2. *Operational Coordination.* The National Office for Combating Terrorism should encourage Governors to designate State emergency management entities as domestic preparedness focal points for coordination with the Federal government. The National Office should identify and promote the establishment of single-source, "all hazards" planning documents, standardized Incident Command and Unified Command Systems, and other model programs for use in the full range of emergency contingencies, including terrorism. Adherence to these systems should become a requirement of Federal preparedness assistance.

3. *Training, Equipping, and Exercising.* The National Office for Combating Terrorism should develop and manage a comprehensive national plan for Federal assistance to State and local agencies for training and equipment and the conduct of exercises, including the promulgation of standards in each area. The National Office should consult closely with State and local stakeholders in the development of this national plan. Federal resources to support the plan should be allocated according to the goals and objectives specified in the national strategy, with State and local entities also providing resources to support its implementation.

4. *Health and Medical Considerations.* The National Office for Combating Terrorism should reevaluate the current U.S. approach to providing public health and medical care in response to acts of terrorism, especially possible mass casualty incidents and most particularly bioterrorism. The key issues are insufficient education and training in terrorism-related subjects, minimum capabilities in surge capacity and in treatment facilities, and clear standards and protocols for laboratories and other activities, and vaccine programs. A robust public health infrastructure is necessary to ensure an effective response to terrorist attacks, especially those involving biologic agents. After consultation with public health and medical care entities, the National Office should oversee the establishment of financial incentives coupled with standards and certification requirements that will, over time, encourage the health and medical sector to build and maintain required capabilities. In addition, Federal, State, and local governments should clarify legal and regu-

latory authorities for quarantine, vaccinations, and other prescriptive measures.

5. *Research and Development, and National Standards.* The National Office for Combating Terrorism should establish a clear set of priorities for research and development for combating terrorism, including long-range programs. Priorities for targeted research should be responder personnel protective equipment; medical surveillance, identification, and forensics; improved sensor and rapid readout capability; vaccines and antidotes; and communications interoperability. The National Office must also coordinate the development of nationally recognized standards for equipment, training, and laboratory protocols and techniques, with the ultimate objective being official certification.

6. *Providing Cyber Security Against Terrorism.* Cyber attacks inside the United States could have "mass disruptive," even if not "mass destructive" or "mass casualty" consequences. During the coming year, the Advisory Panel will focus on specific aspects of critical infrastructure protection (CIP), as they relate to the potential for terrorist attacks. In our discussions thus far, we have identified several areas for further deliberation, including CIP policy oversight; standards; alert, warning, and response; liability and other legal issues, and CIP research. We will make specific policy recommendations in our next report.