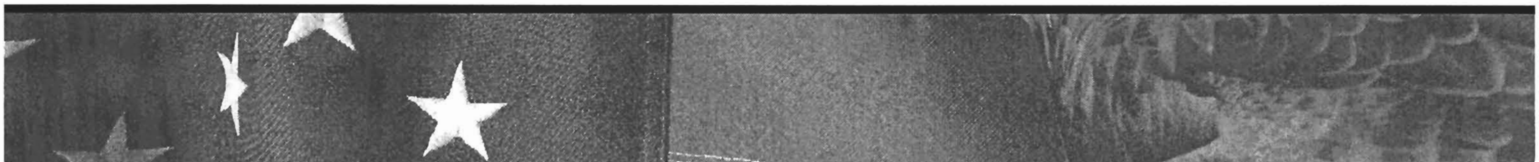
America at Risk:
The State of Homeland Security

Initial Findings



January 2004

Prepared by the Democratic Members of the
House Select Committee on Homeland Security
Jim Turner, Ranking Member

Democratic Members of the House Select Committee on Homeland Security

Jim Turner, Texas
  Ranking Member
Bennie G. Thompson, Mississippi
  Ranking Member, Subcommittee on Emergency Preparedness and Response
Loretta T. Sanchez, California
  Ranking Member, Subcommittee on Infrastructure and Border Security
Louise M. Slaughter, New York
  Ranking Member, Subcommittee on Rules
Zoe Lofgren, California
  Ranking Member, Subcommittee on Cybersecurity, Science, and Research & Development
Karen McCarthy, Missouri
  Ranking Member, Subcommittee on Intelligence and Counterterrorism
Edward J. Markey, Massachusetts
Norman D. Dicks, Washington
Barney Frank, Massachusetts
Jane Harman, California
Benjamin L. Cardin, Maryland
Peter A. DeFazio, Oregon
Nita M. Lowey, New York
Robert E. Andrews, New Jersey
Eleanor Holmes Norton, District of Columbia
Sheila Jackson-Lee, Texas
Bill Pascrell, Jr., New Jersey
Donna M. Christensen, U.S. Virgin Islands
Bob Etheridge, North Carolina
Charles A. Gonzalez, Texas
Ken Lucas, Kentucky
James R. Langevin, Rhode Island
Kendrick B. Meek, Florida

America at Risk: The State of Homeland Security

INITIAL FINDINGS

Over two years since the tragedy of September 11, 2001, and approaching the first anniversary of the largest government overhaul over 50 years, the United States remains vulnerable to terrorist attack.

While the Bush Administration is correct to claim that we are safer now than we were on September 11, this standard sets the bar far too low. The key question is whether we are as safe as we need to be in light of the threats we face. The answer is, unfortunately—no. Gaps in our homeland security continue to exist, and the Bush Administration is not moving fast enough, and is not taking strong enough action, to effectively close them.

Al-Qaeda continues to seek ways to kill our citizens, destroy property and infrastructure, disrupt our economy, and demoralize our nation. Our enemies are opportunistic, and will remain fixated on identifying and exploiting our weaknesses. We must remain vigilant in bolstering our homeland defenses as rapidly and effectively as we can to protect ourselves from any possible terrorist attack.

The men and women who patrol our borders, inspect cargo at our ports, analyze intelligence, and respond to emergencies, are setting the standard for excellence, but they are not receiving the leadership or support they deserve. Although the Department of Homeland Security (DHS) has been in existence for almost a year, our national homeland security efforts continue to be woefully inadequate.

In September 2003, Democrats on the House Select Committee on Homeland Security laid out a comprehensive strategy to close the security gaps that are facing America. We will build on that strategy next month by publishing a report detailing how the Bush Administration has failed to take sufficiently aggressive action to protect the homeland, and will introduce solutions to our country's most pressing homeland security problems. Today, we are outlining the initial findings of this report. These findings identify key areas where the United States remains vulnerable, and highlight reasons why current approaches for solving our security problems are not working.

We must be alert in identifying our security gaps, inventive in determining the most effective way to overcome them, and diligent in ensuring that such gaps never exist again. Our nation deserves nothing less.

HOMELAND SECURITY INTELLIGENCE

SECURITY GAP:

- In December 2002, the Congressional Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001 (Joint Inquiry) stated that the U.S. government was unable to prevent the al-Qaeda attacks due to failures in collecting intelligence, assembling and analyzing the information that was collected, placing suspected terrorists on watch lists, understanding the terrorist threat as it related to specific U.S. security vulnerabilities, and sharing information across government agencies and with state and local authorities.
- Congress created the Information Analysis and Infrastructure Protection (IAIP) Directorate of DHS to address these failures by analyzing intelligence related to the terrorist threat and matching threats to specific homeland vulnerabilities, providing threat and vulnerability assessments to guide all DHS activities, sharing information with state and local officials to improve prevention measures, and issuing terrorist threat alerts.

FAILURE TO CLOSE THE GAP:

- The President requested and Congress approved funds for 692 employees for IAIP for this year. As of January 9, 2004, only 36% of that total had been hired.
- Despite a legal mandate, DHS has not yet established clear, consistent procedures for sharing terrorist information with state and local officials. In a recent Government Accounting Office (GAO) survey, only 13% of federal officials and 35% of state officials believed that the sharing of terrorism information between federal, state, and local officials was effective.
- According to Robert Liscouski, DHS Assistant Secretary for Infrastructure Protection, a comprehensive terrorist threat and vulnerability assessment is unlikely to be completed within the next five years.
- The Bush Administration created a new Terrorist Screening Center (TSC) to manage an integrated watch list containing records on those suspected of being involved in terrorism. However,
    - According to the Administration, "initial capabilities of the TSC [are] limited." Currently, the TSC does not have a comprehensive terrorist watch list, sufficient personnel, or full authority to use watch list information held by other agencies.
    - Less than 20% of the government's records on suspected terrorists have been integrated into the TSC's watch list.
    - Other federal agencies are not yet working with the TSC as intended. The TSC was not involved in checks run against passenger lists on Air France

and other airlines that led to cancelled and delayed flights during the most recent Orange Alert.

NUCLEAR MATERIAL STOCKPILES

SECURITY GAP:

- DHS has warned that al-Qaeda remains focused on obtaining, producing, or stealing nuclear materials. The Central Intelligence Agency (CIA) has also stated that one of al-Qaeda's end goals remains the use of a nuclear weapon to cause mass casualties.
- When the Soviet Union dissolved 12 years ago, it left behind enough enriched uranium and plutonium to make 60,000 nuclear warheads. Much of this material is unguarded and unaccounted for.
- The International Atomic Energy Agency has reported that there have already been 18 thefts worldwide involving highly enriched uranium and plutonium, which can be used to make a nuclear bomb.
- The threat posed by unsecured nuclear materials extends far beyond Russia and the states of the former Soviet Union. Some 20 tons of highly enriched uranium exists at 130 civilian research facilities in 40 countries, many of which are stored in conditions leaving them vulnerable to terrorists, or determined criminals who could sell the material to terrorist groups. The amount of this material needed to make a nuclear weapon is measured in kilograms – far less than one ton.

FAILURE TO CLOSE THE GAP:

- No single senior official within the U.S. government is responsible, and therefore could be held accountable for, the coordination and ultimate success of multiple American programs designed to prevent nuclear materials from falling into the hands of terrorists. According to former Assistant Secretary of Defense Graham Allison, "(w)ere the President today to ask his cabinet who is responsible for preventing nuclear terrorism, either a dozen people would raise their hands, or no one would."
- Funding for the "Nunn-Lugar" Cooperative Threat Reduction Programs—the principal U.S. government efforts to secure loose nuclear material worldwide—has remained relatively flat over the last several years at about $1 billion annually. In 2001, a bi-partisan expert commission led by former senator Howard Baker and Lloyd Cutler stated that the pace of efforts was inadequate, and that support for U.S. nuclear security activities should be tripled.
- Removal of nuclear material from the most vulnerable sites outside of the former Soviet Union has been occurring at the rate of one site every four years. At such a pace, it would take almost 100 years to remove such dangerous material at remaining high risk facilities worldwide.

AVIATION SECURITY

SECURITY GAP:

- On December 21, 2003, Secretary of Homeland Security Tom Ridge justified the recent increase in the national threat level, saying "Recent reporting reiterates that al-Qaeda continues to consider using aircraft as a weapon. And they are evaluating procedures both here and abroad to find gaps in our security posture that can be exploited."
- The Transportation Security Administration (TSA) has spent more than $10 billion on passenger and baggage screening since its inception in November 2001, but numerous and well-publicized reports show that dangerous items are still getting aboard airlines.
- 2.8 million tons of cargo flies on passenger planes annually, affecting roughly half of all airplanes. This cargo, which ranges from envelope size to hundreds of pounds, is not routinely screened and subject to only loose industry responsibility.
- Thousands of airport employees and vendors have access to sensitive airport areas and airplanes without being required to go through the routine electronic screening used for passengers and flight crews.
- The Congressional Research Service (CRS) estimates that 25-30 non-state groups, including al-Qaeda, are believed to possess 5,000 to 150,000 shoulder-fired missiles. One man attempted to smuggle a missile into the United States with the intention to sell it to terrorist groups, and some of these missiles have been fired at aircraft overseas. U.S. passenger planes have no defense against these readily available weapons.

FAILURE TO CLOSE THE GAP:

- Undercover investigations have been conducted by TSA, the DHS Inspector General, and the GAO to determine how well TSA screeners are finding weapons on passengers and in baggage. All three investigations have determined that prohibited items are still passing through TSA screening check points. Comparisons with similar investigations conducted before TSA started its screening operations show that much improvement is still needed.
- Even though Nathaniel Heatwole e-mailed TSA specifics on what he was doing, Heatwole was able to bring weapons onto six separate flights. In two cases, the weapons he brought onboard remained hidden for more than 30 days.
- TSA admits that at least five major airports are not fully screening baggage electronically. Other means of security are used, such as making sure that bags are only loaded on the plane if the passenger is on board, but this provides absolutely no security against suicide attacks.

- TSA announced an inspection program for air cargo in November, 2003, but inspections are conducted on a random basis by shippers and freight forwarders. TSA plans to identify and electronically screen 100% of high-risk cargo, but this will not be done until at least 2005, and TSA has no experience to date with classifying cargo by risk. Further, TSA will not have a fully developed database of companies authorized to ship cargo on aircraft until the end of this fiscal year.
- DHS has initiated a $120 million technology development program for airplane missile defense systems. However, this program will provide no defenses to aircraft for several years.

BORDER SECURITY

SECURITY GAP:

- All 19 of the 9/11 hijackers entered the United States through official ports-of-entry; at least three of them entered with valid visas, but remained in the United States beyond the terms of their stay. DHS estimates that at least 2.3 million visitors in the United States have overstayed their visas.
- Over a two-year period, the U.S. Border Patrol apprehended over 2 million people for illegally entering the United States; yet, there are approximately 7 million illegal aliens residing in the United States.
- The United States shares a 5,525-mile border with Canada and a 1,989-mile border with Mexico. Extensive portions of these borders have no physical security, are not regularly patrolled, and are devoid of any electronic monitoring or aerial surveillance.
- There is only one Border Patrol agent for every 11 miles of our northern border. Even with five Border Patrol agents per mile on our southern border, illegal migrants routinely cross into the United States from Mexico.
- Over 440 million people legally entered the United States through one of over 300 ports-of-entry in Fiscal Year 2002 (FY02). Approximately 80% of all inspections are conducted at land ports-of-entry, 17% at air and 3% at sea ports-of-entry. The United States does not currently screen foreign visitors against all databases of known and suspected terrorists.
- There over 200 versions of legitimate state-issued identification cards and over 50,000 legitimate versions of birth certificates issued in the United States. U.S. citizens re-entering the country are randomly inspected and only required to present some form of valid identification, which presents terrorists with opportunities to use counterfeit documents to gain entry to the United States.
- Significant travel and commerce passes through our borders and could be hindered by even small delays in the inspections process. $1.4 trillion in imports and $974 billion in exports passed through our ports-of-entry in FY02, with an estimated 11 million containers crossing our land borders each year. The peak

wait time at the Blaine Peace Arch port-of-entry in Washington state could increase by more than 11 hours if the average inspection time increased by just nine seconds, according to the GAO.

FAILURE TO CLOSE THE SECURITY GAP:

- The US-VISIT system has potential, but is not currently an effective counter-terrorism tool:
    - US-VISIT screens fewer than 10% of all foreign visitors.
    - The Administration is not implementing US-VISIT where it would make the biggest impact. US-VISIT is in place at 115 airports and 14 of 42 seaports, but is not working at any land ports-of-entry where 80% of all inspections take place.
    - Fewer than 25% of embassies and consulates are equipped to screen visa applicants through US-VISIT.
    - Visitors from 27 countries whose nationals do not require a visa to enter the United States are currently exempt from US-VISIT. Thus, US-VISIT would not have subjected Zacarias Mousaoui, a French citizen, and Richard Reid, a British citizen, to its heightened inspection process. The Administration extended for one year a congressional deadline in the USA PATRIOT Act for these "visa waiver" countries to present machine-readable passports upon entering the United States.
    - US-VISIT cannot effectively screen foreign visitors at ports-of-entry against a comprehensive terrorist database;
    - An internal memorandum suggests that US-VISIT operations may be suspended for some travelers when wait times at airports are considered to be excessive.
- The Administration has failed to put enough law enforcement staff on the border.
    - Despite DHS' recent announcement that 1,000 agents are now deployed on the northern border, this was only accomplished by removing several hundred agents from the southern border which potentially reduces security along the U.S.-Mexico frontier.
    - The 2001 USA PATRIOT Act and the Enhanced Border Security and Visa Entry Reform Act of 2002 required the Administration to hire thousands of new agents to secure the northern border. To date, the overall staffing requirements have not been achieved.
    - More than two years after the 9/11 attacks, the Administration has failed to produce a comprehensive, long-term border staffing strategy.
- The U.S. entry process is vulnerable to terrorist exploitation because a wide range of documents, which have no security features, are accepted as positive identification at ports-of-entry. Unreliable forms of identification are also accepted in many states to obtain valid drivers licenses, which are then used to cross U.S. borders.

- Inspection times are likely to increase due to shortfalls in border infrastructure, thereby increasing pressures on security and hindering commerce. Our land ports-of-entry are not well equipped to handle any growth in travel or the expanded inspections process. For example, 64 ports have less than 25% of required space for the federal inspections process, and some ports lack any land for expansion. No survey has been done to determine how much space may be needed to collect exit data through US-VISIT.

PORT SECURITY

SECURITY GAP:

- The U.S. Intelligence Community assesses that our country is more likely to be attacked with a weapon of mass destruction delivered by a ship, truck, or airplane than by a ballistic missile. A weapon of mass destruction detonated in a container or at a seaport could cause tremendous numbers of casualties, and an estimated economic loss ranging from $58 billion to $1 trillion.
- Over 90% of the world's trade moves in cargo containers. Six million containers enter U.S. seaports, annually. There is no comprehensive system deployed to screen those containers for radiological or nuclear materials.
- In 2001, 5,400 vessels made 60,000 port calls to American ports. Currently there is no system in place to track vessels entering the United States.
- The Interagency Commission on Crime and Security at Seaports has concluded that security at ports is "poor to fair and in few cases good," citing a lack of standards for physical, procedural, and personnel security. The Federal Bureau of Investigation (FBI) considers ports to be highly vulnerable to terrorist attacks.
- The U.S. Coast Guard fleet of cutters is older than 39 of 41 of the world's major naval fleets and its personnel strength is several times smaller than it was in World War II.

FAILURE TO CLOSE THE GAP:

- To counter the threat of terrorists using cargo containers to facilitate attacks, the Bush Administration has increased scrutiny of high risk containers, launched the Container Security Initiative (CSI), which sends inspection teams to foreign ports, and initiated the Customs Trade Partnership Against Terrorism (C-TPAT), which requires the private sector to enhance security in exchange for quicker processing of shipments. However:
  - o While U.S. Customs and Border Patrol (CBP) claims that 100% of high risk cargo is inspected, the GAO has determined that the cargo manifest data used to identify which containers require heightened scrutiny is "one of the least reliable or useful for targeting purposes."
  - o High-risk cargo at many seaports is not inspected with radiation detection portals, which are most capable of detecting a nuclear or radiological weapon. Such

portals have been deployed at only a few American ports. Other equipment on site at seaports such as hand held radiation pagers and VACIS machines are not designed to detect nuclear or radiological weapons in cargo containers.
  - CSI personnel are temporarily stationed overseas for only 120 days which is not enough time to develop relationships with foreign customs services required to enhance targeting information.
  - Only 100 of the 4,500 C-TPAT participants have had their security practices verified, leaving thousands of companies receiving the benefit of reduced inspections without demonstrating progress on security.
- The Administration has not deployed a long range vessel tracking system capable of locating and monitoring suspicious vessels.
- The Administration has issued regulations setting standards for physical, procedural, and personnel security at ports and the Coast Guard estimates that ports will need to spend $1.1 billion dollars over the next year to comply with the regulations. Although Congress provided some grant funds for ports to use to enhance security, the Administration has not included any such grant funding in its budget since 9/11.
- Despite its increased homeland security duties, under current budget trends, the Coast Guard will not replace its aging cutters and aircraft as part of Project Deepwater until 2022. Also, the additional resources the Coast Guard has received since 9/11 do little to increase its personnel strength.

CRITICAL INFRASTRUCTURE PROTECTION

SECURITY GAP:

- Taped messages from Osama bin Laden have stated that, "The youths of God are preparing [to] fill your hearts with terror and target your economic lifeline." While 9/11 seriously damaged the airline industry, overseas al-Qaeda targets have included oil interests, tourism targets, and banks—critical infrastructures that could be attacked within the United States.
- While the United States has not suffered a terrorist attack since 9/11, the number of critical infrastructure targets in the U.S. is nearly endless:
  - At over 7,000 U.S. chemical facilities, a toxic release could threaten in excess of 10,000 people;
  - Millions of rail and truck cars carrying dangerous chemicals around the country every day are potential bombs on wheels;
  - The massive blackout in the United States in August 2003, while not terrorism related, demonstrated serious vulnerabilities in our electricity sector;
  - There have been credible threats of airplane attacks against nuclear facilities;

- Millions of citizens are potential targets every day at concentrated points like bridges, tunnels, and subway stations as well as at large buildings and public entertainment venues.

- While 85% of critical infrastructure is owned by the private sector, the federal government has a constitutional responsibility to provide for the common defense.

FAILURE TO CLOSE THE GAP:

- According to the Brookings Institution, the Administration "largely ignores" major private-sector critical infrastructure, "current efforts fall woefully short," and "specific policy steps are now overdue."
- Testimony before the House Select Committee on Homeland Security gave DHS "not a passing grade" on critical infrastructure protection. A number of former senior national security officials and senior state-level homeland security officials have given the Administration's Critical Infrastructure Protection efforts grades ranging from "a gentleman's C" to a "D" to "absent."
- According to the GAO, the Administration has failed to 1) define "the roles, responsibilities, and relationships among key CIP organizations, including state and local governments and the private sector," 2) indicate "timeframes or milestones for… accomplishing specific actions," and 3) establish "performance measures for which entities can be held responsible."
- While the Homeland Security Act of 2002 requires the DHS to carry out a comprehensive risk assessment of critical infrastructures, the Administration has made little progress. The Assistant Secretary for Infrastructure Protection "would be surprised, frankly, if we had that done in the next five years."
- DHS testified that it would complete a plan for a comprehensive risk assessment by December 2003. However, the White House's recently released Homeland Security Presidential Directive 7 gives the DHS yet another year to develop a 'plan' to develop a 'strategy' to identify, prioritize, and protect critical infrastructures. The Directive is an admission by the Administration that the DHS is not getting the job done.

CHEMICAL PLANT SECURITY

SECURITY GAP:

- The United States is home to over 66,000 chemical production and storage facilities spread throughout our cities, towns, and rural areas.
- In 2001, the Army Surgeon General suggested that an attack on a chemical plant in a densely populated area could result in up to 2.4 million casualties.
- A terrorist attack causing a massive breach of chemical containment at any one of 123 facilities in the United States could threaten over one million people.

- The Department of Justice has described the threat to chemical plants as "both real and credible" and potentially more dangerous than an attack on a nuclear power plant.
- In November 2003, *60 Minutes* reported unlocked gates, absent guards, dilapidated fences, and unprotected tanks filled with deadly chemicals at dozens of facilities in major metropolitan areas, including Chicago, Houston, New York, Los Angeles, and Baltimore.
- In the Pittsburgh area, one reporter found easy access to over 200 tons of corrosive chlorine gas at four different sites.

FAILURE TO CLOSE THE GAP:

- Over a year ago, Secretary Ridge and former Environmental Protection Agency (EPA) Administrator Christine Todd Whitman stated that "voluntary efforts alone are not sufficient to provide the level of assurance Americans deserve" and chemical facilities "must be required to take steps" to improve security.
- The industry itself has called for "oversight, inspection, and strong enforcement authority at DHS to ensure that facilities are secure against the threat of terrorism."
- Today, the industry remains self regulated. Chemical facilities are not required to assess their own vulnerabilities or safeguard their facilities from attack. A March 2003 GAO study concluded that "no federal oversight or third-party verification ensures that voluntary industry assessments are adequate and that necessary corrective actions are taken."
- The GAO also pointed out that "the extent of preparedness at U.S. chemical facilities is unknown."
- The Bush Administration's chemical security legislation does not:
    - require DHS to review or ensure the adequacy of vulnerability assessments;
    - ensure that facilities upgrade security;
    - support industry adoption of inherently safer technologies; or
    - take advantage of chemical industry expertise of the Environmental Protection Agency.

CYBERSECURITY

SECURITY GAP:

- According to a recent survey conducted by the Pew Internet and American Life Project, almost half of Americans fear terrorists will launch cyberattacks on our critical infrastructures, disrupting major services and crippling economic activity.
- The National Institute of Standards and Technology (NIST) estimates that software bugs and errors cost the U.S. economy $59.5 billion per year.

- The Sobig, Blaster, and Welchia viruses caused more than than $32.8 billion in economic damages in August 2003 alone. The Sobig virus also successfully shut down the 23,000-mile-long CSX rail system this past summer when it infected the railroad's computers.
- The possible consequences of a cyber attack are demonstrated by recent instances where hackers successfully shut down the Worchester, Massachusetts airport, and released millions of gallons of raw sewage into an Australian community's waterways.
- Individuals have also gained access to critical systems of the California Independent System Operator, the nonprofit corporation that controls the distribution of 75% of the state's power, and the Roosevelt Dam in Arizona.

FAILURE TO CLOSE THE GAP:

- In the December 2003 "Computer Security Report Card" issued by the House Committee on Government Reform, eight of the agencies surveyed, including DHS, received an "F" on the security of their own computer network systems.
- In February 2002, the Administration released a "National Strategy to Secure Cyberspace," setting forth five cybersecurity priority areas, including the development of a cybersecurity response system, a threat and vulnerability reduction program, and awareness and training programs, as well as plans for securing government computers developing national security and international cooperation. Implementation of the plan has been delayed for nearly a year and two Presidential advisors on cybersecurity have left the government, one after only two months.
- In addition to losing its top cybersecurity officials, the Administration has dismantled the Critical Infrastructure Board. The top cybersecurity position in the government is now the Director of the National Cyber Security Division, buried deep within DHS. There is no longer a Presidential advisor or senior official with the authority to direct all the agencies responsible for cybersecurity should a cyber-crisis occur.
- To ensure that the United States is better prepared to prevent and combat terrorist attacks on private and government computers, Congress enacted the Cybersecurity Research and Development Act of 2002 which authorized $903 million in research and development funds over five years to the National Science Foundation (NSF) and the NIST. For FY04, the Act specified $110.25 million for NSF. Yet, the President's FY04 budget only requested $35 million for the NSF's cybersecurity efforts.

BIOTERRORISM

SECURITY GAP:

- Pentagon officials believe that al-Qaeda is pursuing sophisticated biological weapons and a United Nations panel recently declared it is "just a matter of time" before al-Qaeda attempts a biological or chemical attack.
- The anthrax attacks of October-November 2001 demonstrated that criminals already possess the ability to manufacture and use bioweapons to indiscriminately kill and injure civilians, and cause economic disruption and terror.
- Stores of dangerous pathogens, and the expertise to use them as weapons, remain in many sites in the former Soviet Union, in laboratories and collections throughout the world, and in research facilities in the United States.
- According to the Defense Science Board, at least 56 new countermeasures are needed to defend against the 19 major bioterrorism agents.
- The CIA has reported that rapid advances in biotechnology are making possible the creation of previously unknown biological agents that "could be worse than any disease known to man."
- The National Intelligence Council concluded in 2000 that infectious diseases "will endanger U.S. citizens at home and abroad, threaten U.S. armed forces deployed overseas, and exacerbate social and political instability in key countries and regions in which the United States has significant interests."

FAILURE TO CLOSE THE GAP:

- In 2003, the GAO reported that Department of Defense efforts to secure former biological weapons sites in Russia are in disarray.
- The Federal Bureau of Investigation, the Centers for Disease Control, and the U.S. Department of Agriculture failed to meet a November 12, 2003 deadline for certifying the security of U.S. laboratories and personnel that use weaponizable pathogens.
- Since the anthrax attacks, no new drugs or vaccines against CDC priority pathogens have been developed and introduced.
- While at least six federal agencies, along with state and local governments and the private sector, have roles in preparing and responding to bioterrorism, the Administration has not developed a comprehensive, coherent plan for biodefense. Even a limited plan, applying only to the Department of Health and Human Services and required by law, is more than six months overdue.
- In December 2003, the nonpartisan Trust for America's Health reported that public health preparedness has risen only modestly and haphazardly since 9/11. For example, only six states have enough laboratory capacity to deal with a public health emergency, and only two states have sufficient workers to distribute live-saving medicines from the Strategic National Stockpile.
- Despite the danger posed by bioengineered weapons that could release new or altered pathogens, the Administration has no plan to address this serious threat.

FIRST RESPONDER PREPAREDNESS

SECURITY GAP:

- On average, fire departments across the country have only enough radios to equip half the firefighters on a shift, and breathing apparatuses for only one third. Only 10% of fire departments in the United States have the personnel and equipment to respond to a building collapse.
- Police departments in cities across the country do not have the protective gear to safely secure a site following an attack with weapons of mass destruction.
- Most cities do not have the necessary equipment to determine what kind of hazardous materials emergency responders may be facing.
- Numerous interviews gathered as part of a New York City Fire Department inquiry into 9/11 indicated that the lack of interoperable communications was at least partially responsible for the loss of 343 firefighters at the World Trade Center.

FAILURE TO CLOSE THE GAP:

- Independent analysis estimates that the United States will fall approximately $98.4 billion short of meeting critical emergency responder needs over the next five years.
- However, the true needs of our first responders remain unknown, because the Administration has not defined national preparedness goals and standards that should be used by each community in America.
- State allocations for FY04 homeland security grants announced by the Administration continue to reflect the lack of any true assessment of the threats and vulnerabilities facing our nation; states such as California, New York, Texas and Florida receive less than $6 per capita, while low-population states such Wyoming, North Dakota and Vermont receive more than five times as much per person.
- In April 2003, the GAO testified that it had identified at least 16 different first responder grant programs, which are fragmented, confusing, and administratively burdensome for state and local officials.
- The Administration's FY04 budget request did not include any funds designated for state and local governments to enhance interoperable communications systems, and Congress cut first responder communications programs by 42% last year; at the same time, at least six Federal departments—with no one agency in charge—are involved in developing standards for state and local communications systems and equipment.

SECURITY, PRIVACY AND CIVIL RIGHTS

SECURITY GAP:

- The Gilmore Commission found in 2003 that "security" and "civil liberties" are mutually reinforcing parts of America's effort to strengthen our homeland.
- Innovative information technologies can make a substantial contribution to the war on terror by providing the government with new tools to identify potential terrorists.
- In addition, there exists significant amounts of information in the private sector that, when accessed by the government under proper guidelines and safeguards, can strengthen the war on terror by identifying terrorists and saving lives.
- In October 2002, The Markle Foundation's report, "Protecting America's Freedom in the Information Age," stated that the government, when utilizing new technologies and gathering information, needs guidelines to "identify the types of databases involved, define the purposes of the data review, and clarify the authorization for collecting and disseminating whatever is found" to effectively combat terrorism and protect privacy.

FAILURE TO CLOSE THE GAP:

- The Markle Foundation's second report, "Creating a Trusted Network for Homeland Security," released in December 2003, found that the government lacks a "systematic effort to consider the privacy implications of [its] proposed programs or to develop an overall policy framework that would govern the deployment of new technologies."
- The Markle Foundation reports concluded that the Administration's failure to formulate a policy framework to assess both the privacy implications of using new technologies and the value of gathering information available in the private sector has limited the effective use of information in the war against terror.
- Because of this failure, efforts to use new technologies and collect and analyze information "have been met with outcries of invasion of privacy and repeatedly shut down," according to the Markle Foundation. The following are examples of homeland security programs that have been terminated or delayed due to the Administration's failure to incorporate privacy protections into their plans and operations.
    - *The Terrorist (formerly known as Total) Information Awareness (TIA) program*: Created by the Defense Advanced Research Project Agency's Information Awareness Office, TIA was a data-mining program designed to capture as much information as possible on individuals and use computers and human analysis to detect potential terrorist activity. Congress

eliminated the TIA program, in part, due to its failure to properly assess privacy issues at its creation.

- o *Computer Assisted Passenger Prescreening System (CAPPS) II program*: CAPPS II is designed to pre-screen airline passengers using both public and private databases to check their backgrounds and rank them on their potential threats. Congress mandated it not be deployed until the GAO completes a privacy and civil liberties assessment. Congress expressed concern that the program lacks and security protections to protect against the unauthorized access of personal information.
- o *JetBlue-Defense research project:* The DHS, the Department of Defense, and the Federal Trade Commission are investigating the potential privacy violations caused by JetBlue's release of 5 million passenger itineraries to a defense contractor as part of a study seeking ways to identify "high risk" customers.

INFORMATION TECHNOLOGY (IT) AND HOMELAND SECURITY

SECURITY GAP:

- The creation of the DHS brought together 22 agencies and over 170,000 employees into an organization that inherited over 2,000 IT applications, 100 of which are considered major.
- Major IT applications include systems for threat identification and management, incident response, law enforcement, warning and alert communications, port of entry/exit management, and immigration.
- In many cases, these applications are outdated, insufficient, disconnected or duplicative.
- For the DHS to be an effective agency and fulfill its mission to protect the homeland, it needs to exercise strong IT management. Effective use of IT:
  - o is integral to DHS' ability to "connect the dots" and strengthen information-sharing among intelligence and law enforcement, a failure which proved so costly on 9/11;
  - o is essential to create a unified and well-run DHS that is greater than the sum of its parts.
- According to the Brookings Institution, "information technology should represent perhaps the highest priority for homeland security efforts."

FAILURE TO CLOSE THE GAP:

- While Secretary Ridge has claimed that the administration is using new technologies, a restructured homeland security organization, and streamlined processes to make the nation significantly more secure, criticism of the Administration's ineffective use of information technology to improve homeland security is nearly universal:

- According to the Joint Inquiry, while information technology remains one of this nation's greatest advantages, it has not been "fully [or] effectively applied in support of U.S. counterterrorism efforts." Persistent problems include "a reluctance to develop and implement new technical capabilities aggressively," a "reliance on outdated and insufficient technical systems," and "the absence of a central counterterrorism database."
- According to the Markle Foundation, the "government has not yet taken advantage of America's [information] technology expertise to combat terrorism."

- Management of IT within the DHS is unstable. According to the DHS Office of the Inspector General, turnover among divisional Chief Information Officers since the DHS opened its doors less than a year ago has been 45%.

- The Administration is failing to use IT effectively on mission-critical projects, including information sharing and integrating disparate terrorist watch lists:
  - According to the Brookings Institution, "Despite rhetoric about using IT aggressively to promote homeland security, the Bush Administration budgets and programmatic activities to date do not match the rhetoric…In regard to information technology, the Administration still has no plan for quickly improving real-time information sharing…among the [broad] set of public and private actors who are vital to preventing to homeland attacks."
  - While the technology to integrate separate terrorist watch lists is widely available and implementation should take no more than 6-12 months, the Administration, two-and-a-half years after 9/11, has yet to integrate data from separate lists into an integrated and robust terrorist watch list and database.

- The DHS has fallen short on even basic technology projects that would improve its daily operations.
  - Despite DHS promises to "[merge] the personnel and pay systems of all DHS component agencies into a single system," and that, "the new system will be completed by the end of [2003]," the DHS has still not integrated payroll and benefit systems for its own employees.
  - The DHS is failing to make it easier for technology companies to help protect the homeland. In testimony before the House Committee on Small Business, technology business executives expressed frustration with the lack of a reliable and comprehensive one-stop online resource to figure out existing contracting and business opportunities.