

CORD

Democratic Strategy on Homeland Security: Making America Safer: Closing the Security Gap

Item Type	House Minority Staff Report
Download date	2026-06-10 22:27:26
Link to Item	https://hdl.handle.net/20.500.14300/1707

The background of the entire page is a stylized American flag, featuring white stars on a blue field and red and white stripes. The stars are of various sizes and are scattered across the page. The stripes are horizontal and run across the width of the page.

DEMOCRATIC STRATEGY ON HOMELAND SECURITY

MAKING AMERICA SAFER: CLOSING THE SECURITY GAP

**CONGRESSMAN JIM TURNER,
RANKING MEMBER**

*Prepared by the Democratic Members of
the House Select Committee on Homeland Security*

DEMOCRATIC STRATEGY ON HOMELAND SECURITY

MAKING AMERICA SAFER: CLOSING THE SECURITY GAP

The attacks of September 11th changed America, and the world.

We remember so vividly the determination and commitment that resounded throughout this Congress in the aftermath of that dreadful day. Never again would we allow these terrorists to cross our borders unquestioned to plan their deadly acts on American soil. Never again would we allow them to walk through our airports unchallenged, hijack an aircraft, and turn it into a powerful weapon. Never again would we send our bravest citizens - our police, firefighters, and emergency crews - into a fiery inferno ill-equipped and unable to communicate with each other. Never again would we allow large gaps in our security to exist that could be exploited by those who seek to do us harm, perhaps with weapons of mass destruction.

In the aftermath of the attacks of September 11, the Congress responded with unprecedented unity and speed. We authorized the President to use all necessary force to destroy the al-Qaeda network and the Taliban government that provided it safe harbor. We enacted legislation to overhaul our airport security system, fortify our borders, and provide our intelligence and law enforcement agencies with tools needed to track down terrorists at home and abroad. We passed legislation to secure our seaports. Democrats proposed that we form a new Cabinet-level department to protect the homeland. Months later, the President endorsed this proposal and we worked together to establish the Department of Homeland Security.

But despite the spirit and unity of purpose that animated our response to September 11, we remain vulnerable as a nation on many fronts. Many of the glaring governmental failures revealed by the September 11 attacks have not been remedied. Many of the initiatives needed to protect our homeland have not been vigorously pursued. The Administration's strong rhetoric has not been met with the same level of commitment and resolve.

Secretary Ridge has stated that "today we are more secure and far better protected than on September 10, 2001. And every single day we get even more secure." But this standard sets the bar far too low. Now, two years after the most deadly single-day attack in our nation's history, the question we should be asking is whether we are as secure as we need to be from future terrorist attacks. Unfortunately, the answer is "no." In the words of an expert bipartisan commission of the Council of Foreign Relations, we are "dangerously unprepared" to prevent and respond to another terrorist attack.

What follows is Democrats' strategy to secure the homeland and a call for action to the Administration. It is a bold strategy to make America safer and more secure as quickly as possible. It is a plan that puts security first. It is a plan that says "we have waited too long." It is a plan that calls on the Administration to fulfill its commitment to the American people to secure the homeland as best we can.

I. PREVENTING TERRORIST ATTACKS

CREATE A UNIFIED TERRORIST “WATCH LIST”

Two years after September 11th, our government still does not have a single database of suspected terrorists for the worldwide use of intelligence officers, federal, state, and local law enforcement, border inspectors, and immigration officials. While the Administration promised to fix this problem months ago, today nine federal agencies are operating 12 separate watch lists, leaving open the possibility that a terrorist could be allowed to enter the United States because it was on one agency’s watch list but not another’s.¹

- *The Administration must ensure that the government creates a unified terrorist watch list, so that the kind of intelligence gaps leading to the attacks of September 11th never happen again.*

SHARE INFORMATION WITH STATE AND LOCAL LAW ENFORCEMENT

To prevent terrorist attacks, the federal government needs to provide specific, useable threat information to state and local law enforcement. Today, state and local law enforcement officials have not been granted the security clearances they need, currently receive scattered and sometimes conflicting information from the federal government, and lack the best information technology and interoperable communications equipment available.²

- *Federal agencies must get the flow of information moving to state and local law enforcement and other officials who are the eyes and the ears of our communities.*

SET PRIORITIES FOR PROTECTING AMERICA BASED ON THREATS AND VULNERABILITIES

Two years after September 11th, America still does not have a comprehensive national threat and vulnerability assessment to guide our efforts to prevent and respond to terrorist attacks. The Department of Homeland Security has not carried out this essential task.³

- *The Department of Homeland Security must develop a comprehensive terrorist threat assessment, catalogue our critical vulnerabilities across the nation, and use these tools to set priorities and create a detailed strategy to protect the homeland.*

SECURE FOREIGN STOCKPILES OF NUCLEAR MATERIALS

Today, huge stockpiles of nuclear, chemical, and biological weapons materials lie unguarded and vulnerable at sites across parts of the former Soviet Union. The Administration’s efforts to secure these materials have been inadequate.⁴

- *The Administration must fully implement the bipartisan Nunn-Lugar program to remove nuclear, chemical and biological materials -- the building blocks of international terrorism -- from repositories in the former Soviet Union.*

II. PROTECTING OUR BORDERS ON LAND, SEA AND AIR

HARDEN OUR LAND BORDERS TO PREVENT TERRORISTS FROM ENTERING THE UNITED STATES

Hire additional border agents and inspectors. The USA Patriot Act and the Border Security and Visa Entry Reform Act of 2002 required the Administration to hire hundreds of new agents and inspectors for the northern border. Almost two years later, the Administration has not met this basic mandate.⁵

- *The Administration must comply with the laws it endorsed by hiring thousands of new border patrol agents and inspectors to provide vigilance at ports of entry and along our borders. All inspectors must be rigorously trained to detect fraudulent documents and carry out other essential duties.*

Monitor the border 24/7. Hundreds of miles of our border go unmonitored by personnel or technology every day. Yet technology currently exists - such as unmanned aerial vehicles, remote sensors, and long range cameras - to monitor every mile of the northern and southern border for passage of terrorists, illegal migrants or cargo.⁶

- *The Department of Homeland Security should deploy new and existing technologies to ensure that every mile of our land border is secured.*

Keep Track Of Foreign Nationals Who Enter And Exit America. Today, there is not a single system for keeping track of who enters and exits America. Even more alarming, border agents and inspectors do not have real-time information on potential terrorists who are likely to try and enter our nation. In light of our security situation, the Administration has failed to fully implement a comprehensive automated system to keep track of who enters and exits the United States.⁷

- *The Department of Homeland Security must make tracking foreign nationals in the United States a national homeland security priority by developing and deploying a comprehensive entry/exit system and providing access to a unified terrorist watch list to front-line agents and inspectors.*

SECURE OUR PORTS AND COASTLINE

Check Cargo For Weapons Of Mass Destruction. Millions of cargo containers enter the United States and travel through our communities every year. Currently, less than 3 percent of the cargo containers entering American ports are ever checked to determine their contents. This Administration has not deployed the personnel or equipment to ensure that these containers are free of weapons of mass destruction.⁸

- *The Administration must ensure that robust teams of Customs inspectors are permanently placed at high risk ports abroad, increase accountability for companies shipping goods into the U.S., develop technology to detect weapons of mass destruction, and deploy systems to track every container and ship entering an American port.*

Implement Port Security Plans. America’s ports are developing plans to provide the security necessary in the post-September 11th world, such as installing cameras, building fences and posting guards. Yet the Administration provided no support for these efforts in its most recent budget. Due to the lack of funding and commitment, many ports are struggling to get these changes in place, leaving them extremely vulnerable.⁹

- *The Administration must commit the personnel and resources to fully secure our ports.*

Strengthen The Coast Guard. Since September 11th, the U.S. Coast Guard has been asked to lead the nation’s efforts to secure 95,000 miles of coastline and 361 ports while ensuring the flow of commerce. However, they are short on personnel and their plans to upgrade ships and air patrol are 5 years behind schedule.¹⁰

- *The Administration must strengthen the Coast Guard by increasing personnel by 15 percent and upgrading their fleet of frontline ships and planes in half the time of current plans.*

PROVIDE COMPREHENSIVE AVIATION SECURITY

Screen Cargo On All Passenger Planes. Today, 22 percent of all air cargo moves on passenger flights without a security check, despite a law that TSA will screen all cargo.¹¹ TSA instead relies on “known shippers” despite evidence of numerous security violations.¹²

- *The Department of Homeland Security must establish a security screening process for cargo placed on passenger planes.*

Protect Passenger Planes From Missile Attack. Passenger planes are totally undefended against attack by surface to air missiles. Such missiles are widely available and of known interest to terrorists. The Administration has not deployed any defenses against this critical threat.¹³

- *The Department of Homeland Security must accelerate research for on-board anti-missile technology for passenger aircraft, improve airport perimeter security, and deploy missile defenses as soon as technically feasible.*

III. PROVIDING SECURITY INSIDE AMERICA

ASSERT LEADERSHIP TO SECURE CRITICAL INFRASTRUCTURE

Since September 11th, the Administration has paid insufficient attention to the protection of critical infrastructures within the United States, including chemical and nuclear facilities, commercial transport, mass transit, power systems and other utilities, and high-volume buildings and public venues like skyscrapers and stadiums. While 85 percent of critical infrastructure is privately owned, the Administration's over-reliance on voluntary private action to enhance security has left us with a weak patchwork of efforts that does not give America's communities the protection they deserve.¹⁴

- *The Administration must assert strong federal leadership to improve critical infrastructure protection across the board. It must rapidly develop a single comprehensive national list of risks and vulnerabilities in all critical infrastructure sectors and work together with the private sector and municipal governments to provide the necessary level of security at these facilities. When unacceptable vulnerabilities remain, swift action must be taken to eliminate them.*

Chemical Facilities

A terrorist attack on a chemical facility could send a deadly toxic cloud into population centers. Today there are over 3,000 chemical facilities where a toxic release could threaten more than 10,000 people. An accident at any of over 120 of those facilities could put more than 1 million people at risk. These plants remain highly vulnerable to a terrorist attack.¹⁵

- *The Administration must require chemical facilities to assess their security vulnerabilities and implement security improvement plans.*

Electrical Power Grid

The blackout of 2003 clearly demonstrated the weaknesses in our electricity grid and its vulnerability to potential terrorist attack. Our electrical systems are vulnerable to failures in key nodes, need better fail-safe mechanisms to isolate outages, and lack sufficient redundancy to compensate for outages.¹⁶

- *The Administration must take action to modernize the power grid and harden it against potential attack and disruption by ensuring adequate back-up systems, improved fail-safe mechanisms, and more secure operating and safety systems and protocols.*

Nuclear Power Plants

The United States has 104 nuclear reactors in 31 states. Those who live in communities with nuclear power plants must have assurances that the highest levels of security are maintained and that emergency planning is thorough and comprehensive.¹⁷

- *The Administration must maintain the highest levels of security at our nuclear power facilities.*

MAKE CYBER SECURITY A TOP PRIORITY

Appoint Senior Cyber Security Official. Today, there is no senior Administration official in charge of cyber security in the federal government -- no one is responsible for planning to prevent an electronic September 11th that could damage our financial systems, public utilities, telecommunications and other vital systems.¹⁸

- *The Administration must create a Cyber Command Center led by a senior Administration official so that America can organize its defense against potential cyber attacks and organize a response in a time of crisis.*

Improve Training and Awareness. America's cyber security ultimately rests in the hands of the private sector and individual citizens. Today, little is being done to help the tens of thousands of systems administrators across the nation keep their networks secure. Not enough is being done to equip home users with the tools to protect their privacy and computers from cyber attacks.¹⁹

- *The Administration must support efforts by educational institutions to reach out to computer users and provide the security training necessary for them to protect themselves from cyber attack.*

Promote Standards and Practices. There are currently no standardized security certifications and guidelines for government and business computer systems, let alone for the consumer market.²⁰

- *The Administration must develop a public-private partnership to develop a recognized "seal of approval" for standards, benchmarks, and best practices.*

IV. PREPARING OUR COMMUNITIES

ARMING FIRST RESPONDERS WITH THE TOOLS THEY NEED

According to a prominent bipartisan commission, America is "dangerously unprepared" to respond to a catastrophic terrorist attack. Yet, two years after September 11th, there has been no systematic review to determine the equipment, training, personnel, and planning America's first responders need to protect our communities from terrorist attacks. Grant programs remain inefficiently administered and lack a coherent strategy. While funding for some programs has increased, we have no way of measuring the capabilities of our first responder communities and determining the investments necessary to provide the right level of security for all Americans.²¹

- *The Department of Homeland Security must determine the needs of all our communities and create a Terrorism Preparedness Grant Program that will get the best equipment and training in the hands of the police, firefighters and emergency personnel who will be the first on the scene of an attack.*

ENABLE FIRST RESPONDERS TO COMMUNICATE

America's first responders still can't talk with one another at a time of crisis. Communications equipment still is not interoperable and that means that too often at a disaster site, firefighters, police and emergency personnel can't communicate. Two years after September 11th, the situation remains as disconnected as ever.²²

- *The Department of Homeland Security must deploy nationwide the communications equipment necessary for first responders to take effective and coordinated action.*

DEVELOP VACCINES TO COUNTER BIOTERRORISM

The threat of bioterrorism is a clear and present danger to the American people, but we are not prepared to respond to the breadth and sophistication of the potential biological attacks that we face. The Administration's "Project BioShield" aspires to develop vaccines for five pathogens in the next decade, but the Defense Science Board estimates that we need 57 vaccines, antidotes, and diagnostics to address the current level of threat.²³

- *The Administration must implement a robust plan that asserts federal leadership, in conjunction with the private sector, to produce the medicines we will need to counter the bioterror threat.*

BUILD SURGE CAPACITY IN MAJOR HOSPITALS

The effects of an attack using chemical, biological or radiological weapons would be sudden and devastating on our communities. America's health care system is already stretched to capacity.²⁴

- *Federal agencies must help major hospitals accommodate potential large increases in patients who suffer the effects of catastrophic attack and acquire the specialized tools our hospitals need to diagnose and respond to chemical, biological or radiological attacks.*

V. PROTECTING OUR COUNTRY AND OUR CONSTITUTION

We can strengthen our homeland security while protecting privacy and traditional civil rights and liberties. Our country can be secure while continuing to be a beacon for democracy around the world.

- *The Administration must take strong measures to protect security across the board while maintaining respect for privacy, due process, and the right to counsel for all Americans.*

END NOTES

I. PREVENTING TERRORIST ATTACKS

¹ U.S. intelligence agencies were tracking at least two of the September 11 hijackers, but failed to use watch lists to prevent their entry to the United States. Yet, the Administration has failed to address the problem of multiple, incompatible, and sometimes inaccessible watch lists.

According to the GAO, *“Nine federal agencies...develop and maintain 12 watch lists...These lists include overlapping but not identical sets of data, and different policies and procedures govern whether and how these data are shared with others”* (General Accounting Office, “Information Technology: Terrorist Watch Lists Should be Consolidated to Promote Better Integration and Sharing,” GAO-03-322, April 15, 2003).

² According to the Congressional Joint Inquiry, *“The agencies of the Intelligence Community should act promptly to expand and improve counterterrorism training programs within the Community, insuring coverage of such critical areas as information sharing among law enforcement and intelligence personnel”* (Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, S. Rep. No. 107-351, H. Rep. No. 107-792 [107th Congress], December 2002).

Yet, according to the GAO, *“Information on threats, methods, and techniques of terrorists is not routinely shared; and the information that is shared is not perceived as timely, accurate, or relevant. Moreover, federal officials have not yet established comprehensive processes and procedures to promote sharing”* (General Accounting Office, “Homeland Security: Efforts to Improve Information Sharing Need to be Strengthened,” GAO-03-760, August 27, 2003).

³ Without a threat and vulnerability assessment, the Administration cannot focus its efforts on those attacks that are most likely to occur, that are aimed at our most vulnerable sites, and that could cause significant damage if terrorists succeeded in their plans.

⁴ According to a recent Harvard University report, *“In the aftermath of the September 11 attacks, it is simply not acceptable to allow limited budgets, lack of high-level attention, and bureaucratic wrangling to delay the efforts needed to keep nuclear weapons and their essential ingredients out of terrorist hands”* (Matthew Bunn, Anthony Wier, and John P. Holdren, *Controlling Nuclear Warheads and Materials: A Report Card and Action Plan*, Washington, D.C.: Nuclear Threat Initiative and the Project on Managing the Atom, Harvard University, March 2003).

II. PROTECTING OUR BORDERS ON LAND, SEA, AND AIR

⁵ Congress enacted laws that required the Administration to hire hundreds of new agents to secure the northern border (U.S.A. Patriot Act [P.L. 107-56]; the Enhanced Border Security and Visa Entry Reform Act of 2002 [P.L. 107-173]). Almost two years later, according to the GAO, however, the Border Patrol still hasn't met staffing levels mandated almost 10 years ago [prior to 9/11] (General Accounting Office, “Testimony of Richard Stana: Challenges Facing DHS in Balancing its Border Security and Trade Facilitation Missions,” GAO-093-902T, June 16, 2003).

⁶ “For example, at the time of our inspection, one northern border sector had identified 65 smuggling corridors along the more than 300 miles of [northern] border within its area of responsibility, but the sector had only 36 sensors with which to monitor these corridors” (Glenn Fine, Inspector General for the Department of Justice, testimony before the National Commission on Terrorist Attacks Upon the United States, April 1, 2003).

⁷ A GAO report expressed serious concerns about the Department’s ability to implement a comprehensive entry-exit system, citing problems with adequate planning, system capabilities, schedules, and costs (General Accounting Office, “Testimony of Richard Stana: Challenges Facing DHS in Balancing its Border Security and Trade Facilitation Missions,” GAO-093-902T, June 16, 2003).

⁸ The GAO reports that “more than six million cargo containers arrive at our ports every year, but less than three percent of these are physically inspected. This tremendous flow of goods [with a low inspection rate] makes container shipments a prime target for terrorists” (General Accounting Office, “Port Security: Nation Faces Formidable Challenges in Making Initiatives Successful,” GAO-02-993T, August 5, 2003).

⁹ The Coast Guard estimates ports will need to spend \$1.1 billion over the next year on security measures (*Federal Register*, U.S. Coast Guard, Interim Final Rule Facility Security. July 1, 2003, p. 39319). The Administration’s most recent budget, however, requests no resources for these efforts (Department of Homeland Security Appropriations Bill, Report Fiscal Year 2004, House Rpt. 108-169, p. 106).

¹⁰ According to Brookings Institution security expert Michael O’Hanlon, the Coast Guard’s manpower is at a level “several times smaller for example than during World War II” (Michael O’Hanlon, “Cargo Security” testimony before the Committee on Governmental Affairs, U.S. Senate, March 20, 2003).

¹¹ Aviation and Transportation Security Act, Pub. L. No. 107-71, §110.

¹² According to TSA, “there is a 35 percent to 65 percent likelihood that terrorists are planning to put a bomb in cargo on a passenger plane, while the federal government is focused almost exclusively on screening passengers and baggage” (Greg Schneider, “Terror Risk Cited for Cargo Carried on Passenger Jets; 2 Reports List Security Gaps,” *Washington Post*, June 10, 2002, p. A1).

¹³ “The [Homeland Security] Department isn't convinced that there is a cost-effective method to thwart a determined terrorist on the ground aiming at an aircraft overhead” (Renaë Merle, “U.S. Weighing Missile Defenses for Airliners,” *Washington Post*, August 22, 2003, p. E1).

III. PROVIDING SECURITY INSIDE AMERICA

¹⁴ According to the Transportation Research Board, worldwide, roughly one-third of terrorist attacks target transportation systems, and the most frequently targeted transportation mode is public transit (Transportation Research Board, *Emergency Preparedness for Transit Terrorism*, 1997). Furthermore, according to the National Research Council, the mobility, range, and omnipresence of transportation vehicles and containers make them “a ready means of delivering

terrorist weapons” (Making the Nation Safer, The Role of Science and Technology in Countering Terrorism, National Research Council, 2002). “Roughly 800,000 hazardous materials shipments by truck occur each day....A release of 90 tons of chlorine [from a rail tank] could affect populations up to 14 miles away” (Protecting the American Homeland: One Year On, Brookings Institution, 2002, updated with a new preface, 2003). According to the Brookings Institution, the Bush Administration “largely ignores” major infrastructure in the private sector. In “many private-sector settings – from chemical plants to hazardous materials trucking firms and nuclear facilities – current efforts fall woefully short of what is required.” In early 2003, the Department of Homeland Security “issued a strategy document for protecting critical infrastructure, but the document lacked the types of specific policy steps that are now overdue” (Protecting the American Homeland: One Year On, Brookings Institution, 2002, updated with a new preface, 2003).

¹⁵ According to the GAO, “123 chemical facilities located throughout the nation have toxic ‘worst case’ scenarios where more than a million people could be at risk of exposure to a cloud of toxic gas if a release occurred. To date, no one has comprehensively assessed the security of chemical facilities” (General Accounting Office, “Homeland Security: Voluntary Initiatives are Under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown,” GAO-03-439, March 14, 2003). As the *National Journal* reported recently, “Counter terrorism experts shudder to think about the number of deaths an intentional release of a toxic chemical could cause. And the Bush Administration’s inertia heightens their worries” (“Security Leak,” *National Journal*, August 2, 2003).

¹⁶ According to the National Research Council, “the most insidious and economically harmful attack would be one that exploits the vulnerabilities of an integrated electric power grid...The nation’s electric power systems must clearly be made more resilient to terrorist attacks” (*Making the Nation Safer, The Role of Science and Technology in Countering Terrorism*, National Research Council, 2002).

¹⁷ The National Research Council states that “nuclear power plants may present a tempting high visibility target for terrorist attack, and the potential for a September 11-type surprise attack in the near term using U.S. assets such as airplanes appears to be high. Such attacks potentially have severe consequences...[and] do great harm to the nation’s near term energy security” (*Making the Nation Safer, The Role of Science and Technology in Countering Terrorism*, National Research Council, 2002).

¹⁸ The National Academies found that “We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. Although we trust them, they are vulnerable—to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack...Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb” (*Cyber Security Today and Tomorrow: Pay Now or Pay Later*, Computer Science and Telecommunications Board, National Research Council, 2002).

According to Roger Cressey, the former chief of staff for the now-dismantled President’s Critical Infrastructure Protection Board, the information technology industry has “made it pretty clear” that the Administration has sent “bad signals” by not replacing the cybersecurity advisor to the President and by creating the Cyber Security Division “only after criticism” (*DHS Needs IT’s*

Trust, eweek.com, August 25, 2003, available at http://www.eweek.com/print_article/0,3668,a=55581,00.asp).

¹⁹As detailed in a report from a workshop sponsored by the National Science Foundation and the American Association of Community Colleges, “*Potential cybersecurity threats create an additional need for an expanded technical workforce with appropriate, specific knowledge and skills. All computer users need to be aware of the basic aspects of computer security so that they can protect themselves at home and in the workplace. The challenge of providing specialized training for computer experts and basic computer security training for all U.S. citizens extends to institutions at all levels of the formal educational system*” (*Cyber Security Education: The Role of Community Colleges in Protecting Information, A Report from a Workshop Sponsored by the National Science Foundation and the American Association of Community Colleges*, June 26-28, 2002).

²⁰ Dr. S. Shankar Sastry, a cybersecurity expert at the University of California at Berkeley, states “*to build good security habits, government agencies should encourage public-private partnerships with academic researchers, corporations, venture capitalists, and consumers, the security experts suggest. What's more, security technology must be painstakingly developed, rigorously tested, and tailored to the public's needs*” (*Homeland Security Begins With Your PC: Security experts urge open exchange and cooperation*, July 23, 2003, available at <http://www.pcworld.com/news/article/0,aid,111730,00.asp>).

IV. PREPARING OUR COMMUNITIES

²¹ According to a Council on Foreign Relations Task Force, America remains “*dangerously unprepared*” to respond to a catastrophic terrorist attack (Report of an Independent Task Force Sponsored by the Council on Foreign Relations, “*Emergency Responders: Drastically Underfunded, Dangerously Unprepared,*” June 2003). Yet two years after September 11th, there has been no systematic review to determine the equipment, training, personnel, and planning standards for America’s first responders to protect our communities from terrorist attacks. In December of 2002, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction [“*Gilmore Commission*”] also called for a comprehensive approach to measuring how well we are doing with the resources being applied to homeland security, in order to answer the question, “*How well prepared are we?*” (*Fourth Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction*, Gilmore Commission, December 16, 2002, available at <http://www.rand.org/nsrd/terrpanel/>).

In April 2003, GAO testified that they had identified at least sixteen (16) different grant programs that were being used by the nation’s first responders, and that these multiple fragmented grant programs create a confusing and administratively burdensome process for state and local officials (General Accounting Office, “*Grant System Continues to be Highly Fragmented,*” GAO-03-718T, April 29, 2003).

²² Numerous interviews gathered as part of a New York City Fire Department inquiry into the events of September 11th indicated that non-interoperability was at least partially responsible for the loss of 343 firefighters at the World Trade Center (Lund, Donald A., *Learning to Talk: The*

Lessons of Non-Interoperability in Public Safety Communications Systems, The ATLAS Project, University of New Hampshire, April 2002, p. 14).

The Department of Homeland Security testified that it will take approximately six months to more than a year to complete pilot interoperable communication system projects, to be followed by a study and finally, the development of national standards. (Hearing, “Response to Terrorism: How is DHS Improving Our Capabilities?” Select Committee on Homeland Security, United States House of Representatives, June 19, 2003).

²³ A 2000 Defense Science Board study regarding medical countermeasures for use against major biological pathogens estimated that 19 diagnostics, 19 vaccines, and 19 therapeutics – or a total of 57 countermeasures – are needed to address the current level of threat. Today, only one of the 57 countermeasures exists. (Defense Science Board, “The Projected Evolution of Diagnostics, Vaccines, and Therapeutics against Major Bioagents with Strategic R&D and Supply Actions,” Summer 2000).

²⁴ Medical experts have stated that, “...*hospital surge capacity and specialized medical capability across the United States has never been more restricted. While the public and the political communities assume that the healthcare systems are adequately preparing for terrorism incidents that would generate catastrophic casualty loads, the medical community is struggling just to maintain its everyday capacity*” (Joseph A. Barbera, MD, Anthony G. Macintyre, MD, Craig A. DeAtley, PAC, “Ambulances to Nowhere: America’s Critical Shortfall in Medical Preparedness for Catastrophic Terrorism.” BCSIA Discussion Paper 2001-15, ESDP Discussion Paper ESDP-2001-07, John F. Kennedy School of Government, Harvard University, October 2001).