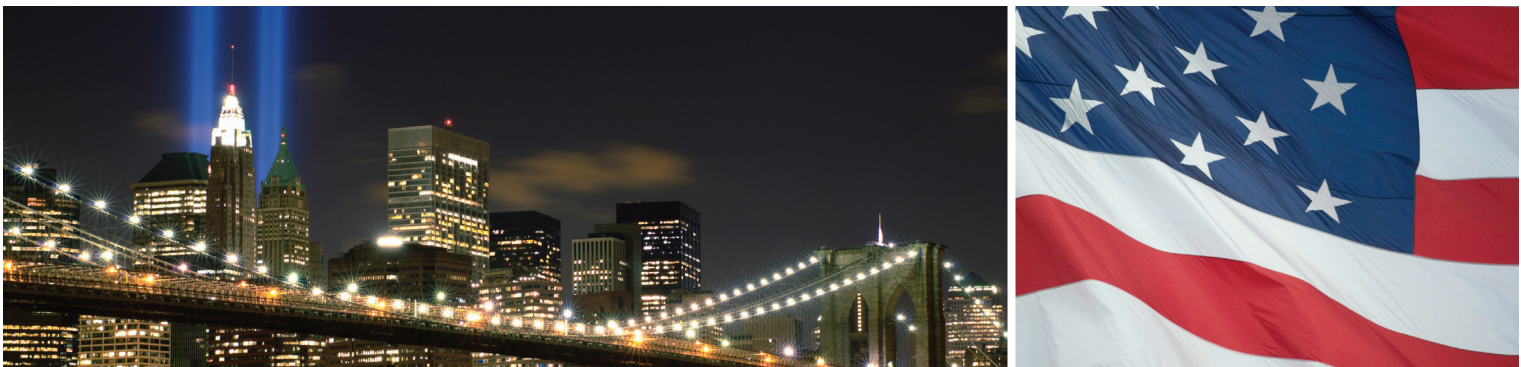




National Security  
Preparedness Group



Tenth Anniversary Report Card:  
**The Status of the 9/11  
Commission Recommendations**

September 2011



BIPARTISAN POLICY CENTER

1225 Eye Street NW, Suite 1000  
Washington, DC 20005  
(202) 204-2400

[WWW.BIPARTISANPOLICY.ORG](http://WWW.BIPARTISANPOLICY.ORG)



BIPARTISAN POLICY CENTER

# National Security Preparedness Group

## CO-CHAIRS

**The Honorable Lee Hamilton**  
Former Representative from Indiana and Vice Chairman of the 9/11 Commission

**The Honorable Thomas Kean**  
Former Governor of New Jersey and Chairman of the 9/11 Commission

## MEMBERS

**The Honorable Frances Townsend**  
Former Homeland Security Advisor and Deputy National Security Advisor for Combating Terrorism

**The Honorable Edwin Meese III**  
Former Attorney General

**The Honorable Dick Thornburgh**  
Former Attorney General and Governor of Pennsylvania

**The Honorable Jim Turner**  
Former Representative from Texas and Ranking Member of the House Homeland Security Committee

**The Honorable Dave McCurdy**  
Former Representative from Oklahoma and Chair of the House Intelligence Committee

**Dr. John Gannon**  
Former Deputy Director of the CIA for Intelligence

**Peter Bergen**  
Director, National Security Studies Program at the New America Foundation

**The Honorable Spencer Abraham**  
Former Secretary of Energy and U.S. Senator from Michigan

**Dr. Stephen Flynn**  
President, Center for National Policy

**The Honorable Tom Ridge**  
Former U.S. Secretary of Homeland Security and Governor of Pennsylvania

**The Honorable Dan Glickman**  
BPC Senior Fellow and Former Secretary of Agriculture

**Professor Bruce Hoffman**  
Director, Center for Peace and Security Studies, Georgetown University

## PROJECT DIRECTOR

**Rob Strayer**  
Former Deputy Staff Director, Senate Homeland Security Committee

### DISCLAIMER

This report is the product of the Bipartisan Policy Center’s National Security Preparedness Group. The findings and recommendations expressed herein do not necessarily represent the views or opinions of the Bipartisan Policy Center, its founders, or its board of directors.



# Foreword

We serve as co-chairs of the Bipartisan Policy Center’s National Security Preparedness Group (NSPG), which is a follow-on to the 9/11 Commission. NSPG monitors the implementation of the 9/11 Commission’s recommendations and focuses on emerging security threats to our nation.

Ten eventful years have now passed since violent Islamist extremists, members of the terrorist organization al Qaeda, hijacked four commercial airplanes and flew them into the twin towers of the World Trade Center in New York City, the Pentagon in Washington, D.C., and a field in Pennsylvania. These horrific attacks killed nearly 3,000 of our fellow Americans and citizens of foreign countries, altering our society forever.

Over the course of nearly 20 months, the 9/11 Commission investigated the facts and circumstances surrounding the attacks. The 9/11 Commission Report, issued in July 2004, made 41 recommendations for keeping our country safe. These recommendations were endorsed by both presidential candidates at the time and almost every member of Congress.

We have reflected often on why the 9/11 Commission was successful. First, because of the great damage and trauma the 9/11 attacks produced, the American public demanded action and had high expectations for measures and reforms that would improve the nation’s security. Importantly, the statutory mandate for the Commission was limited, precise, and clear – the Commission was authorized to investigate the facts and circumstances surrounding the attacks and to make


recommendations to keep the country safe; the Commission had an extraordinary non-partisan staff, the members of which possessed deep expertise and conducted their work with thoroughness and professionalism; the Commissioners had deep experience in government and political credibility with different constituencies; the final report was unanimous and bipartisan; families of the victims of 9/11 provided solid and sophisticated support throughout the life of the Commission and in the years since; and following the Commission, the Commissioners and staff continue to work closely with Congress and the executive branch to implement and monitor reform.

The success of the Commission’s work was due to political leadership embracing its findings and recommendations, pushing hard to enact them, and continuing to drive reform. That support and leadership have been critical in improving the nation’s security.

Now, on the solemn occasion of the 10th anniversary of the attacks, is an appropriate time to reflect and evaluate where we are in national security reform – and what we have yet to achieve.

Sincerely,

  
Tom Kean

  
Lee Hamilton





# Table of Contents

---

**Chapter 1: Introduction** .....6

Effect of the 9/11 Attacks .....6

The Government’s Response .....6

Evolving Terrorist Threat to the United States .....7

**Chapter 2: Nine Major Unfinished 9/11 Commission Recommendations** .....10

Unity of Command and Effort .....12

Radio Spectrum and Interoperability .....14

Civil Liberties and Executive Power .....15

Congressional Reform .....16

Director of National Intelligence .....17

Transportation Security .....17

Biometric Entry-Exit Screening System .....18

Standardize Secure Identifications .....18

Develop Coalition Standards for Terrorist Detention .....19

**Chapter 3: Conclusion** .....20

# Chapter 1: Introduction

## Effect of the 9/11 Attacks

The terrorist attacks of September 11, 2001 exacted a devastating toll on so many of our families, profoundly and dramatically transforming government, the private sector, and our daily lives. The suddenness of the attacks on American soil and the loss of so many lives made us feel vulnerable in our homes, and caused us to question whether our government was properly organized to protect us from this lethal threat. The economic damage resulting from the attacks was severe. In short order, we shifted from a “peace dividend” at the end of the Cold War to massive expenditures of taxpayer dollars on new security measures.

The human tragedy was, of course, the greatest loss. Nothing can replace the loved ones lost to that act of terrorism. But the consequences for our economy and the private sector have been striking. More than 80 percent of our nation’s critical infrastructure is owned by the private sector, and protecting it from terrorist operations has become an urgent priority. Working together, the government and private sector have improved their information sharing and, therefore, our security posture.

Businesses in all sectors have adapted to this new reality. They have focused on how best to protect personnel as well as food and water supplies; they have developed continuity plans to prepare for possible disruptions; and they have adopted innovative safety features into building construction. U.S. importers, working with the Department of Homeland Security, have pioneered new ways to ensure the integrity of shipping containers that bring goods into the country. The insurance industry’s risk analysis has evolved to reflect new realities. These necessary innovations have increased the costs of doing business, and future innovations may raise costs even higher.

## The Government’s Response

Over the past 10 years, our government’s response to the challenge of transnational terrorism has been dramatic. At the federal level, we have created major new institutions. The Department of Homeland Security itself was a massive reconfiguration of government, combining 22 agencies into a new department, with a workforce of 230,000 people and an annual budget of more than \$50 billion. In total, some 263 organizations have been established or redesigned.

The intelligence community has also adapted. In response to the recommendations of the 9/11 Commission, Congress created the Office of the Director of National Intelligence (DNI) and the National Counterterrorism Center in 2004 to advance a unified effort across the intelligence community. Four DNIs in six years have worked with the Intelligence Community (IC), sometimes with difficulty, to establish appropriate and effective roles and responsibilities. Today, key IC relationships in the new order appear to be improving and moving in a constructive direction.

At the same time, the intelligence budget has surged to more than \$80 billion – more than double what was spent in 2001. And throughout the national security community, a flexible and resilient workforce has been trained to protect the American people in a new environment. The FBI, CIA, and the broader intelligence community have implemented significant reforms, disrupting many plots and bringing to justice many terrorist operatives.

Despite this considerable progress, some major 9/11 Commission recommendations remain unfulfilled, leaving the U.S. not as safe as we could or should be. These unfulfilled recommendations require urgent attention because the threat from al Qaeda, related terrorist groups, and individual adherents to violent Islamist extremism

persists. In late July, a U.S. soldier was arrested on suspicion of plotting to murder U.S. soldiers at Fort Hood, Texas. Other brands of extremism are also highly lethal and threaten all of us, as the recent events in Norway so painfully remind us.

## Evolving Terrorist Threat to the U.S.

Former CIA Director and current Secretary of Defense, Leon Panetta, declared that we are “within reach of strategically defeating al Qaeda.” Only the future will tell whether that is accurate, but certainly the death of Osama bin Laden is our most significant advancement to date in our efforts to defeat al Qaeda.

The bin Laden raid resulted from years of hard work, cooperation, vigilance, and tenacity. It involved surveillance, the analysis of many bits of information, and seamless interaction between the CIA and the military. Bin Laden’s capture reflected the highest level of collaboration among IC agencies and the military.

Although Osama bin Laden is dead, al Qaeda is not; it is a network, not a hierarchy. Over a period of years, al Qaeda has been very adaptive and resilient. Al Qaeda and its affiliates will almost certainly attempt to avenge his death, however, they will not necessarily attack soon.

Al Qaeda’s capabilities to implement large-scale attacks are less formidable than they were 10 years ago, but al Qaeda and its affiliates continue to have the intent and reach to kill dozens, or even hundreds, of Americans in a single attack.

Al Qaeda has been marked by rapid decentralization. The most significant threats to American national security come from affiliates of core al Qaeda, such as al Qaeda in the Arabian Peninsula where U.S.-born Anwar al-Awlaki has played a prominent role. Al Qaeda’s influence is also on the

rise in South Asia and continues to extend into failing or failed states such as Yemen and Somalia.

In assessing terrorist threats to the American homeland, senior U.S. counterterrorism officials now call attention to al Qaeda’s strategy of “diversification” – attacks mounted by a wide variety of perpetrators of different national and ethnic backgrounds that cannot easily be “profiled” as threats.

Most troubling, we have seen a pattern of increasing terrorist recruitment of American citizens and residents to act as “lone wolves.” In 2009, there were two actual terrorist attacks on our soil. The Fort Hood shooting claimed the lives of 13 people, and a U.S. military recruiter was killed in Little Rock, Arkansas. Today, we know that Americans are playing increasingly prominent roles in al Qaeda’s movement. Muslim-American youth are being recruited in Somali communities in Minneapolis and Portland, Oregon, in some respects moving the front lines to the interior of our country.

Alarmingly, we have discovered that individuals in the U.S. are engaging in “self-radicalization.” This process is often influenced by blogs and other online content advocating violent Islamist extremism. While there are methods to monitor some of this activity, it is simply impossible to know the inner thinking of every at-risk person. Thus, self-radicalization poses a serious emerging threat in the U.S.

Because al Qaeda and its affiliates will not give up, we cannot let our guard down. Our terrorist adversaries and the tactics and techniques they employ are evolving rapidly. We will see new attempts, and likely successful attacks.

Our enemy continues to probe our vulnerabilities and design innovative ways to attack us. Such innovation is best exemplified by the discovery in October 2010 of explosives



packed in toner cartridges addressed to synagogues in Chicago and shipped on Fed Ex and UPS cargo flights from Yemen. This plot constituted an assault on our international transportation and commerce delivery systems and it was committed without the terrorists ever having to set foot within the U.S. Although the plot failed, terrorists will not abandon efforts to develop new ways to inflict great harm on us.

Another way that terrorists can attack without ever physically crossing our borders is through a cyber attack. Successive DNIs have warned that the cyber threat to critical infrastructure systems – to electrical, financial, water, energy, food supply, military, and telecommunications networks – is grave. Earlier this month, senior DHS officials described a “nightmare scenario” of a terrorist group hacking into U.S. computer systems and disrupting our electric grid, shutting down power to large swathes of the country, perhaps for a period as long as several weeks. As the current crisis in Japan demonstrates, disruption of power grids and basic infrastructure can have devastating effects on society.

This is not science fiction. It is possible to take down cyber systems and trigger cascading disruptions and damage. Defending the U.S. against such attacks must be an urgent priority.

All of these continued and nascent threats mean that we must not become complacent, but remain vigilant and resolute. We have significantly improved our security since 9/11, but the work is not complete. We should begin by tackling the unfinished recommendations of the 9/11 Commission.

This is not science fiction. It is possible to take down cyber systems and trigger cascading disruptions and damage. Defending the U.S. against such attacks must be an urgent priority.



National Security Preparedness Group



# Chapter 2: Nine Major Unfinished 9/11 Commission Recommendations

To be sure, substantial progress has been made in fulfilling many of the 9/11 Commission’s 41 recommendations. Dedicated men and women in government and private sector should be credited for their tireless efforts and accomplishments in improving our national security during

the last decade. This report does not chronicle all of their successes here, but highlights the transformation of the intelligence community and improvements to screening airline passengers.

Recommendation	Primary Responsible Entity			
	DHS	State and Local Governments	Executive Office of the President	Congress
	Unity of Command and Effort			
	Radio Spectrum and Interoperability			
	Civil Liberties and Executive Power			
	Congressional Reform			
	Director of National Intelligence			
	Transportation Security			
	Biometric Entry-Exit Screening System			
	Standardize Secure Identifications			
	Develop Coalition Standards for Terrorist Detention			

Improvement Needed

Unfulfilled

Success Highlights

Intelligence Community Transformation

Legal, policy, and cultural barriers between agencies created serious impediments to information sharing that prevented disruption of the 9/11 attacks. Therefore, the 9/11 Commission made a number of specific recommendations to improve information sharing across our government. Information sharing within the federal government, and among federal, state, local authorities, and with allies, while not perfect, has considerably improved since 9/11.

Progress among national agencies, and between the IC and the military in the field, has been striking. The degree of interagency collaboration in Afghanistan and Iraq is unprecedented. On the domestic side, however, there has been less unity of effort and much slower progress among multiple agencies that are either new or have new counterterrorism missions.

The level of cooperation among all levels of government is higher than ever. There are now 105 Joint Terrorism Task Forces throughout the nation, and 72 Fusion Centers in which federal, state, local authorities investigate terrorism leads and share information. State and local officials have a far greater understanding not only of threats and how to respond to them, but also of their communities and those who may be at risk of radicalization.

The FBI has gone through dramatic change and continues to transform from an agency overwhelmingly focused on law enforcement to one that prioritizes preventing terrorism. This is a significant cultural change that can be furthered by placing the status of intelligence analysts on par with special agents, who have traditionally risen to management at the Bureau.

Airline Passenger Screening

The CIA has improved its intelligence analysis and removed barriers between its analysts and operations officers. Recruiting well-placed sources, however, remains difficult and the CIA has had difficulty recruiting qualified officers with necessary language skills.

On September 11, 2001, 19 terrorists turned airplanes into weapons. Some of those hijackers were flagged for additional screening, but the follow-up was lackluster. Others would have been flagged had better information sharing been in place. Along with information sharing improvements, the procedures for identifying airline passengers who should be prevented from boarding an airplane, or be subjected to additional screening, have been greatly enhanced.

The Transportation Security Administration (TSA) now screens the names of all airline passengers against the “no fly” and “automatic selectee” terrorist watchlists before they board an airplane. This is known as the Secure Flight program. Until last year, the airlines had the responsibility of comparing passengers against these watchlists, but that process resulted in numerous errors in missing individuals on the no fly list as well as incorrectly identifying passengers as being the particular individual on the list. It also placed sensitive information in the hands of far too many people, including officials at foreign government-owned airlines. This is an important improvement to our security.



A decade after 9/11, the nation is not yet prepared for a truly catastrophic disaster.

Unity of Command and Effort

**Recommendation: “Emergency response agencies nationwide should adopt the Incident Command System (ICS). When multiple agencies or multiple jurisdictions are involved, they should adopt a unified command. Both are proven frameworks for emergency response. Regular joint training at all levels is ... essential to ensuring close coordination during an actual incident.”**

The 9/11 attacks demonstrated that robust and well-rehearsed emergency response capabilities can be overwhelmed by a significant terrorist attack. In 2005, Hurricane Katrina revealed that a catastrophic natural disaster could produce a chaotic and disorganized response by all levels of government, causing large-scale human suffering. A decade after 9/11, the nation is not yet prepared for a truly catastrophic disaster.

Teamwork, collaboration, and cooperation at an incident site are critical to a successful response, and can save many lives in the face of massive casualties. We therefore recommended that federal, state, and local emergency response agencies nationwide adopt the Incident Command System (ICS); an essential element of this is a unified command with one person in charge of directing the efforts of multiple agencies. This overall commander, we believed, would be best suited to advance the goal of unity of effort.

Following 9/11, DHS incorporated ICS into the National Incident Management System (NIMS). NIMS provides nationwide guidance to clarify the roles of federal, state, and local governments, non-profit organizations, and the private sector in protecting against, responding to, and recovering from disasters, and it is an essential part of the National Response Framework. DHS has trained first responders throughout the country in the operation of NIMS.

All levels of government have concentrated on planning and exercising for disaster response to an extent rarely

seen before the 9/11 attacks. Over the last several years, the federal government has coordinated massive National Level Exercises (NLE), knitting together agencies across the country and around the world. The purpose of the congressionally-mandated, DHS-managed NLE is to prepare and coordinate a multiple-jurisdictional, integrated response to a national catastrophic event. The NLE 2011 scenario took place in May and involved thousands of players representing federal, state, and local agencies at 50 sites across the country. Dozens of foreign countries participated and the private sector played a prominent role in the exercise.

While this represents important progress, the nation’s ability to establish unity of command and effort were put to the test during the 2010 Gulf Coast oil spill. The goal was to provide a unified, coordinated response under the leadership of DHS, with the Coast Guard as lead agency and British Petroleum as the responsible party. The response was divided into four main categories of effort: command, planning, operations, and logistics. This structure allowed each team to grow rapidly as more people arrived to respond to the spill; tens of thousands were ultimately involved.

Management of the crisis was an improvement over the often seriously fragmented approaches taken in response to previous disasters but the response was not without flaws. The Coast Guard Commandant was placed in overall command of the incident, but state and local officials, responding to political pressures, at times focused their efforts on what they judged to be priorities for their constituents. State and local authorities set up their own local command centers and were often at odds with the overall plan for strategic response and clean up, creating resource demands in conflict with the overarching program. The complexity of the problem highlights the difficulty of establishing strong central command and control, and integrating incident response across all levels of government.

Progress continues to be made on unity of effort, but it is far from complete. In order to ensure unity of effort, there

Our discussions with community leaders and first responders indicate that many metropolitan areas, with multiple agencies responding to a disaster, still have not solved the problem of a unified command structure.

must be comprehensive planning across federal agencies and with state and local authorities. The Department of Homeland Security’s Inspector General found that the federal government had not adequately developed catastrophic disaster operations plans to address “specific roles, responsibilities, and actions for each federal department and agency responding to an incident.” Without sufficient planning by the federal government to determine appropriate agency roles and responsibilities, it is impossible for state and local governments to develop operational plans that sync up with the federal government’s plans. As a result, at the site of a catastrophic disaster there could be confusion about who is responsible for which actions, particularly between the federal government and state and local governments.

In 2008, the Federal Emergency Management Agency (FEMA) implemented a pilot program in five states to integrate state and federal catastrophic planning efforts. The program helped the states fill gaps in catastrophic planning and build relationships with FEMA, other states, local governments, and the private sector. However, an April 2011 report by the Government Accountability Office (GAO), found continuing gaps in catastrophic planning in these states. Some states lacked a section on “direction, control, and coordination” in their catastrophic incident plans, and one state estimated that it would take five years before it could complete its catastrophic incident plan. The GAO also found that states had not exercised their catastrophic operational plans to determine effectiveness or clarify change of command. These planning and exercises are essential elements of establishing unity of effort before a disaster strikes.

While the FEMA pilot program that GAO reviewed has been discontinued, states may use grant funding for catastrophic planning. Federal support in the form of grants and direct technical assistance for planning has repeatedly been cited

by states and major urban areas as critical and should be a continued focus area for limited federal preparedness resources.

The executive branch also must ensure that all federal departments and agencies relevant to disaster mitigation and response be involved in disaster planning. Just this year, the administration adopted a major course change to its government-wide approach to catastrophic disaster planning. In March 2011, the president issued a revised directive on disaster preparedness that requires all federal departments and agencies with disaster-response capabilities to develop operational plans in support of interagency planning frameworks. The directive tasks DHS with the responsibility for revising the national preparedness system, in coordination with other federal agencies and all levels of government, in order to provide new guidance “for planning, organization, equipment, training, and exercises to build and maintain domestic capabilities.” As this guidance is released, all levels of government will need to redouble their engagement in planning and exercises to ensure unity of effort.

In addition to the practical implementation of establishing unity of effort planning and exercises, there remain political challenges. Our discussions with community leaders and first responders indicate that many metropolitan areas, with multiple agencies responding to a disaster, still have not solved the problem of a unified command structure. This is a political problem that in most cases must be addressed by state and local government.

While the government has made substantial progress, our recommendation is still a long way from being fully implemented.



Despite the lives at stake, the recommendation to improve radio interoperability for first responders has stalled because of a political fight over whether to allocate 10 MHz of radio spectrum – the D-block – directly to public safety for a nationwide network.

Radio Spectrum and Interoperability

**Recommendation: “Congress should support pending legislation which provides for the expedited and increased assignment of radio spectrum for public safety purposes.”**

The inability of first responders to communicate with each other on demand was a critical failure on 9/11. Incompatible and inadequate communications led to needless loss of life. To remedy this failure, the Commission recommended legislation to provide for the expedited and increased assignment of radio spectrum for public safety purposes.

To date, this recommendation continues to languish. Despite the lives at stake, the recommendation to improve radio interoperability for first responders has stalled because of a political fight over whether to allocate 10 MHz of radio spectrum – the D-block – directly to public safety for a nationwide network, or auction it off to a commercial wireless bidder who would then be required to provide priority access on its network dedicated to public safety during emergencies.

Since 9/11, faltering advances were made as some radio spectrum in the 700 MHz band were allocated to public safety, but it remains largely unused by first responders. The overwhelming majority of our nation’s police chiefs and leaders of first responder agencies support the allocation of the D-block to the existing dedicated public safety spectrum in order to construct a nationwide, interoperable public safety broadband network. This network would allow diverse public safety agencies to communicate with each other, and support mission critical voice, video, text, and other data transmissions.

In his February 2011 State of the Union address, President Obama called for allocating the D-block spectrum to public safety. He also supports allocating \$7 billion in federal funding to support a build-out of the broadband network for cash-strapped localities and rural communities. The

U.S. Senate Commerce Committee voted in June to report legislation to the full Senate that would allocate this spectrum to public safety, but this bill has not passed the Senate and the House has not yet considered similar legislation.

We support the immediate allocation of the D-block spectrum to public safety and the construction of a nationwide, interoperable broadband network. Because we don’t know when the next attack or disaster will strike, we urge the Congress to act swiftly.

Following the allocation of spectrum for public safety use, heavy lifting is needed to deploy an operational nationwide interoperable network. Standards must be established for the public safety broadband network to ensure nationwide interoperability of wireless devices on the network. In addition, wireless devices that operate on the public safety broadband network should be interoperable with devices on other portions of spectrum. This interoperability is important so that a first responder’s public safety network device could also operate on a commercial wireless network if the public safety broadband network transmitter is disrupted, or a first responder moves into an area where the public safety broadband network transmitters have not been deployed, as is likely to be the case in many rural areas.

The public safety broadband network and devices must be integrated with existing narrowband emergency communications technology, procedures, and interoperability plans. To save money, where possible, the public safety broadband network deployment should leverage existing communications infrastructure the federal government has already procured, such as Department of Justice’s Integrated Wireless Network or Customs and Border Protection’s (CBP) Tactical Communications System, and the radio towers that state and local governments have constructed or leased. For example, CBP’s radio towers provide an existing infrastructure base for communications in remote rural areas where there is no other existing communications infrastructure.

The 9/11 Commission recommended creating a Privacy and Civil Liberties Oversight Board to monitor actions across the government. Congress and the president enacted legislation to establish this Board but it has, in fact, been dormant for more than three years.

Civil Liberties and Executive Power

**Recommendation: “[T]here should be a board within the executive branch to oversee adherence to the [privacy] guidelines we recommend and the commitment the government makes to defend our civil liberties.”**

An array of security-related policies and programs present significant privacy and civil liberty concerns. In particular, as the FBI and the rest of the intelligence community have dramatically expanded their surveillance of potential terrorists, they have used tools such as National Security Letters that may implicate the privacy of Americans. Privacy protections are also important in cyber security where the government must work with the private sector to prevent attacks that could disrupt information technology systems and critical infrastructure. The same Internet that contains private correspondence and personal information can also be used as a conduit for devastating cyber attacks.

To ensure that privacy and liberty concerns are addressed, the 9/11 Commission recommended creating a Privacy and Civil Liberties Oversight Board to monitor actions across the government. Congress and the president enacted legislation to establish this Board but it has, in fact, been dormant for more than three years.

The Obama administration recently nominated two members for the Board, but they have not yet been confirmed by the Senate. We take the administration at its word that this Board is important: in its May 2009 review of cyber security policy, the administration noted the Board’s importance for evaluating cyber security policies. We urge the president to appoint individuals for the remaining three positions on the board, including the chairman, immediately, and for the Senate to evaluate their nominations expeditiously.

Despite the faltering progress on the Board, some agencies have established chief privacy officers. We commend

Finally, the public safety broadband network construction process should be managed carefully to avoid cost overruns and ensure that taxpayers get the most value for their dollars. Rigorous oversight by Congress and the administration is needed to monitor progress in establishing the network.

Challenges to the interoperability of other first responder communications networks also require greater attention. Statewide communications interoperability plans and the creation of a national emergency communications plan have advanced emergency coordination across jurisdictions. In addition, DHS has worked with 60 urban areas to successfully demonstrate emergency communications among primary operational leadership, allowing them to manage resources and make timely decisions – within one hour of a routine incident involving multiple agencies.

While this represents progress, taking one hour to establish emergency communications between agency leadership should not be the final goal. That would still be inadequate for an attack on the scale of 9/11, resulting in loss of life. In particular, first responders, not just leadership, need to have the ability to communicate with one another immediately during a disaster.

Across urban areas, regions, and states, coordination and planning must be improved in the areas of technology deployment, standard operating procedures, training, and exercises. Several grant programs at different federal agencies can be used to enhance interoperability, but further efforts are needed to ensure the most effective use of these grants on the highest priority projects, especially with deployment of the public safety broadband network. While expanding the spectrum and resources available to first responders is critical to improving interoperability, these additional issues must be addressed to achieve real-time interoperable communications for catastrophic disasters.

The rules governing congressional organization reflect the needs and economy of the 19th century, not the challenges of the 21st century.

the dedicated efforts of privacy officers in each of the respective agencies with national security responsibilities; they are doing their work with professionalism. In particular, assessments they have authored on the impact of policies, regulations, and directives issued by their respective departments on civil liberties have been strong.

If we were issuing grades, the implementation of this recommendation would receive a failing mark. A robust and visible Board can help reassure Americans that these programs are designed and executed with the preservation of our core values in mind. Board review can also give national security officials an extra degree of assurance that their efforts will not be perceived later as violating civil liberties.

Congressional Reform

**Recommendation: “Congress should create a single, principal point of oversight and review for homeland security. Congressional oversight for intelligence – and counterterrorism – is now dysfunctional.”**

When we issued our 2004 report, we believed that congressional oversight of the homeland security and intelligence functions of government was dysfunctional. It still is. So long as oversight is governed by current congressional rules and resolutions, we believe the American people will not get the security they want and need. The rules governing congressional organization reflect the needs and economy of the 19th century, not the challenges of the 21st century.

We recommended that Congress create a single, principal point of oversight and review for homeland security. This has not been done. The homeland security committees in the House and Senate do not have sufficient jurisdiction over important agencies within the Department of Homeland Security. Instead, jurisdiction has been carved up to accommodate antiquated committee structures. As a result,

too many committees have concurrent and overlapping jurisdiction. This is a recipe for confusion.

This is not just a theoretical problem; it has already produced unclear security policies. The Senate Commerce Committee has jurisdiction over the TSA and has used this authority to set security standards for screening cargo shipped from abroad on airplanes. But cargo shipped on maritime vessels is governed by the security policies of U.S. Customs and Border Protection (CBP), which falls under the jurisdiction of the Senate Homeland Security Committee. Those CBP policies were significantly enhanced by the SAFE Port Act of 2006 in legislation that the Homeland Security Committee produced. The security of cargo should not depend on whether it moves by air or sea and the committee that has jurisdiction over the agency that regulates that method of transit. Both TSA and CBP are part of the Department of Homeland Security and oversight should be with the Senate Homeland Security Committee.

The unwieldy jurisdictional divisions result in the inefficient allocation of limited resources needed to secure our nation. The Department of Homeland Security responds to the inquiries of more than 100 committees and subcommittees. In 2009 and 2010, DHS provided more than 3,900 briefings and DHS witnesses testified more than 285 times. This amounted to many thousands of hours of work, often duplicating efforts, and cost taxpayers tens of millions of dollars.

The result is that DHS receives conflicting guidance and Congress lacks one picture of how that enormous organization is functioning. Congress should be helping integrate the sprawling DHS; a fragmented oversight approach defeats that purpose.

We also recommended that Congress create a Joint Committee for Intelligence or create House and Senate committees with combined authorizing and appropriating powers. Agencies listen to the people who

It still is not clear, however, that the DNI is the driving force for intelligence community integration that we had envisioned.

control their purse, but appropriations for the CIA, for example, come under an already overburdened House Appropriations Subcommittee on Defense. The thrust of our recommendation is to ensure that there is credible, robust expert oversight of the intelligence community’s funding and other activities. Our recommendation would ensure that the intelligence appropriations process is not an appendage to the massive defense budget. The House Permanent Select Committee on Intelligence announced a decision this year to include three Members of the House Appropriations Committee to participate in Intelligence Committee hearings and briefings. This is a positive step, but there is more to do here.

We firmly reinforce what we said in our final report: That it is in our country’s security interest that Congress make committee reform a priority.

Director of National Intelligence

**Recommendation: “The current position of Director of Central Intelligence should be replaced by a National Intelligence Director with two main areas of responsibility: (1) to oversee national intelligence centers on specific subjects of interest across the U.S. government and (2) to manage the national intelligence program and oversee the agencies that contribute to it.”**

As recommended by the 9/11 Commission, Congress created the position of Director of National Intelligence (DNI) as the principal intelligence advisor to the president, responsible for directing and coordinating the efforts of the 16 agencies of the intelligence community. In the six years since the creation of this post, the DNI has increased information sharing, improved coordination among agencies, sharpened collection priorities, brought additional expertise into the analysis of intelligence, and further integrated the FBI into the overall intelligence effort. These are significant achievements.

It still is not clear, however, that the DNI is the driving force for intelligence community integration that we had envisioned. Some ambiguity appears to remain with respect to the DNI’s authority over budget and personnel. Strengthening the DNI’s position in these areas would advance the unity of effort in intelligence, whether through legislation or with repeated declarations from the president that the DNI is the unequivocal leader of the intelligence community.

We are also concerned that there have been four DNIs in six years. Short tenures detract from the goals of building strong authority in the office and the confidence essential for the president to rely on the DNI as his chief intelligence advisor.

Transportation Security

**Recommendation: “The TSA and the Congress must give priority attention to improving the ability of screening checkpoints to detect explosives on passengers. The TSA should expedite the installation of advanced (in-line) baggage-screening equipment.”**

While the TSA’s implementation of airline passenger screening against the “no fly” and “automatic selectee” lists is a major success, we are still highly vulnerable to aviation security threats. We know that al Qaeda and its affiliates are committed to attacking U.S. aviation as evidenced by Umar Farouk Abdulmutallab’s attempt to detonate an explosive on Northwest flight 253 in the skies over Detroit, as well as the insertion of bombs into printer cartridges shipped on airplanes from Yemen to the United States. We also know that Osama bin Laden aspired to attack U.S. rail transportation in New York.

We are not satisfied with improvements to TSA’s explosives screening capability. With significant federal funding, TSA has deployed large numbers of enhanced screening

Despite 10 years of working on the problem, the aviation screening system still falls short in critical ways with respect to detection.

equipment used at passenger checkpoints and baggage check screening. Unfortunately, explosives detection technology lacks reliability and lags in its capability to automatically identify concealed weapons and explosives. The next generation of whole body scanning machines also are not effective at detecting explosives hidden within the body and raise privacy and health concerns that DHS has not fully addressed. Our conclusion is that despite 10 years of working on the problem, the aviation screening system still falls short in critical ways with respect to detection.

The Government Accountability Office (GAO) has cited flaws in the way that the TSA and the DHS Science and Technology Directorate conduct research, development, testing, and evaluation of new technology. GAO has found weaknesses in developing and articulating technology program requirements. Ill-defined requirements make it difficult for the private sector to design cost-effective screening equipment that meets DHS’s needs. In addition, GAO faults TSA for not conducting and completing testing and evaluation of new technologies to ensure that they work in an operational environment, as well as not incorporating cost and benefit information while making technology acquisition decisions. As a result, significant amounts of money have been wasted and the GAO continues to identify serious holes in virtually every security layer. Given the threat we face to our transportation systems, we cannot afford to perpetuate these mistakes.

Biometric Entry-Exit Screening System

**Recommendation: “The Department of Homeland Security, properly supported by the Congress, should complete, as quickly as possible, a biometric entry-exit screening system.”**

One area of great progress in securing our borders is the deployment of the biometric entry system known as US-VISIT. This system checks all individuals who arrive at U.S. borders, ensures they are who they say they are, and helps prevent known terrorists from entering the country. Data

collected by US-VISIT are also used by homeland security, defense, law enforcement, and intelligence agencies for other important national security functions. US-VISIT has proven its value as a national security tool.

Despite the successful deployment of the entry component of US-VISIT, however, there still is no comprehensive exit system in place. As important as it is to know when foreign nationals arrive, it is also important to know when they leave. Full deployment of the biometric exit component of US-VISIT should be a high priority. Such a capability would have assisted law enforcement and intelligence officials in August and September 2001 in conducting a search for two of the 9/11 hijackers that were in the U.S. on expired visas.

Standardize Secure Identifications

**Recommendation: “The federal government should set standards for the issuance of birth certificates and sources of identification, such as drivers licenses.”**

Eighteen of the nineteen 9/11 hijackers obtained 30 state-issued IDs that enabled them to more easily board planes on the morning of 9/11. Due to the ease with which fraud was used to obtain legitimate IDs that helped the hijackers carry out a terrorist act, the 9/11 Commission recommended that “the federal government should set standards for the issuance of birth certificates and sources of identification, such as driver’s licenses.”

The REAL ID Act established these standards by statute. In 2008, detailed regulations were issued setting standards and benchmarks for issuing driver’s licenses. While nearly one-third of the states have complied with the first tier of benchmarks, the deadlines for compliance have been pushed back twice to May 2011, and a recent announcement pushed back compliance again until January 2013. The delay in compliance creates vulnerabilities and makes us less safe. No further delay should be authorized; rather, compliance should be accelerated.

The federal government should set standards for the issuance of birth certificates and sources of identification, such as driver’s licenses.

In addition, there are still no minimum standards for birth certificates in place, as required by the Intelligence Reform and Terrorism Prevention Act of 2004. These standards are needed to close a back door that terrorists could use to obtain driver’s licenses.

Develop Coalition Standards for Terrorist Detention

**Recommendation: “The United States should engage its friends to develop a common coalition approach toward the detention and humane treatment of captured terrorists” and that “[n]ew principles might draw upon Common Article 3 of the Geneva Conventions on the law of armed conflict.”**

Within days of his inauguration, President Obama signed a series of executive orders on the treatment of detainees and barring the CIA from using any interrogation methods not already authorized in the U.S. Army Field Manual. This ended the CIA’s authority to use harsh interrogation methods, but the administration is still grappling with how to close the Guantanamo prison facilities.

By bringing the U.S. into compliance with the Geneva Conventions as well as international and customary law on the treatment of prisoners, these executive orders have substantially fulfilled our recommendation. Looking forward, however, we are concerned that the issue of prisoner treatment has become highly politicized.

This is not good for the country or our standing in the world. Showing that bipartisan agreement is possible, and intending to reaffirm our values, the five Republicans and

five Democrats on the Commission unanimously agreed on this recommendation. Together, we believed that our country’s values require adherence to the rule of law and a commitment to human rights and humane treatment.

A lingering problem that two presidents have confronted is reconciling the rule of law with indefinitely detaining alleged terrorists. For too long, the president and Congress have delayed resolving this difficult problem. In some cases we lack sufficient evidence against the detainees, or the evidence we have is problematic because of the way it was obtained. We regard as positive the Executive Order that requires periodic review of the status of prisoners at Guantanamo. Congress and the president, however, must decide on a comprehensive approach that spells out clearly the rules of evidence and procedures and the forums in which they will be applied. Congress should anchor these decisions in a firm statutory basis.



## Chapter 3: Conclusion

Today, our country is undoubtedly safer and more secure than it was a decade ago. We have damaged our enemy, but the ideology of violent Islamist extremism is alive and attracting new adherents, including right here in our own country. With important 9/11 Commission recommendations outlined in this report still unfulfilled, we fail to achieve the security we could or should have.

The terrorist threat will be with us far into the future, demanding that we be ever vigilant. Changing circumstances require that we regularly reassess our priorities and expenditures to determine what is needed to defend our country and people.

Our terrorist adversaries and the tactics and techniques they employ are evolving rapidly. We will see new attempts, and likely successful attacks. One of our major deficiencies before the 9/11 attacks was a failure by national security agencies to adapt quickly to new and different kinds of enemies. We must not make that mistake again.

Our national security departments require strong leadership and attentive management at every level to ensure that all parts are working well together, and that innovation and imagination are championed. Our agencies and their dedicated workforces enacted much change and we commend their achievements in protecting the American people. But there is a tendency toward inertia in all bureaucracies. Vigorous congressional oversight is imperative to ensure sustained vigilance and continued reforms.

Our task is difficult. We must constantly assess our vulnerabilities and anticipate new lines of attack. We have done much, but there is much more to do.



National Security Preparedness Group

