BIPARTISAN POLICY CENTER

STATEMENT OF TOM KEAN & JAMIE GORELICK

Former 9/11 Commissioners

Today's Rising Terrorist Threat and the Danger to the United States
Testimony before the House Committee on Homeland Security
July 23, 2014

Introduction

Mr. Chairman, Mr. Ranking Member, members of the Committee: We are grateful for the opportunity to appear before you today. This Committee has been at the center of improving our country's defenses against terrorist attacks. We are deeply grateful to you for your sustained support of the 9/11 Commission's recommendations and your leadership in reforming our national security institutions. Overseeing and guiding the Department of Homeland Security, which is still a young and evolving department, is one of the most important national security duties of the Congress. Over the past decade, this Committee has been a steadfast champion of needed reform.

Today, we are appearing in our capacity as former 9/11 Commissioners. Governor Kean and Congressman Hamilton, the Chair and Vice Chair of the 9/11 Commission, now lead the Homeland Security Project at the Bipartisan Policy Center. Drawing on a strong roster of national security professionals, the Project's mission is to be a bipartisan voice on homeland- and national-security issues. It works as an independent group to monitor the implementation of the 9/11 Commission's recommendations and address other emerging threats to our nation.

On July 22, 2004, we issued *The 9/11 Commission Report*, the official report of the devastating attacks of September 11, 2001. Ten years later, the ten former members of the Commission reconvened, under the auspices of the Bipartisan Policy Center, to take stock of the terrorist threat and the country's readiness to face it.

Continuing Terrorist Threat from Al Qaeda and its Affiliates

When we wrote our report ten years ago, we were acutely mindful of the responsibility we bore to the American people—and the families of the victims—to provide the most complete account possible of the events leading up to that terrible day. We used what we learned from that awful history to make recommendations as to how to make America safer. Today, we are pleased that most of those recommendations have been enacted into law or adopted as policy.

A decade after releasing our report, we are struck by how dramatically the world has changed. In the United States, federal, state, and local authorities have implemented major security reforms to protect the country. Overseas, the United States and allies went on the offensive against al Qaeda and related terrorist organizations. Ten years ago, many feared that al Qaeda would launch more catastrophic attacks on the United States. That has not happened. While homegrown terrorists struck Fort Hood and the Boston Marathon, with tragic results, and while major attempted attacks on aviation have been disrupted, no attack on a scale approaching that of 9/11 has taken place.

U.S. and allied efforts have badly hurt "core" al Qaeda, the organization that attacked us on 9/11. Al Qaeda's leadership has been seriously diminished, most notably by the killing of Usama bin Ladin. The blows the United States has dealt those who struck us on 9/11 are a credit to the ceaseless work of dedicated men and women in our military and in our intelligence services, who often serve their country without accolades or even public acknowledgement.

However, the threat from jihadist terrorism persists. While core al Qaeda has been damaged in recent years, its affiliates and associated groups have dispersed throughout the greater Middle East. Al Qaeda spinoffs—some small, some worryingly large—now have a presence in more theaters of operation than they did half a decade ago, operating today in at least 16 countries.

In *The 9/11 Commission Report*, we said that one of the key lessons of the 9/11 story was that there can be "no sanctuaries" for terrorist groups. Geographic sanctuaries (like pre-9/11 Afghanistan) enable terrorist groups to gather, indoctrinate and train recruits, and they offer breathing space in which to develop complex plots (like the 9/11 attacks). The Islamic State in Iraq and Syria ("ISIS") now controls vast swaths of territory in Iraq and Syria, creating a massive terrorist sanctuary. Afghanistan could revert to that condition once American troops depart at the end of 2014. The recent Taliban offensive in Helmand Province illustrates that danger.

Meanwhile, al Qaeda in the Arabian Peninsula ("AQAP") remains interested in striking the United States. The Saudi-born Ibrahim al-Asiri, AQAP's chief bomb maker, devised the underwear bomb worn by Umar Farouk Abdulmuttalab. Al-Asiri remains at large and there are concerns that he is gaining experience in the concealment and miniaturization of bombs and manufacturing them from nonmetallic materials, making them far harder to detect.

More than 10,000 foreign fighters have flooded into Syria. Once there, these fighters have access to on-the-job training in military operations, fashioning improvised explosive devices, and using assault weapons. Many come from Western Europe, but more than 70 are believed to be from the United States. One of these Americans, a Florida man in his early 20s, recently blew himself up in a suicide attack in northern Syria, the first instance of an American suicide bomber there. American counterterrorism and homeland security officials and European allies are deeply concerned that hardened fighters from Syria may redirect their venom and battlefield experience toward the United States or their European countries of origin. In at least one instance, this appears already to have happened: The suspect in the deadly May 24 shooting attack on the Jewish Museum in Brussels had spent more than a year in Syria, where he is believed to have joined up with jihadist groups.

Federal Bureau of Investigation Director James Comey has described the situation in Syria as, in several respects, "an order of magnitude worse" than the terrorist training ground that existed in Afghanistan before 9/11. It is unclear whether the United States and its allies have sufficient resources in place to monitor foreign fighters' activities in Syria (and neighboring Iraq) and to track their travel back to their home countries.

The convulsions across the Muslim world, from the Sahel to Pakistan, create opportunities for extremist groups to work their will. Opportunities to exert power may, to some extent, keep terrorists focused on their home regions. According to the State Department, terrorist attacks rose 43 percent worldwide in 2013. These attacks killed 17,891 and wounded 32,577. The Department reports that the vast majority of these incidents were local or regional, not international, in focus.

It does not follow, however, that terrorist groups have relaxed their enmity toward the United States and its allies. The 2012 attack on U.S. facilities in Benghazi, Libya, resulted in the deaths of four Americans, including the American ambassador. In 2013, al Shabaab attacked the Westgate mall in Nairobi, Kenya, murdering more than 60 innocent people. These are reminders that dedicated terrorists can successfully execute deadly attacks against targets associated with the United States and the West.

Some national security officials believe that the forces of Islamist extremism in the Middle East are stronger than in the last decade. Partly, this is a consequence of the Arab Spring and the power vacuums and ungoverned spaces that have sprung up in its wake. Partly, it is the result of America's inability or reluctance to exert power and influence in a number of places. Officials are also deeply concerned about the region's seemingly endless supply of disaffected young people vulnerable to being recruited as suicide bombers. We explained in *The 9/11 Commission Report* that the "United States finds itself caught up in a clash within a civilization," which "arises from particular conditions in the Muslim world." This clash has only intensified since then.

Our assessment is that the terrorist threat is evolving, not defeated. Al Qaeda's various spinoffs are, at the moment, enmeshed in their own local conflicts, but hatred of the United States remains a common thread. While some of these groups are not capable of striking the U.S. homeland, they may seek to attack outposts of the U.S. presence overseas, including diplomatic posts, military bases, or softer targets such as American businesses in foreign countries.

Homegrown terrorism remains a serious concern as well. Purveyors of hatred spread their radical ideology over the Internet, attempting to recruit new terrorists both abroad and in the United States. The risk is not only that new terrorist cells are being created; online propaganda can also influence "lone wolf" terrorists, who can be extremely difficult for authorities to spot. The support of the American Muslim community in opposing extremism, increased awareness by the public at large, and a massive law enforcement effort have made the United States a much harder target than it was on 9/11. But the tragedy of the Boston Marathon bombing is a reminder of how dangerous homegrown extremists can be, despite these advances.

In sum, the terrorist threat has evolved, but it is still very real and very dangerous. The absence of another 9/11-style attack does not mean the threat is gone: As 9/11 showed, a period of quiet can be shattered in a moment by a devastating attack. The pressing question is whether the United States is prepared to face the emergent threats of today—and those it is likely to face in the years to come.

Unfinished Business

The Intelligence Reform and Terrorism Prevention Act of 2004 ushered in the most significant restructuring of the Intelligence Community since 1947. Despite this progress, some recommendations from *The 9/11 Commission Report* remain unimplemented.

First and foremost is reform of Congress's committee structure for overseeing homeland security. Your Committee is Congress's expert on DHS and should be preeminent in terms of overseeing and legislating for the Department. Our recommendation of ten years ago remains urgent today: "Through not more than one authorizing committee … in each house, Congress should be able to ask the Secretary of Homeland Security whether he or she has the resources to provide reasonable security against major terrorist acts within the United States and to hold the Secretary accountable for the department's performance." Regrettably, an unwieldy hodgepodge of other committees still exercises residual oversight and legislative jurisdiction over DHS. In 2004, we remarked with astonishment and alarm that DHS reported to 88 committees and subcommittees of Congress. Incredibly, DHS reports that that number has since *increased*, to 92.

This is not an academic concern. In *The 9/11 Commission Report*, we said that Congress, as a whole, adjusted slowly to the rise of transnational terrorism as a threat to national security. In the years before September 11, terrorism seldom registered as important, and Congress did not reorganize itself after the end of the Cold War to address new threats. Splintered committee jurisdiction resulted in episodic and inadequate attention to terrorism and to the overarching strategies needed to combat terrorist organizations. Put simply, when everyone is responsible, no one is.

We knew that, of "all our recommendations, strengthening congressional oversight may be among the most difficult." Unfortunately, we were right. While the Executive Branch has, at Congress's behest and urging, undergone historic change and institutional reform, Congress has proved deeply resistant to reforming its own structures for DHS oversight. In particular, it has delayed in yielding to this Committee preeminent authorizing jurisdiction and oversight responsibility over all DHS components.

Again and again, past and present DHS senior managers have told us that this fragmented congressional oversight is counterproductive to national security goals. DHS is still a young department, continually learning and striving to improve. Congress should help guide senior officials in managing the Department as a cohesive whole, rather than as a collection of disparate parts. The proliferation of oversight committees has the opposite effect. More than 90 different committees and subcommittees cannot develop expertise about the Department as a whole. Nor can committees that only oversee certain DHS components understand the effect of what they do on the Department's overall mission, or compare all of the competing priorities among which Department leaders must choose. Emblematic of this inability is the fact that Congress has not, since the Department's creation, enacted a final comprehensive DHS authorization bill setting policy and spending priorities for the Department.

Reporting to this vast array of committees also places an extraordinary administrative burden on DHS, which must prepare reams of written testimony and respond to countless questions for the record. This burden distracts from other, higher-priority tasks.

Effective congressional oversight is especially important in areas, like homeland security, where much of the government's activity necessarily occurs out of public view. Unlike other areas of policy, where the press and public can themselves monitor what their government is doing, the public must rely on Congress to be its eyes and ears with respect to sensitive and classified national security programs.

We have full confidence that this Committee, and the Senate Committee on Homeland Security and Governmental Affairs, have the expertise and focus to best do that job for the American people. It is long past time for other committees to step back and allow you to fully take the reins for DHS. At the very minimum, the next Congress should sharply reduce the number of committees and subcommittees with some jurisdiction over the department. The Department of Homeland Security should receive the same streamlined oversight as the Department of Defense.

These changes should take effect when the next Congress convenes and the House and Senate adopt new rules in January. Planning should begin now to make this possible.

The 9/11 Commission recommended creating a Director of National Intelligence (DNI) to oversee national intelligence centers on specific subjects of interest across the U.S. government, and to manage the national intelligence program and oversee the agencies that contribute to it.

Congress created that office in the Intelligence Reform and Terrorism Prevention Act of 2004. Despite differences of view ten years ago, senior leaders in the Intelligence Community today believe that the Office of the DNI has found its role in the national security apparatus. The DNI has been accepted as the manager of the Community. Joint duty is becoming more common: More than 10,000 Intelligence Community civilian employees are certified as having done joint duty, with 1,000 doing so each year.

Many senior officials told us that personal chemistry among the leaders of the Intelligence Community and Pentagon is as important, if not more important, than legislated authority for the overall smooth and effective functioning of the national security system. It is not just a law that makes an organization or system work—it is the people. The current DNI's conception of his office has enabled him to successfully manage the Community and elicit cooperation from its components. In particular, future DNIs should follow these key policies: (1) coordinating the work of the various intelligence agencies, rather than replicating that work or turning ODNI itself into an operational entity; (2) advancing interagency information sharing, unified IT capabilities, joint duty, and other Community-wide initiatives; and (3) providing centralized budgetary planning to ensure that the Community as a whole possesses the most effective combination of tools.

Today, the Office of the DNI continues to be hampered by Congress's failure to update its practices to reflect post-9/11 reforms. One such anachronism: Intelligence Community funds are not conveyed in a single appropriation. Instead, many Community funds are buried in appropriations for the Department of Defense (DOD), a vestige of bygone days when the top-line intelligence budget was classified. With that figure now a matter of public record, there is no longer any reason to hide intelligence funds in the DOD budget.

A unified Intelligence Community budget, managed by the Director of National Intelligence and overseen by a single subcommittee in each house of Congress, would enable the DNI to manage Community resources without navigating a bureaucratic labyrinth. It would also help ensure better oversight of the intelligence budget. Cohesive and comprehensive oversight of all Intelligence Community funding would be easier if appropriations for all sixteen member agencies, plus ODNI, were conveyed in a single bill.

We believe that there is today greater agreement on this point than ten years ago. We were particularly struck by the statement of a former senior leader of the Department of Defense that the DNI should have full authority to manage the Intelligence Community's budget. To that end, we reiterate our original recommendations: Congress should pass a separate appropriations act for the National Intelligence Program. The DNI should receive all funds appropriated in that bill and have full authority to apportion them among Community agencies and reprogram them as needed to meet new priorities.

The Importance of Data Collection and Analysis

In *The 9/11 Commission Report*, we noted the importance of intelligence collection and analysis in counterterrorism, and we recommended reforms to improve both. Intelligence gathering is the single most effective way to thwart terrorism—but identifying and finding terrorists, who go to great lengths to cover their tracks, is a very difficult task. Often no single report is definitive. Rather, it is the accumulation and filtering of vast amounts of information, zeroing in on what is relevant, that leads to intelligence breakthroughs. This was true of the hunt for bin Ladin, which was conducted over a decade and built on the efforts of hundreds, if not thousands, of intelligence officers.

Data collection and analysis are vital tools for preventing terrorist attacks. Terrorist networks rely on a variety of technologies to communicate, to plan operations, and to recruit new personnel. The government currently makes use of powerful technology to collect and analyze data from communications. Those capabilities will be enhanced as technology advances in the years ahead. As these technical capabilities advance, it will be even more important to define legal parameters that limit these technologies' uses to true needs.

We believe these programs are worth preserving, albeit with additional oversight. Every current or former senior official with whom we spoke told us that the terrorist and cyber threats to the United States are more dangerous today than they were a few years ago. And senior officials explained to us, in clear terms, what authorities they would need to address those threats. Their case is persuasive, and we encountered general agreement about what needs to be done.

Senior leaders must now make this case to the public. The President must lead the government in an ongoing effort to explain to the American people—in specific terms, not generalities—why these programs are critical to the nation's security. If the American people hear what we have heard in recent months, about the urgent threat and the ways in which data collection is used to counter it, we believe that they will be supportive. If these programs are as important as we believe they are, it is worth making the effort to build a more solid foundation in public opinion to ensure their preservation. While the American public has become more skeptical, now is the time to engage them in an honest, transparent discussion of these issues.

Greater oversight would also help bolster these programs' legitimacy. It imperils public and political support for these programs to limit classified briefings on their details (and often existence) to only eight leaders in Congress, the "Gang of Eight." All members of the intelligence oversight committees in the House and Senate should be briefed. The Privacy and Civil Liberties Oversight Board, whose creation was a 9/11 Commission recommendation, is finally functioning, providing an array of well-informed voices on the civil-liberties implications of sensitive national security programs.

Information Sharing

The 9/11 Commission Report said that the "biggest impediment to all-source analysis—to a greater likelihood of connecting the dots—is the human or systemic resistance to sharing information." Before 9/11, the government had a weak system for processing and using the vast pool of intelligence information it possessed. One striking example of this inadequacy: In January 2000, the NSA acquired information that could have helped identify one of the eventual hijackers, Nawaf al Hazmi. This information was not shared with other agencies because no agency made a specific request for it.

Such failures underscore that intelligence-sharing among agencies is critically important and will not happen without leadership driving it.
The tone is set at the top. Information-sharing has improved significantly since 9/11. There is now a regularly scheduled meeting on threats convened by the President and attended by the heads of agencies with responsibilities for counterterrorism. The President is directly involved. This forum helps ensure the President is kept up to date on threats to the country and what each agency is doing in response. The President's active participation ensures that agencies collaborate (rather than compete) and that they are focused on delivering their best. The meeting also enables senior officials to share information with each other. This valuable practice should be carried over into future administrations.

A major step toward improved information-sharing is underway in the form of the Intelligence Community Information Technology Enterprise (ICITE). In this system, the Intelligence Community will have a single desktop for agencies in the Community, providing a common computing environment. Instead of each agency building its own software, which was the practice in the past, the Community is implementing an architecture that will be used by all. Authorized users will be able to use common email and related applications. The Intelligence Community cloud will be privately hosted inside the Intelligence Community itself, managed under the Community's security standards and under the Community's security watch.

The National Counterterrorism Center (NCTC), also a 9/11 Commission recommendation, is performing well. NCTC has helped make progress toward instilling a "need-to-share" culture among agencies responsible for counterterrorism, and we have heard that NCTC has received exceptional cooperation from the key intelligence collectors in the government. In general, we believe that government officials now recognize that the government cannot prevent terrorist attacks without bringing together relevant information from many different sources and agencies. Responsibility for making this a reality ultimately rests with managers in each agency: The system must hold accountable every manager with responsibility for sharing information.

One aspect of information sharing is lagging somewhat. "Vertical" sharing—sharing among federal, state, local, and tribal officials, as well as the private sector—needs attention. Before 9/11, this form of sharing was woefully inadequate. It has improved substantially since then, but the process is still maturing. It is possible that if Boston authorities had been advised of concerns about Boston Marathon bomber Tamerlan Tsarnaev's interest in connecting with overseas extremist elements, they could have kept a watchful eye on him.

We note, however, that this cannot be a one-way street. State and local law enforcement can also be generators of useful information. The 9/11 hijackers had several encounters with local law enforcement during their time in the United States. Tamerlan Tsarnaev also had several run-ins with the law. At a minimum, state and local law enforcement officials should be trained to recognize the precursors of radicalization.

Biometric Exit Tracking

The 9/11 Commission Report identified terrorists' travel and need for identification documents as vulnerable points in their operations. With the REAL ID Act gradually being implemented by the states, the country is poised to fulfill our recommendation that the federal government "set standards for the issuance of birth certificates and sources of identification, such as driver's licenses."

But, as you know, another key recommendation, a biometric exit-tracking system, has still not been implemented, and there is no finish line in sight. Without reliable exit-tracking, our government does not know when a foreign visitor admitted to the United States on a temporary basis has overstayed his or her admission. Had this system been in place before 9/11, we would have had a better chance of detecting the plotters before they struck. Creating an exit-tracking system is a difficult and expensive challenge, but there is no excuse for the fact that 13 years after 9/11 we have neither this capability in place nor a clear plan to get there.

The Cyber Threat

Our mandate as a commission was to recommend national security reforms to prevent another 9/11. In our recent conversations with senior national security leaders, however, we encountered another concern over and over again: intensifying attacks on the country's information systems, in both the private and public sectors.

Over the past decade, cyber threats have grown in scale and intensity, with major breaches at government agencies and private businesses. The threat emanates largely not from terrorist groups but from traditional state actors such as China, Russia, and Iran. The U.S. government has confirmed that Chinese-government-backed hackers gained access to more than two dozen of America's most advanced weapons systems, including missiles, fighter jets, and advanced ships. In September 2013, Iran hacked into U.S. Navy computer systems. Iran has also been behind cyber attacks on banks and oil companies operating in the Middle East. The Shamoon virus, attributed by many to Iran, infected a key state-owned oil company in Saudi Arabia and left 30,000 computers inoperable.

Non-state actors are also causing increasing damage in the digital world. Sophisticated computer hackers have infiltrated, exploited, and disrupted military, government and private-sector systems. Denial-of-service attacks have tied up companies' websites, inflicting serious economic losses. A Russian teenage hacker may have been behind the massive malware attack on the retailer Target, which compromised the credit- and debit-card data of 40 million customers. Increasingly, cyber attacks are targeting smartphones as well. Cyber attacks can constitute another form of asymmetric terrorism. The Syrian Electronic Army is a collection of computer hackers who are loyal to Bashar al-Assad but who operate independently. It has targeted Syrian opposition political groups as well as Western websites. This is the first instance in the Arab world of an organization of civilian cyber experts forming to target groups it deems to be enemies.

Security officials are concerned that terrorist groups' skills in computer technology—and in particular in manipulating offensive cyber capabilities—will increase in the years ahead. Terrorists may also seek to acquire malicious software from adversary nations or from hackers who are proficient at malware coding. This will make an already unpredictable and dangerous cyber realm even more so.

The importance of the Internet to American life and to societies across the globe has expanded at a phenomenal rate. As the country becomes ever more dependent on digital services for the functioning of critical infrastructure, business, education, finance, communications, and social connections, the Internet's vulnerabilities are outpacing the nation's ability to secure it. Just as the United States needs to protect its physical infrastructure, so too must we protect the cyber domain.

A growing chorus of senior national security officials describes the cyber domain as the battlefield of the future. Yet, in the words of one former senior leader with whom we spoke, "We are at September 10th levels in terms of cyber preparedness." That needs to change. One lesson of the 9/11 story is that, as a nation, Americans did not awaken to the gravity of the terrorist threat until it was too late. We must not repeat that mistake in the cyber realm.

Government officials should explain to the public—in clear, specific terms—the severity of the cyber threat and what the stakes are for our country. Public- and private-sector leaders should also explain what private citizens and businesses can do to protect their systems and data.

We support cybersecurity legislation that would enable private companies to responsibly collaborate with the government in countering cyber threats. Companies should be able to share cyber threat information with the government without fear of liability.

The U.S. government can and should do more to deter cyber attacks from state adversaries. The administration should determine and communicate through appropriate channels what the consequences of cyber attacks against us will be, and then act on the basis of those statements. And we should work with our allies to establish norms of cyberspace, clearly defining what is considered an attack by one country on another.

The administration and Congress also need to clearly delineate the respective responsibilities of the various agencies in the cyber realm. DHS and other domestic agencies need to complement, rather than attempt to replicate, the technical capabilities of NSA.

Waning Sense of Urgency Among the American People

One of America's most pressing challenges as a country is to resist the natural urge to relax our guard after 13 years of a draining counterterrorism struggle. In the absence of a major attack, it is easier for some who did not lose loved ones to forget the trauma of 9/11. Increased vigilance has helped us avoid another attack on that scale, but vigilance inevitably wanes over time.

A complacent mindset lulled us into a false sense of security before 9/11. The first World Trade Center bombing in 1993, the East Africa embassy bombings in 1998, and the *Cole* attack in 2000 were warnings of the virulence of the al Qaeda threat. But the United States did not do enough. In particular, the government did not explain to the American people the pattern that was emerging. Without appropriate public understanding, there was insufficient political support for the strenuous counterterrorism efforts that would have been necessary to defeat al Qaeda.

Avoiding complacency also means taking seriously small things that could be warning signs of something larger beginning to take shape. American officials knew suspicious men were attending flight schools, but in the pre-9/11 mindset it was not considered urgent. Is the April 2013 rifle attack on an electrical substation in Metcalf, California, a harbinger of a more concerted assault on the national electrical grid or another component of critical infrastructure? What might we be missing today that, three years from now, will prove to have been a signal, a piece of a larger mosaic?

As we survey the changes in government made during the last decade, it is evident that the government has come a long way. But the threat remains very real, and the United States cannot lose focus now. Terrorists can still hurt Americans, abroad and here at home.

To sustain public support for policies and resource levels, national security leaders must communicate to the public—*in specific terms*—what the threat is, how it is evolving, what measures are being taken to address it, why those measures are necessary, and what specific protections are in place to protect civil liberties. In this era of heightened skepticism, generalities will not persuade the public. Leaders should describe the threat and the capabilities they need with as much granularity as they can safely offer.

Conclusion

Over the last thirteen years, 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.

Our terrorist adversaries and the tactics 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 that our national security agencies were not adapting quickly enough to the new kind of enemy that was emerging. We must not make that mistake again.

While over the past decade our government's record in counterterrorism has been good, the terrorist threat will be with us far into the future, demanding that we be ever vigilant.

Thank you for inviting us to testify, and for this Committee's longstanding leadership on these critical issues.