BIPARTISAN POLICY CENTER

Bipartisan Policy Center

Homeland Security Project

Michael E. Leiter, Task Force Member

Testimony before the House Homeland Security Subcommittee on Oversight, Management and Investigations

September 14, 2012

Introduction

Mr. Chairman, Mr. Ranking Member, members of the Subcommittee: I am pleased to have the opportunity to appear before you today. This Subcommittee has been at the center of ensuring that needed reform is taking place in our government. I am deeply grateful to you for your sustained leadership in that effort. The subject of today's hearing, *"Lessons from Fort Hood: Why Can't We Connect the Dots to Protect the Homeland?"* is of critical importance to national security.

Today, I appear in my capacity as a Task Force Member of the Bipartisan Policy Center's *Homeland Security Project*, a successor to the 9/11 Commission. Drawing on a strong roster of national security professionals, the HSP works as an independent, bipartisan group to monitor the implementation of the 9/11 Commission's recommendations and address other emerging national security issues.

HSP includes the following membership:

> **Governor Thomas H. Kean**, Former Governor of New Jersey; Chairman of the 9/11 Commission; and Co-Chair of the Homeland Security Project;
> **The Honorable Lee H. Hamilton**, Former Congressman from Indiana; Vice-Chair of the 9/11 Commission; and Co-Chair of the Homeland Security Project;
> **Peter Bergen**, Director, National Security Studies Program at the New America Foundation;

Christopher Carney, Former Congressman from Pennsylvania and Chair of the U.S. House Homeland Security Oversight Committee;
Stephen E. Flynn, Ph.D., Founding Co-Director of the George J. Kostas Research Institute for Homeland Security and Professor of Political Science at Northeastern University;
Dr. John Gannon, Former Deputy Director of the CIA for Intelligence;
Dan Glickman, Senior Fellow, Former Secretary of Agriculture; Former Chairman of the U.S. House Intelligence Committee;
Dr. Bruce Hoffman, Director, Center for Peace and Security Studies, Georgetown University;
Michael P. Jackson, Chairman and CEO, VidSys, Inc. and Former Deputy Secretary of the U.S. Department of Homeland Security;
Ellen Laipson, President and CEO of the Stimson Center and member of the President's Intelligence Advisory Board;
Michael E. Leiter, Senior Counselor to the Chief Executive Officer, Palantir Technologies and Former Director of the National Counterterrorism Center;
Edwin Meese III, Former U.S. Attorney General, Ronald Reagan Distinguished Fellow in Public Policy and Chairman of the Center for Legal and Judicial Studies at The Heritage Foundation;
Erroll G. Southers, Former Chief of Homeland Security and Intelligence for the Los Angeles Airports Police Department; and Associate Director of the National Center for Risk and Economic Analysis of Terrorism Events at the University of Southern California;
Richard L. Thornburgh, Former U.S. Attorney General and Governor of Pennsylvania;
Frances Townsend, Former Homeland Security Advisor and Deputy National Security Advisor for Combating Terrorism;
Jim Turner, Former Congressman from Texas and Ranking Member of the U.S. House Homeland Security Committee;

My HSP colleagues and I believe the depth of this group's experience on national security issues can be of assistance to you and the executive branch and we look forward to continuing to work with you.

I will also draw on my experience as former Director of the National Counterterrorist Center (NCTC), a post I stepped down from one year ago. While I will address certain aspects of deficiencies in information sharing surrounding the Fort Hood shootings, I believe I can best help the subcommittee by sharing my views about how well the government is sharing information generally. While my testimony is in part based on my work with the HSP, it does not necessarily reflect the views of my HSP Board Member colleagues.

Now, exactly eleven years after the tragic 9/11 attacks, and eight years since *The 9/11 Commission Report*, is an appropriate time to take stock of how well our government is sharing information.

Overview

The 9/11 Commission documented major failures of national security-related agencies to share vital terrorist-related information in the months and years before the 9/11 attacks. In the pre-9/11 period, legal, policy, and cultural barriers among agencies created serious impediments to information sharing. The Commission made a number of specific recommendations to improve information sharing across our government and regarded it imperative that all levels of government make improvements.

Information sharing within the federal government, and among federal, state, local, and tribal authorities, and with allies, while not perfect, has been considerably improved since 9/11. The level of cooperation among all levels of government is higher than ever. State and local officials have a far greater understanding not only of the threat and how to respond to it but also of their communities and those who may be at risk of radicalization.

The formation of the National Counterterrorism Center (NCTC) was a major step toward improved information sharing. When the follow-on organization to the Commission issued grades and reviews in late 2005 and subsequently, it cited the creation of NCTC and its performance as a success in national security reform. Although I am admittedly biased on this point, I certainly agree that NCTC has played and continues to play a critical information-sharing role.

NCTC's information sharing responsibilities are extremely broad and encompass items that many now take as a given—even though ten years ago they were nonexistent. For example, NCTC's maintenance of a consolidated watchlist that is available to local police during a car stop, foreign service officers checking a visa application, and homeland security professionals at a border, ensure that a critical information sharing gap from 9/11 is filled. Similarly, NCTC's three-times daily video conferences ensure that every element of the U.S. government knows what threats are on the radar. In addition the presence of analysts from more than twenty organizations at NCTC, sitting side-by-side, and sharing information countless times a day is a radical (and positive) shift from 2001. Finally, the Interagency Threat Assessment and Coordination Group (ITACG) provides greater information sharing between state and local officials and the whole of the U.S. Counterterrorism Community. In short, when it comes to information sharing the U.S. government has moved forward in leaps and bounds.

This improvement is, of course, not just because of NCTC but because of an equally concerted effort by the FBI, DHS, and others. Most notably there are now 104 Joint Terrorism Task Forces throughout the nation, and 72 Fusion Centers in which federal, state, local, and tribal authorities investigate terrorism leads and share information. Since 2004, DHS has provided more than $340 million in funding to the Fusion Centers. Information sharing with the private sector has also become routine and is an important part of our defenses.

Despite these improvements, there is no doubt that weaknesses exist—although I frankly believe we must be careful not to equate more recent information sharing failures with those of the past. Information sharing is no more monolithic than any other complex issue or business process. Although information sharing is a good headline, when considering information sharing successes and failures we have to "look under the hood" to see what is really going on, lest we fix things that weren't the problem in the first place.

While the mechanisms are in place for better information sharing, the fact is that we missed opportunities to stop the Christmas Day bomber from boarding Northwest Flight 253, as well as opportunities to intervene before the Fort Hood shootings. In my view each of these represents a different challenge.

With respect to the first, information regarding the bomber was shared and shared widely. In the simplest of terms, the issue was not that people didn't have the data, but instead that they had too much data—and policy issues existed about what steps should be taken based on that data. With respect to the second, relevant information was not sufficiently recognized as such and passed to other operators, and FBI information technology hampered the connection of key data.

An enormous amount of intelligence information constantly pours into our national security system. Sifting through it, synthesizing it, making sense of it, and making sure it receives the necessary attention is a backbreaking challenge, one that requires attentive management and testing to determine where the flaws are and how to fix them. It also requires the latest software and technology to ensure that searches dive into all databases so that no pertinent information on an inquiry fails to be captured. That technology exists and is available today it simply needs to be widely deployed.

Of course, we should not view information sharing as an unmitigated good—or at least not as a good that does not require attendant

modifications to other aspects of intelligence and homeland security as it advances. There is no greater illustration of this than the tragedy of WikiLeaks, which has disclosed to the world—both our adversaries and friends—sensitive information about our intelligence and policies. This publication of sensitive government documents has harmed our government's ability to conduct its affairs and has had serious consequences for our national security.

In my view WikiLeaks demonstrates why as we share information we must also increase our ability to control the information that is shared and take special care to control the wholesale movement of sensitive information *off* of protected networks. It is not new that those who wish to harm the nation will attempt to steal our secrets; it is new that with the spread of electronic information they can steal petabytes rather than mere pages of documents.

Still a Need for Improvement

Where, then, can improvements still be made? We offer some suggestions along the traditional lines of correction: legal, policy, budgetary, personnel, and technology.

With respect to the first, legal, we must recognize that the Constitution and countless statutes govern the mosaic that is information sharing. In my experiences at NCTC, statutes ranging from the Foreign Intelligence Surveillance Act (FISA) to the Violence Against Women's Act drove what could and could not be shared. If there was one statute that was most at issue, however, it was FISA. In my view although FISA obviously provides critical protection of U.S. persons' privacy, it also makes for an exceedingly complex decision making process within the Intelligence Community. Any way in which we can simplify this statute while maintaining protections would be invaluable for both collectors and analysts.

On the policy front, I believe it is important that we accelerate the

review and adoption of Executive Branch implementation guidelines for any information sharing-related policies. In my view the Executive Branch has done an admirable job getting to the right polices in cases like the Attorney General Guidelines for various elements like NCTC, but the time required to adopt such policies borders on the biblical. Yes there are difficult issues that must be addressed, but these issues are too important to allow the process to drag on as it most usually does.

Also on the policy front—but directly related to the budgetary—we remain concerned that FBI and DHS information sharing efforts with State and Local governments lack full cohesion. With declining budgetary resources, it strikes us as important to determine the best way to spend the marginal on DHS-sponsored fusion centers—where today the FBI has more people in place than does DHS. The U.S. Government must, eleven years after 9/11, ensure that respective Departmental foci are consistent with the reality of long-standing intergovernmental relationships and on-the-ground presence. I believe that the FBI's new responsibility as domestic DNI representatives is a very positive step in that direction.

Nowhere will budget play a bigger role in information sharing than state and local fusion centers, which are facing wide and deep budgetary challenges. In addition, budgetary issues will be faced in the context of protecting information from leaks (which is required to enable information sharing), training for personnel on advanced analytic tools that enable information sharing, and having sufficient personnel to collect and exploit information so it can be shared effectively.

On the personnel front, many agencies must continue to train personnel to ensure that they know what information is relevant and hence what must be shared. In particular, the FBI needs to—as it generally has in the past—prioritize enhancing the status of its analysts and ensuring that analysis drives operations. Similarly, DHS must continue to improve its analytic cadre and move away from contract personnel. All analysts and operators must continue to receive high quality training on

issues like radicalization, to recognize signs of danger.

Finally, on the technology front, we continue to face a relative maze of government information systems of significantly varying capability. We cannot be so naïve to say that one big database of information can be created: this is neither technically feasible nor wise as it relates to protection of information and privacy. That being said, we must ensure that operators and analysts have advanced technology that allow them to make connections in disparate data sets, share their knowledge across organizations, and keep information secure. And perhaps most importantly, the Congress must continue to closely monitor government information technology reforms as the bipartisan Executive Branch record on this front is less than inspiring.

Conclusion

In sum, up until now the government's counterterrorism capability has grown with much energy and devotion, but it has done so while flush with resources. The nation's current fiscal situation means we have to be smarter in how we use our resources so that we get the maximum bang for our counterterrorism buck and can stay one step ahead of the ever-changing terrorist threat.

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 that our national security agencies were not changing at the accelerated rate required by a new and different kind of enemy. We must not make that mistake again. Sharing information rapidly is a major comparative advantage we have over terrorists. We must regularly review how we are doing and move quickly to address any problems, fill any gaps that arise.

Thank you for inviting me to testify, and for this Subcommittee's leadership on these critical issues.