UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON TERRORISM AND HOMELAND SECURITY

SENATOR JON KYL
RANKING MEMBER

NINE YEARS AFTER SEPTEMBER 11:

KEEPING AMERICA SAFE

111TH CONGRESS

Report Submitted by Minority Staff

We calculated in advance the number of casualties from the enemy who would be killed based on the position of the [World Trade Center] tower. We calculated that the floors that would be hit would be three or four floors. I was the most optimistic of them all . . . due to my experience in this field, I was thinking that the fire from the gas in the plane would melt the iron structure of the building and collapse the area where the plane hit and all the floors above it only. This is all that we had hoped for.

— *Osama bin Laden*
November 2001[1]

Four years after the attacks of Sept. 11, and one year after the Sept. 11 Commission issued its final report, the desperate aftermath of Hurricane Katrina reminds us how much remains to be done to improve homeland security and emergency preparedness across our country.

— *Thomas Kean and Lee Hamilton*
The 9/11 Public Discourse Project
September 2005[2]

Since that terrible day, we have been spared another major attack on American soil. This is a significant achievement, made possible by the diligence of many courageous Americans defending us at home and overseas. But the threat that struck so terribly on 9/11 remains extremely dangerous. [Al Qaeda] and its affiliates have continued to strike at American and allied interests around the globe . . . These attacks are a reminder that the Al Qaeda network is an adaptable enemy, willing to exploit any complacency or oversights in our defenses. It is also a patient enemy: The attacks of 9/11, for example, were conceived by Khalid Sheik Mohammed in 1996. We can only assume that [Al Qaeda] and its affiliates continue to desire, and plan, further attacks against our homeland.

— *Thomas Kean and Lee Hamilton*
The 9/11 Public Discourse Project
September 2005[3]

---

[1] John Barry and Evan Thomas, *Evil in the Cross Hairs*, NEWSWEEK, Dec. 24, 2001, at 14 (transcript of the Osama bin Laden videotape).

[2] Thomas Kean and Lee Hamilton, *Sept. 11's Unfinished Business*, THE SAN JOSE MERCURY NEWS, Sept. 11, 2005, *available at* http://www.9-11pdp.org/press/2005-09-11_op-ed.pdf.

[3] Thomas Kean and Lee Hamilton, *Reviewing Our Defenses, Four Years After 9/11*, FORWARD, Sept. 9, 2005, *available at* http://www.9-11pdp.org/press/2005-09-09_op-ed.pdf.

TABLE OF CONTENTS

INTRODUCTION

On the morning of September 11, 2001, the nation and the world changed forever when 19 terrorists hijacked four commercial planes: American Airlines Flight 11 crashed into the North Tower of the World Trade Center; United Airlines Flight 175 crashed into the South Tower of the World Trade Center; American Airlines Flight 77 crashed into the Pentagon; and United Airlines Flight 93 crashed in Somerset County, Pennsylvania.[4] Masterminded by Osama bin Laden and his Al Qaeda terrorist network, the attacks killed 3,016 people and wounded thousands more.[5]

On that day, we were "a country awakened to danger and called to defend freedom."[6] The President quickly realized that the key to victory was to take the fight to the terrorists. If we did not take the offensive — draining terrorist "swamps" by eliminating and capturing terrorists wherever they sought haven — we would be forever on the defensive, and the primary battlefield would not be in Iraq or Afghanistan, but right here at home. The magnitude of the challenge is illustrated by the 1984 assassination attempt on Prime Minister Margaret Thatcher by Irish Republican Army terrorists. Their warning — and one that remains relevant today — was: "Remember, we only have to get lucky once; you have to be lucky always."[7] We have done much to turn the odds in our favor, but terrorists remain a grave threat to national security and public safety.

The Subcommittee on Terrorism and Homeland Security focused its efforts during the 111th Congress on securing our borders, protecting personally identifiable information, resolving legal issues related to the war against terrorists, and increasing preparedness in the event of a terrorist attack. To this end, the Subcommittee held hearings on vulnerabilities in the passport adjudication process; strategies for sharing classified information among federal, state, and local

---

[4] *A Nation Challenged: Indictment Chronicles "Overt Acts" That It Says Led to Sept. 11 Attacks*, N.Y. TIMES, Dec. 12, 2001, at B6.

[5] James Barron, *Two Years Later: Ceremonies; Another 9/11, and a Nation Mourns Again*, N.Y. TIMES, Sept. 12, 2003, at A1; David Chen, *Man Behind Sept. 11 Fund Describes Effort as a Success, With Reservations*, N.Y. TIMES, Jan. 1, 2004, at B1.

[6] 147 CONG. REC. S9553 (daily ed. Sept. 20, 2001) (address by Pres. George W. Bush to Joint Session of Congress).

[7] *See, e.g.*, Paul Brown, *Cabinet Survives IRA Hotel Blast*, SUNDAY UK GUARDIAN, Oct. 13, 1984.

governments; techniques for increasing the security of biological laboratories; methods for preventing cybersecurity attacks; deficiencies with the Espionage Act; the establishment of a system of trial and detention that balances the rights of enemy detainees with the need to protect our nation from future attacks; and America's preparedness for responding to potential terrorist attacks using weapons of mass destruction. The attached report is a summary of the Subcommittee's efforts to understand these issues and determine what remains to be done to secure the homeland.

_____

JON KYL

Ranking Member

Subcommittee on Terrorism and Homeland Security

Committee on the Judiciary

United States Senate

Nine Years After September 11: Keeping America Safe

OVERVIEW

In the 111th Congress, the Subcommittee on Terrorism and Homeland Security continued its investigations into ways to keep America safe. The Subcommittee's efforts led to an understanding of potential cybersecurity threats and the need for improved security in the public and private sector; targeted solutions to address barriers to information sharing among federal, state, and local government agencies; a plan for classifying and restricting access to biological agents; measures designed to combat the risk of passport fraud; a critical study of the terrorist detention and trial process; and an understanding of preparedness deficiencies within the government for responding to a terrorist attack using weapons of mass destruction.

The Subcommittee's efforts to promote effective governance require vigorous and effective oversight of the departments within its jurisdiction. Most important, of course, are the Departments of Justice and Homeland Security. The Subcommittee directs significant resources to this oversight and welcomes the submission of briefings or reports that supplement its own independent research. These resources complement the hearing process and serve as mechanisms for further understanding the successes and failures of policies designed to secure the border and combat terrorism.

EXECUTIVE SUMMARY

PROTECTING NATIONAL SECURITY AND CIVIL LIBERTIES: STRATEGIES FOR TERRORISM INFORMATION SHARING

Information sharing among federal, state, and local governments is critical to prevent future terrorist attacks. The Subcommittee convened a hearing to examine strategies that would encourage information sharing among federal, state, and local governments.[1] Privacy concerns have traditionally served as a barrier to information sharing.[2] Other obstacles to information sharing include lack of funding to assign officials to fusion centers,[3] problems with security clearances,[4] and FBI classification of information that may aid local law enforcement investigations.[5] Experts recommend giving priority to information sharing[6] and changing the mindset from a "need to know" to a "need to share" basis.[7] Adopting a decentralized database[8] and implementing privacy guidelines[9] should allay privacy concerns while facilitating information sharing. Implementing the Suspicious Activity Report System (SARS) nationwide should better integrate state and local law enforcement agencies into the federal network.[10]

---

[1] *Protecting National Security and Civil Liberties: Strategies for Terrorism Information Sharing: Hearing Before the Subcomm. on Terrorism and Homeland Security of the Senate Comm. on the Judiciary*, 111th Cong., 1st Sess. (Apr. 21, 2009) at 8-9 (statement of J. Thomas Manger) [hereinafter "Hearing of Apr. 21, 2009"].

[2] Hearing of Apr. 21, 2009, at 2 (statement of Benjamin Cardin).

[3] Hearing of Apr. 21, 2009, at 10-11 (statement of J. Thomas Manger).

[4] Hearing of Apr. 21, 2009, at 10 (statement of J. Thomas Manger).

[5] Hearing of Apr. 21, 2009, at 10 (statement of J. Thomas Manger).

[6] Hearing of Apr. 21, 2009, at 5 (statement of Zoe Baird).

[7] Hearing of Apr. 21, 2009, at 7 (statement of Slade Gorton).

[8] Hearing of Apr. 21, 2009, at 5 (statement of Zoe Baird).

[9] Hearing of Apr. 21, 2009, at 7 (statement of Slade Gorton).

[10] Hearing of Apr. 21, 2009, at 9 (statement of J. Thomas Manger).

THE PASSPORT ISSUANCE PROCESS: CLOSING THE DOOR TO FRAUD

Steps must be taken to improve the security of the passport adjudication process. On March 13, 2009, the Government Accountability Office (GAO) issued details of its undercover operation designed to test the security of the passport application system.[11] The GAO study revealed multiple vulnerabilities in the passport application process, including failure to verify Social Security numbers and inability to detect fraudulent documents.[12] GAO laid out five steps that should be taken to improve the security of the passport adjudication process: (1) devote more training and resources to the issue of passport fraud; (2) examine using commercial options for information verification; (3) develop a self-policing test system; (4) improve access to driver's licenses and vital statistics information; and (5) mandate a 24-hour waiting period for passport approval.[13] The Subcommittee convened a hearing to examine the findings of the report and determine what measures should be taken to ensure that the State Department addresses the failures highlighted in the report.[14] The State Department responded to the criticisms of GAO study by taking immediate steps to improve the security of the passport adjudication process.[15] In addition, the State Department designed a long-term plan, based on GAO's recommendations, to ensure the integrity of American passport issuance.[16]

---

[11] GAO, *State Department: Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process*, GAO-09-447 (Washington, D.C., March 13, 2009) [hereinafter "GAO Rep. of March 13, 2009"].

[12] GAO Rep. of March 13, 2009, Highlights.

[13] *The Passport Issuance Process: Closing the Door to Fraud: Hearing Before the Subcomm. on Terrorism and Homeland Security of the Senate Comm. on the Judiciary*, 111th Cong., 2nd Sess. (May 5, 2009) at 21-22 (statement of Jess Ford) [hereinafter "Hearing of May 5, 2009"]; Hearing of May 5, 2009 at 31-32 (written statement of Jess Ford).

[14] Hearing of May 5, 2009, at 1-2 (statement of Benjamin Cardin).

[15] Hearing of May 5, 2009, at 6, 10, 17, 21 (statement of Brenda Sprague).

[16] Hearing of May 5, 2009, at 6, 7 (statement of Brenda Sprague).

The decision to try terrorists in Article III courts or before military tribunals will be made on a case-by-case basis by joint teams of officials from the Department of Justice (DOJ) and the Department of Defense (DOD).

The Detention Policy Task Force,[17] under the guidance of the DOJ and DOD, issued a protocol laying out factors that DOJ and DOD will use in deciding whether to try a case in an Article III court or in a military commission.[18] The protocol presumes that cases will be prosecuted in an Article III court, but if compelling factors make it more appropriate to prosecute a case in a reformed military commission, it may be prosecuted there.[19] The Subcommittee convened a hearing to examine the factors that DOJ and DOD would consider in deciding whether to try a case in an Article III court or in a reformed military commission.[20] The Subcommittee also looked at the ability of Article III courts to handle cases of suspected terrorists and at the complicated evidentiary and constitutional issues that could arise if detainees were brought into the United States for trial in Article III courts. Concerns were raised about *Miranda* rights; evidentiary issues; the risk of release of suspected terrorists into the United States, either before or after adjudication; and the procedures for safeguarding classified information and intelligence sources. Questions remained about the United States' ability to prevent released detainees from remaining in the country, the application of a voluntariness standard in military commission trials, the ability of the Classified Information Procedures Act (CIPA) to safeguard intelligence, and the application of *Miranda* rights. There was, however, general agreement among the senators and the non-government witnesses that a two-tier system, where the decision of forum depends on the quality of the evidence, risks delegitimizing both Article III trials and military commissions.

---

[17] The Detention Policy Task Force was established pursuant to Executive Order 13493 of January 22, 2009 to identify lawful options for the disposition of individuals captured or apprehended in connection with armed conflicts and counterterrorism operations.

[18] Detention Policy Task Force, *Memorandum for the Attorney General and the Secretary of Defense* (July 7, 2009), *available at* http://www.fas.org/irp/agency/doj/detention072009.pdf [Hereinafter "Detention Policy Task Force Memo"].

[19] Detention Policy Task Force Memo, at 2.

[20] *Prosecuting Terrorists: Civilian and Military Trials for GTMO and Beyond: Hearing Before the Subcomm. on Terrorism and Homeland Security of the Senate Comm. on the Judiciary*, 111th Cong., 1st Sess. (July 28, 2009) [hereinafter "Hearing of July 28, 2009"].

STRENGTHENING SECURITY AND OVERSIGHT AT BIOLOGICAL RESEARCH LABORATORIES

Experts agree that the Department of Health and Human Services should be the lead regulator of biological research laboratory security. The anthrax attacks following the 9/11 terrorist attacks raised concerns in Congress about the procedures in place to protect the nation's biological research laboratories and restrict access to biological agents that can be used as weapons.[21] Because biological agents are likely to be used in future weapons of mass destruction,[22] it is essential for Congress to consider policies that protect against security threats while promoting open and collaborative research.[23] Though studies are still ongoing,[24] it appears that a tiered approach to classifying and accessing biological agents may be a viable method of advancing openness in the research community while maintaining security.[25]

CYBERSECURITY: PREVENTING TERRORIST ATTACKS AND PROTECTING PRIVACY IN CYBERSPACE

Cybersecurity intrusions pose a significant threat to the nation's critical infrastructures. Cybersecurity[26] intrusions occur when criminals, nation-states, or other entities infiltrate our networks and computer systems and steal money, intellectual property, or classified military information.[27] Foreign governments,[28] criminals, and terrorists[29] have exploited weaknesses of the Internet to

---

[21] *Strengthening Security and Oversight at Biological Research Laboratories: Hearing Before the Subcomm. on Terrorism and Homeland Security of the Senate Comm. on the Judiciary*, 111th Cong., 1st Sess. (Sept. 22, 2009) at 3 (statement of Benjamin Cardin) [hereinafter "Hearing of Sept. 22, 2009"].

[22] Hearing of Sept. 22, 2009, at 48 (statement of Robert Graham).

[23] Hearing of Sept. 22, 2009, at 19 (statement of Jean Reed).

[24] Hearing of Sept. 22, 2009, at 17, 18 (statement of Jean Reed).

[25] Hearing of Sept. 22, 2009, at 28 (statement of Jean Reed); Hearing of Sept. 22, 2009, at 81 (statement of Benjamin Cardin).

[26] Cybersecurity includes the strategy, policy, and standards relating to "the security of and operations in cyberspace." Cyberspace Policy Review, at iii, *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[27] Cyberspace Policy Review, at iii, *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[28] Hearing of Nov. 17, 2009, at 6-7 (statement of Jon Kyl).

[29] Hearing of Nov. 17, 2009, at 1 (written statement of Benjamin Cardin).

manipulate or corrupt confidential and classified data used to run the government and private businesses.[30] The Federal Bureau of Investigation, the Department of Justice, and other federal agencies have been successful in investigating and prosecuting cyber-criminals[31] while the Department of Homeland Security and the National Security Agency promote cybersecurity awareness and best practices across both the government and the private sector.[32]

THE ESPIONAGE STATUTES: A LOOK BACK AND A LOOK FORWARD

The Espionage statutes are out of date and need updating in order for the government to successfully prosecute and deter future leaks. The Espionage Act was passed almost 100 years ago,[33] and it is, in some respects, arcane. The hearing focused on current deficiencies and possible solutions. Law professor Stephen Vladeck testified that the Espionage Act is ambiguous and its applicability to various modern situations is unclear.[34] Jeffrey Smith, a member of the CIA Director's External Advisory Board, testified that one primary goal for any update to the law is to include more modern terms to broaden the scope of the law[35]—for example, a statute protecting against leaking secrets that are harmful to national security instead of simply national defense.[36] Authorized leaks,[37] unauthorized leaks,[38] a good motive defense,[39] and the Whistleblower Protection Act[40] were also areas of concern. By

---

[30] Hearing of Nov. 17, 2009, at 1 (written statement of Benjamin Cardin).

[31] Hearing of Nov. 17, 2009, at 10 (statement of James Baker).

[32] Hearing of Nov. 17, 2009, at 20 (statement of Richard Schaeffer); Hearing of Nov. 17, 2009, at 33 (statement of Philip Reitinger).

[33] 18 U.S.C. § 793 (1917).

[34] *The Espionage Statutes: A Look Back and A Look Forward: Hearing Before the Subcomm. on Terrorism and Homeland Security of the Senate Comm. on the Judiciary*, 111st Cong., 2nd Sess. (May 12, 2010) at 10-13 (statement of Stephen Vladeck) [hereinafter "Hearing of May 12, 2010"].

[35] Hearing of May 12, 2010, at 18-19 (statement of Jeffery Smith).

[36] Hearing of May 12, 2010, at 18-19 (statement of Jeffery Smith).

[37] Hearing of May 12, 2010, at 36 (statement of Jon Kyl); Hearing of May 12, 2010, at 44 (statement of Benjamin Cardin).

[38] Hearing of May 12, 2010, at 23-25 (statement of Kenneth Wainstein).

[39] Hearing of May 12, 2010, at 56 (statement of Jon Kyl).

[40] Hearing of May 12, 2010, at 44 (statement of Benjamin Cardin).

clarifying the espionage statutes, the government may be able to better deter and prosecute violations in the future.

THE PASSPORT ISSUANCE PROCESS: CLOSING THE DOOR TO FRAUD, PART II

It is critical that those responsible for processing passport applications have the legal authority, the resources, and the technology to verify the identity of passport applicants and detect fraud. On July 29, 2010, the Subcommittee convened a hearing to investigate the results of a Government Accountability Office (GAO) undercover investigation of the passport issuance system.[41] During GAO's investigation, investigators applied for seven U.S. passports using counterfeit and/or fraudulently obtained driver's licenses, birth certificates, and Social Security numbers.[42] Five U.S. passports were issued and two passport applications were denied.[43] Three of the issued passports were delivered to GAO and two of the issued passports were recovered by the State Department prior to delivery.[44] Although GAO's investigation revealed some progress in verifying Social Security numbers[45] and using facial recognition technology,[46] the inability of the State Department to effectively verify an applicant's driver's license and birth certificate remains a concern.[47] The Subcommittee requested a report on the current state of the passport issuance system[48] and concluded that a comprehensive detection system appears to be the most effective way to improve the State Department's ability to verify the identity of passport applicants and to detect fraud.[49] Senators Cardin, Feinstein

---

[41] The Passport Issuance Process: Closing the Door to Fraud, Part II: *Hearing Before the Subcomm. on Terrorism and Homeland Security of the Senate Comm. on the Judiciary*, 111th Cong., 2nd Sess. (July 29, 2010) at 4 (statement of Benjamin Cardin) [hereinafter "Hearing of July 29, 2010"].

[42] Hearing of July 29, 2010, at 12-13 (statement of Greg Kutz).

[43] Hearing of July 29, 2010, at 13-14 (statement of Greg Kutz).

[44] Hearing of July 29, 2010, at 17 (statement of Brenda Sprague).

[45] Hearing of July 29, 2010, at 30 (statement of Greg Kutz).

[46] Hearing of July 29, 2010, at 14 (statement of Greg Kutz).

[47] Hearing of July 29, 2010, at 30 (statement of Greg Kutz).

[48] Hearing of July 29, 2010, at 50-51 (statement of Jon Kyl).

[49] Hearing of July 29, 2010, at 52-53 (statement of Benjamin Cardin).

and Leiberman of the Subcommittee introduced legislation entitled the Passport Identity Verification Act.[50]

GOVERNMENT PREPAREDNESS AND RESPONSE TO A TERRORIST ATTACK USING WEAPONS OF MASS DESTRUCTION

Steps must be taken to improve the nation's ability to effectively respond to a WMD attack. Experts testified that America is unprepared to respond to bioterrorism or electromagnetic pulse attacks, [51] and suggested that the lack of central authority figures in these areas [52] and a general lack of understanding of the threats[53] are highly influential factors in nation's unpreparedness. According to DOJ's Office of Inspector General, DOJ's response program is uncoordinated and fragmented.[54] DOJ is, however, in the process of implementing recommendations offered by its OIG in order to better its preparedness.[55] The National Capital Region Coordination has taken many steps to try to ensure response preparedness in the capital area, including the fostering of strong partnerships with local authorities.[56]

---

[50] Hearing of July 29, 2010, at 5 (statement of Benjamin Cardin).

[51] *Government Preparedness and Response to a Terrorist Attack Using Weapons of Mass Destruction: Hearing before the Subcomm. on Terrorism and Homeland Security of the Senate Comm. on the Judiciary*, 111th Cong., 1st Sess. (Aug. 4, 2010) at 32 (statement of Randall Larsen) [hereinafter "Hearing of Aug. 4, 2010"]; Hearing of Aug. 4, 2010, at 4 (statement of Jon Kyl).

[52] Hearing of Aug. 4, 2010, at 2 (written statement of Randall Larsen); Hearing of Aug. 4, 2010, at 44 (statement of Michael Frankel).

[53] Hearing of Aug. 4, 2010, at 4 (written statement of Randall Larsen).

[54] Hearing of Aug. 4, 2010, at 9 (statement of Glenn Fine).

[55] Hearing of Aug. 4, 2010, at 15 (statement of James Baker).

[56] Hearing of Aug. 4, 2010, at 17 (statement of Steward Beckham).

PROTECTING NATIONAL SECURITY AND CIVIL LIBERTIES: STRATEGIES FOR TERRORISM INFORMATION SHARING

INTRODUCTION

Improving information sharing across federal, state, and local governments could help prevent terrorist attacks. Information sharing improves law enforcement and intelligence community access to timely and accurate information that is essential to thwarting national security threats.[57] Despite this benefit, privacy concerns must be a consideration when developing information sharing networks because law enforcement and intelligence agencies will be reluctant to participate without appropriate safeguards that the information they contribute will be secure.[58]

The Subcommittee held a hearing on April 21, 2009, entitled "Protecting National Security and Civil Liberties: Strategies for Terrorism Information Sharing,"[59] to examine how the federal government could facilitate information sharing among federal, state, and local governments, while balancing national security with privacy interests.

Four experts testified at the hearing: (1) Zoe Baird, President, Markle Foundation; Co-Chair, Markle Foundation Task Force on National Security in the Information Age; (2) Slade Gorton, former United States Senator for Washington; Member, Markle Foundation Task Force on National Security in the Information Age; (3) J. Thomas Manger, Chief of Police, Montgomery County, MD; Chairman, Legislative Committee, Major Cities Chiefs Association; and (4) Caroline Fredrickson, Director, Washington Office, American Civil Liberties Union.

---

[57] The Markle Foundation, *Nation at Risk: Policy Makers Need Better Information to Protect the Country*, March 2009, at 3, *available at* http://www.markle.org/downloadable_assets/20090304_mtf_report.pdf.

[58] The Markle Foundation, *Nation at Risk: Policy Makers Need Better Information to Protect the Country*, March 2009, at 4, *available at* http://www.markle.org/downloadable_assets/20090304_mtf_report.pdf.

[59] *Protecting National Security and Civil Liberties: Strategies for Terrorism Information Sharing: Hearing Before the Subcomm. on Terrorism and Homeland Security of the Senate Comm. on the Judiciary*, 111th Cong., 1st Sess. (Apr. 21, 2009) (Sat 3 (statement of Benjamin Cardin) [hereinafter "Hearing of Apr. 21, 2009"].

THE IMPORTANCE OF INFORMATION SHARING

Since the 9/11 attacks, information sharing among law enforcement and intelligence agencies has been an important component of the government's national security strategy. As Senator Cardin noted in his opening statement, protecting the American people is "one of the most important functions of government."[60] Indeed, the failure to share information among different levels of government was a contributing factor in the 9/11 attacks. According to the National Commission on Terrorist Attacks Upon the United States, a lack of effective information sharing resulted in ten missed opportunities to prevent the 9/11 attacks.[61] With that in mind, Senator Kyl noted that information sharing "is an important issue because it directly affects our nation's ability to respond to ongoing threats, such as radical Islamists and the drug trafficking organizations that operate along our southern border."[62]

Although the government has increased its efforts to encourage information sharing in the wake of 9/11, Ms. Baird, president of the Markle Foundation and Co-Chair of the Markle Foundation Task Force on National Security in the Information Age, testified that more must be done. Because of limited collaboration in the law enforcement and intelligence communities, our nation still cannot "connect the dots."[63] Federal agencies possess certain information, while state and local governments have different pieces of information.[64] Without collaboration, the information retained by each level of government may be worthless because it does not reveal a complete picture.[65]

Former Senator and current member of the Markle Foundation Task Force on National Security in the Information Age, Slade Gorton, warned, "Success breeds complacency . . . And that means that people are paying attention to other matters, and that complacency . . . is the cause of the great risks that we run at the present time."[66] To decrease the likelihood of another domestic terrorist attack, and to protect our cyber and energy infrastructure, the development of information

---

[60] Hearing of Apr. 21, 2009, at 2 (statement of Benjamin Cardin).

[61] The Markle Foundation, *Nation at Risk: Policy Makers Need Better Information to Protect the Country*, March 2009, at 3, *available at* http://www.markle.org/downloadable_assets/20090304_mtf_report.pdf.

[62] Hearing of Apr. 21, 2009, at 85 (written statement of Jon Kyl).

[63] Hearing of Apr. 21, 2009, at 4 (statement of Zoe Baird).

[64] Hearing of Apr. 21, 2009, at 14-15 (statement of Zoe Baird).

[65] Hearing of Apr. 21, 2009, at 14 (statement of Zoe Baird).

[66] Hearing of Apr. 21, 2009, at 8 (statement of Slade Gorton).

sharing networks must remain a national priority.[67] Ms. Baird emphasized this point at the hearing:

> [O]ur country will not be able to address any of the threats . . . unless we have the best information and we are able to use that information effectively to understand those threats; and to use that information in a way that builds public confidence in the government; and in the government's understanding constraints as well as its powers.[68]

If information sharing becomes less of a priority in the law enforcement and intelligence communities, our nation's vulnerability to another domestic attack will likely increase.

PROGRESS ON INFORMATION SHARING

The catastrophe of 9/11 served as an impetus for the development of our nation's information sharing systems, which were essentially nonexistent prior to that date.[69] Senator Cardin noted that a restructuring of federal agencies led to the formation of the Department of Homeland Security, a Director of National Intelligence, and the National Counterterrorism Center.[70] Each of these newly formed entities was able to dedicate more staff and resources to improving the nation's information sharing network by establishing subdivisions to foster information sharing with state and local law enforcement. For example, the Joint Terrorism Task Force (JTTF) within the Department of Justice and fusion centers within the Department of Homeland Security are the result of efforts across the federal, state, and local levels.[71]

Although the nation's information sharing networks have improved since the attacks of 9/11, Thomas Manger, Chief Manger, Chief of Police, Montgomery County, MD, stated that those improvements are insufficient;[72] state and local law enforcement agencies still may not have timely access to federal databases, hindering their ability to protect our nation. To remedy persistent shortcomings in our nation's information sharing network, Senator Cardin

---

[67] Hearing of Apr. 21, 2009, at 5 (statement of Zoe Baird).

[68] Hearing of Apr. 21, 2009, at 4 (statement of Zoe Baird).

[69] Hearing of Apr. 21, 2009, at 8 (statement of J. Thomas Manger).

[70] Hearing of Apr. 21, 2009, at 2 (statement of Benjamin Cardin).

[71] Hearing of Apr. 21, 2009, at 2 (statement of Benjamin Cardin).

[72] Hearing of Apr. 21, 2009, at 8 (statement of J. Thomas Manger).

recommended that the Subcommittee "evaluate whether [these departments] are working as appropriately as we think they should" and investigate whether the government has "overcome the bureaucratic obstacles to get information to those who can prevent a terrorist attack."[73] Congress must continue to assist state and local law enforcement agencies in communicating with federal databases.[74] As an example, Senator Kyl noted that although critical information about terrorist and drug cartel activity exists in federal databases, local law enforcement officials do not have this information when it is needed most,[75] such as when the police stop someone on a traffic charge, but "only later find out that the car was owned by a drug dealer or had been stolen or was operated by someone known to be a carrier for the cartel."[76]

PRIVACY CONCERNS: OVERCOMING BARRIERS TO FULL PARTICIPATION AND COOPERATION

Privacy concerns have acted as barriers to information sharing.[77] As Senator Cardin noted, national security is not the only concern in improving information sharing — a balance must be achieved "in protecting the security of the people of our country and protecting the civil liberties which are the values of our [n]ation."[78]

Creation of effective privacy controls in an information sharing network depends on the full participation and cooperation of the network's members. Government agencies may be reluctant to participate unless adequate privacy controls exist to secure the information. Ms. Baird stated at the hearing: "[T]he privacy and civil liberties policies that are needed governmentwide are also critical to empower government . . . because, by and large, most government employees do not want to do something that is wrong."[79] Senators Cardin and Kyl agreed that to encourage full participation and cooperation among the members of an information sharing network, the network must implement adequate privacy protections to secure information contributed by government agencies.[80]

---

[73] Hearing of Apr. 21, 2009, at 2 (statement of Benjamin Cardin).

[74] Hearing of Apr. 21, 2009, at 22, 23 (statement of Jon Kyl).

[75] Hearing of Apr. 21, 2009, at 22 (statement of Jon Kyl).

[76] Hearing of Apr. 21, 2009, at 22 (statement of Jon Kyl).

[77] Hearing of Apr. 21, 2009, at 2 (statement of Benjamin Cardin).

[78] Hearing of Apr. 21, 2009, at 3 (statement of Benjamin Cardin).

[79] Hearing of Apr. 21, 2009, at 4 (statement of Zoe Baird).

[80] Hearing of Apr. 21, 2009, at 2 (statement of Benjamin Cardin); Hearing of Apr. 21, 2009, at 86-87 (written statement of Jon Kyl).

ISSUES IN IMPROVING INFORMATION SHARING

While adopting appropriate privacy protections is important to developing effective information sharing networks, a number of other barriers obstruct the complete information sharing among federal, state, and local law enforcement agencies, including a lack of funding, security clearance issues, and the automated classification of information through the Guardian system. Chief Manger emphasized the importance of integrating law enforcement into the intelligence community, testifying that "[f]ederal agencies, despite their ever-improving efforts, have . . . yet to completely leverage the vast resources of our Nation's police and sheriffs."[81]

Funding is a major problem when local law enforcement agencies are trying to connect to an information sharing network.[82] For example, to fully connect with the local Joint Terrorism Task Force (JTTF)[83] or fusion center,[84] law enforcement agencies must subsidize the cost of at least one official to work in the JTTF center.[85] Thus, law enforcement agencies must assign, and potentially hire, additional officers in order to participate in the reciprocal exchange of information.[86] If police agencies have inadequate funds to assign someone to the local JTTF or fusion center, they are "likely to get their most timely threat information from the media."[87]

Access to information sharing networks is further hindered because state and local law enforcement find it difficult to obtain security clearances through the FBI and DHS. Although the FBI and

---

[81] Hearing of Apr. 21, 2009, at 8 (statement of J. Thomas Manger).

[82] Hearing of Apr. 21, 2009, at 10 (statement of J. Thomas Manger).

[83] "Joint Terrorism Task Forces (JTTFs) are small cells of highly trained, locally based, passionately committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. It is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement." DOJ, Joint Terrorism Task Force (April 12, 2010), *available at* http://www.usdoj.gov/jttf/.

[84] "The Fusion Center Guidelines define a fusion center as 'a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.'" John Rollins, *Fusion Centers: Issues and Options for Congress*, Congressional Research Service Rept. No. RL34070, at 1 n.2 (Jan. 18, 2009), *available at* http://ftp.fas.org/sgp/crs/intel/RL34070.pdf.

[85] John Rollins, *Fusion Centers: Issues and Options for Congress*, Congressional Research Service Rept. No. RL34070, at 30-31 (Jan. 18, 2009), *available at* http://ftp.fas.org/sgp/crs/intel/RL34070.pdf.

[86] Hearing of Apr. 21, 2009, at 20 (statement of Benjamin Cardin).

[87] Hearing of Apr. 21, 2009, at 10 (statement of J. Thomas Manger).

DHS both provide clearance to local law enforcement, "there has been little progress in accomplishing a process for reciprocal acceptance of those clearances to access systems and conduct briefings."[88] Chief Manger testified that "[r]efusal by one Federal agency to routinely accept the clearances issued by another is a disruptive policy that contradicts information sharing and threatens our progress."[89] Ideally, the standards should be the same for both the FBI and DHS clearances, so that if one agency gives an officer security clearance, the other agency will as well.

Another obstacle arises when law enforcement agencies share information through the Guardian system.[90] Chief Manger testified that "[i]f the FBI decides to enter . . . information into the Guardian system for further investigation by the JTTF, the information immediately becomes classified."[91] This limits local law enforcement's access to the information at times when it "may very well need to access the [Guardian system] in order to get the missing dot that makes the connections."[92] While the use of the Guardian system signifies a step in the right direction, further integration of state and local law enforcement into the system may be necessary for a truly reciprocal and effective information sharing regime.

How Can We Improve Information Sharing?

Each witness offered several suggestions to improve our nation's information sharing networks. Ms. Baird advised the federal government to give priority[93] to information sharing by having the President "convene a Cabinet meeting to affirm information sharing as a top priority and to help overcome the bureaucratic resistance and turf wars that stymie the process."[94] Additionally, the President should move the Program Manager for the Information Sharing Environment

---

[88] Hearing of Apr. 21, 2009, at 10 (statement of J. Thomas Manger).

[89] Hearing of Apr. 21, 2009, at 10 (statement of J. Thomas Manger).

[90] "The Guardian system allows users to enter, assign, and manage terrorism threats and suspicious activities in a paperless environment, and it allows all field offices and Joint Terrorism Task Force (JTTF) members to view information simultaneously." FBI, Frequently Asked Questions (May 8, 2009), *available at* http://www.fbi.gov/hq/nsb/nsb_faq.htm .

[91] Hearing of Apr. 21, 2009, at 10 (statement of J. Thomas Manger).

[92] Hearing of Apr. 21, 2009, at 14 (statement of Benjamin Cardin).

[93] Hearing of Apr. 21, 2009, at 5 (statement of Zoe Baird).

[94] The Markle Foundation, *Nation at Risk: Policy Makers Need Better Information to Protect the Country*, March 2009, at 9, *available at* http://www.markle.org/downloadable_assets/20090304_mtf_report.pdf.

(PM-ISE) into the Executive Office of the President to give the PM-ISE policy clout and assure that the PM-ISE has a lead role in coordinating "all information sharing policy development and implementation across the government, including the intelligence, law enforcement, and homeland security communities."[95] Ms. Baird also advised Congress to hold hearings on information sharing, and the President to order a "high-level review of the current policy and privacy guidelines and processes,"[96] because without establishing information sharing as a top priority, no further steps can be taken to achieve national, cyber, or border security.[97]

Federal, state, and local government officials must alter their approach from one of withholding information to one of sharing information. For example, Ms. Baird stated that "both Congress and the Administration need to find ways to encourage people to come into the modern age, to encourage people to change their work habits, to become collaborative, to understand that agency lines are not written around the current-day problems that we face."[98] According to Senator Gorton, one way to achieve this goal involves changing the information sharing mindset from a "need-to-know" to a "need to share" basis,[99] with the burden resting on "those who would not share rather than the other way around."[100]

Another way to improve information sharing involves the key elements of discoverability and authorized use.[101] Discoverability gives users "the ability to discover data that exists elsewhere," a necessary component to any information sharing system.[102] An authorized use standard allows an agency or its employees to "obtain mission-based or threat-based permission to discover, access, or share information, as opposed to the current system that relies on place-of-collection rules, U.S. persons status, and originator-control limitations."[103] Merging

---

[95] *Id.* at 10.

[96] *Id.*

[97] Hearing of Apr. 21, 2009, at 4 (statement of Zoe Baird).

[98] Hearing of Apr. 21, 2009, at 6 (statement of Zoe Baird).

[99] Hearing of Apr. 21, 2009, at 7 (statement of Slade Gorton).

[100] Hearing of Apr. 21, 2009, at 7 (statement of Slade Gorton).

[101] Hearing of Apr. 21, 2009, at 5 (statement of Zoe Baird).

[102] The Markle Foundation, *Nation at Risk: Policy Makers Need Better Information to Protect the Country*, March 2009, at 11, *available at* http://www.markle.org/downloadable_assets/20090304_mtf_report.pdf.

[103] The Markle Foundation, *Nation at Risk: Policy Makers Need Better Information to Protect the Country*, March 2009, at 12-13, *available at* http://www.markle.org/downloadable_assets/20090304_mtf_report.pdf.

these two concepts creates a system where the information is easily accessible, but only by users who have a specific and official purpose to obtain the information.

In combination with the concepts of discoverability and authorized use, Ms. Baird advocated adopting a decentralized database. A decentralized database is a system in which "the participants share directly with one another,"[104] rather than submitting information to a central hub. The information "stay[s] with those who collect it and who can keep it accurate enough and up to date."[105] The information submitted to the database must also be tagged and placed in electronic directories.[106] To share the data among different levels of government while retaining privacy, Ms. Baird suggested a system containing only limited personally identifiable information.[107] However, in a limited system, a piece of intelligence information that one individual has may not tell the whole picture,[108] "[s]o you need to be able to ensure that that information gets connected up with other people who might have other pieces of information."[109]

The experts also suggested that "while the Obama Administration has started very well in setting out a philosophy for privacy, it needs to enforce a uniform policy on all of the agencies of government, and it needs to make that policy enforceable, not just a set of suggestions."[110] Due to the differences between the intelligence and law enforcement agencies, Ms. Baird suggested that different rules may need to be promulgated for each sector.[111] For instance, rules may be less rigid in the intelligence context because "a law enforcement investigation brings the power of government behind it; whereas, an intelligence investigation might not have the same consequences for an individual."[112]

Importantly, privacy guidelines must be clear and easy to implement. Senator Kyl advised that these guidelines be "done in a

---

[104] *Id*. at 18.

[105] Hearing of Apr. 21, 2009, at 5 (statement of Zoe Baird).

[106] Hearing of Apr. 21, 2009, at 5 (statement of Zoe Baird).

[107] Hearing of Apr. 21, 2009, at 14, 15 (statement of Zoe Baird).

[108] Hearing of Apr. 21, 2009, at 14 (statement of Zoe Baird).

[109] Hearing of Apr. 21, 2009, at 14 (statement of Zoe Baird).

[110] Hearing of Apr. 21, 2009, at 7 (statement of Slade Gorton).

[111] Hearing of Apr. 21, 2009, at 19 (statement of Zoe Baird).

[112] Hearing of Apr. 21, 2009, at 19 (statement of Zoe Baird).

very usable way,"[113] because without such clarity, government officials will err on the side of inaction, rather than sharing information that may not be authorized.[114] Senator Kyl expressed concern that unclear guidelines may advance "the wall of separation that existed before 9/11, where an arbitrary legal standard prevented the sharing of data."[115]

To foster information sharing with state and local governments, Chief Manger suggested that the federal government fully implement the Suspicious Activity Report System (SARS).[116] SARS is a nationwide initiative that provides "consistent criteria and consistent training to all law enforcement personnel," and has the ability to connect events that would not have been connected in the past.[117] "The SARS process has directly enhanced the ability of local police to protect our communities from violent crime including terrorism. Above all, the SARS process can and will be done in a manner that protects the privacy, civil liberties, and civil rights of all."[118] Senator Kyl and Chief Manger expressed the view that it was appropriate for JTTFs to investigate leads from suspicious activity reports and then determine whether information such as "names should go in the data-base."[119] The success of SARS hinges on adequate funding and careful analysis as to what information should be catalogued in the system.[120]

CONCLUSION

Federal, state, and local governments must continue to improve information sharing. To achieve this goal, the federal government must make information sharing a priority.[121] The federal government should consider nationwide implementation of SARS to better integrate state and local governments with the federal government.[122] Congress and the Administration must employ a combination of these initiatives to move forward and improve information sharing among the federal, state, and local governments.

---

[113] Hearing of Apr. 21, 2009, at 23 (statement of Jon Kyl).

[114] Hearing of Apr. 21, 2009, at 24 (statement of Zoe Baird).

[115] Hearing of Apr. 21, 2009, at 23 (statement of Jon Kyl).

[116] Hearing of Apr. 21, 2009, at 9 (statement of J. Thomas Manger).

[117] Hearing of Apr. 21, 2009, at 9 (statement of J. Thomas Manger).

[118] Hearing of Apr. 21, 2009, at 9 (statement of J. Thomas Manger).

[119] Hearing of Apr. 21, 2009, at 18 (statement of J. Thomas Manger).

[120] Hearing of Apr. 21, 2009, at 22 (statement of J. Thomas Manger); Hearing of Apr. 21, 2009, at 22 (statement of Jon Kyl).

[121] Hearing of Apr. 21, 2009, at 5 (statement of Zoe Baird).

[122] Hearing of Apr. 21, 2009, at 9 (statement of J. Thomas Manger).

THE PASSPORT ISSUANCE PROCESS: CLOSING THE DOOR TO FRAUD

INTRODUCTION

A passport issued by the State Department's Bureau of Consular Affairs "not only allows an individual to travel freely in and out of the United States, but also can be used to obtain further identification documents, prove U.S. citizenship, and set up bank accounts. . . ."[123] Passports are generally considered one of the most secure forms of identification in the United States,[124] but that perception of security also makes fraudulently obtained passports a commodity among those engaged in unlawful activity.[125] After stealing an American citizen's identity, "terrorists or criminals could . . . use basic counterfeiting skills to create fraudulent documents for that identity, and obtain a genuine U.S. passport from [the State Department]."[126] According to the Government Accountability Office (GAO), since "passports issued under a false identity help enable individuals to conceal their movements and activities, there is great concern that passport fraud could facilitate acts of terrorism."[127]

On March 13, 2009, GAO released a report on its undercover investigation to determine vulnerabilities in the passport adjudication process.[128] The report detailed multiple weaknesses in the security of the passport issuance process. On May 5, 2009, the Subcommittee convened a hearing entitled "The Passport Issuance Process: Closing the Door to Fraud" to investigate the findings of GAO report. Two witnesses provided testimony at the hearing: Brenda S. Sprague, Deputy Assistant Secretary for Passport Services, Bureau of Consular Affairs, U.S. State Department; and Jess T. Ford, Director, International Affairs and Trade Team, U.S. Government Accountability Office.

---

[123] GAO, *State Department: Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process*, GAO-09-447, at 1 (Washington, D.C., March 13, 2009) [hereinafter "GAO Rep. of March 13, 2009"].

[124] *The Passport Issuance Process: Closing the Door to Fraud: Hearing Before the Subcomm. on Terrorism and Homeland Security of the Senate Comm. on the Judiciary*, 111th Cong., 2nd Sess. (May 5, 2009) at 1 (statement of Benjamin L. Cardin) [hereinafter "Hearing of May 5, 2009"]; Hearing of May 5, 2009, at 2 (statement of Jon Kyl).

[125] Hearing of May 5, 2009, at 28 (written statement of Jess Ford).

[126] GAO Rep. of March 13, 2009, Highlights.

[127] Hearing of May 5, 2009, at 28 (statement of Jess Ford).

[128] GAO Rep. of March 13, 2009; Hearing of May 5, 2009, at 1 (statement of Benjamin Cardin).

GAO'S UNDERCOVER TESTS REVEAL SIGNIFICANT ADJUDICATION FAILURES

GAO conducted an undercover test of the passport issuance process.[129] For the test, GAO developed four scenarios to "simulate the actions of a malicious individual who had access to another person's identity information."[130] Using counterfeit or fraudulently obtained driver's licenses, birth certificates, and Social Security numbers, GAO's undercover investigator was able to obtain four passports.[131] In one case, the investigator obtained a passport using counterfeit documents and the Social Security number (SSN) of a man who had died in 1965.[132] In another case, the 53-year-old investigator was issued a passport despite having used counterfeit documents and a SSN belonging to a fictitious five-year-old.[133]

In all four cases, the inappropriate issuance of passports was attributed to adjudication failures by State Department personnel. For instance, those reviewing the fraudulent passport applications failed to compare and verify the supplied SSNs against the records of the Social Security Administration.[134] They also failed to detect the counterfeit birth certificates and driver's licenses used in the undercover operation.[135] Finally, State Department personnel failed to recognize that one individual had submitted multiple applications and, in doing so, had provided identification representing himself as four different individuals.[136]

---

[129] GAO Rep. of March 13, 2009; Hearing of May 5, 2009, at 20 (statement of Jess Ford).

[130] GAO Rep. of March 13, 2009, at 4.

[131] Hearing of May 5, 2009, at 20 (statement of Jess Ford); GAO Rep. of March 13, 2009, at 4.

[132] Hearing of May 5, 2009, at 20 (statement of Jess Ford); GAO Rep. of March 13, 2009, at 4.

[133] Hearing of May 5, 2009, at 20 (statement of Jess Ford); GAO Rep. of March 13, 2009, at 4.

[134] Hearing of May 5, 2009, at 4 (statement of Dianne Feinstein); GAO Rep. of March 13, 2009, at 6-9.

[135] Hearing of May 5, 2009, at 1 (statement of Benjamin Cardin); GAO Rep. of March 13, 2009, at 6-9.

[136] Hearing of May 5, 2009, at 4 (statement of Dianne Feinstein); GAO Rep. of March 13, 2009, at 6-9.

CAUSES OF ADJUDICATION FAILURES

One weakness in the passport issuance process identified by GAO's investigation and discussed extensively at the Subcommittee's hearing involved the failure of individual passport specialists to verify the results of the required Social Security database check before approving applications.[137] Due to the many errors in the Social Security database, those responsible for reviewing passport applications have considerable discretion in determining the validity of SSNs.[138] Passport specialists may even approve an application before receiving the results of the required Social Security database check, although the State Department officially disapproves of this practice.[139] Ms. Sprague, Deputy Assistant Secretary for Passport Services, Bureau of Consular Affairs, U.S. State Department, contended that, without such a degree of discretion, the passport issuance process would be hindered by trivial data errors.[140]

Under current law, while SSNs are requested as part of an application, an application cannot be denied because of the failure to submit a SSN,[141] although such a failure will subject the application to additional scrutiny.[142] In the second half of 2009, 72,000 out of six million passports issued did not have a SSN included in the application.[143] Ms. Sprague reported that children under the age of one, who often do not yet have SSNs, submit most of these applications.[144]

Beyond issues associated with verifying SSNs, adjudication failures also occur because the State Department and various departments of federal and state governments fail to share information. Mr. Ford, Director of International Affairs and Trade Team, U.S. Government Accountability Office, reported that the State Department has insufficient access to state level records of birth certificates and driver's licenses, thereby making it difficult or impossible to verify the authenticity of these documents.[145] Additionally, in 2005, GAO reported that the State Department did not check applications against

---

[137] Hearing of May 5, 2009, at 20 (statement of Jess Ford).

[138] Hearing of May 5, 2009, at 9, 10-11 (statement of Brenda Sprague).

[139] Hearing of May 5, 2009, at 9-10 (statement of Brenda Sprague).

[140] Hearing of May 5, 2009, at 9, 10-11 (statement of Brenda Sprague).

[141] Hearing of May 5, 2009, at 12 (statement of Brenda Sprague).

[142] Hearing of May 5, 2009, at 13 (statement of Brenda Sprague).

[143] Hearing of May 5, 2009, at 18 (statement of Jon Kyl).

[144] Hearing of May 5, 2009, at 18 (statement of Brenda Sprague).

[145] Hearing of May 5, 2009, at 20, 24 (statement of Jess Ford).

the federal government's consolidated terrorist watch list or the wanted criminal list of federal and state law enforcement agencies.[146]

Furthermore, GAO reported in 2007 that the State Department had no oversight program for the 9,500 passport application acceptance agencies, most of which are post offices. The lack of oversight made it impossible to ensure that fraud was not occurring at the application level.[147] The State Department has begun to address this problem, but the solution is not fully implemented.[148]

A final issue is that passport specialists have not been successful in realizing when supporting documents such as birth certificates are obvious counterfeits.[149] In GAO tests, the investigator used only commercially available hardware, software, and materials to produce the counterfeit identification documents.[150]

GAO Recommendations

In its report, GAO made five recommendations to reduce vulnerabilities in the passport adjudication process.[151] It recommended that the State Department: (1) "do more training and devote more resources to the whole issue of passport fraud, particularly with detecting false and counterfeit documents"; (2) "explore using commercial options to provide real-time checks on the validity of Social Security numbers and other information on applicants"; (3) develop ''red teams'' to conduct intrusive tests and search their systems for vulnerabilities; (4) "work with State-level officials to gain better access to the key information that they need on driver's licenses and vital statistics to help ensure that the documents they receive are authentic"; and (5) "wait 24 hours before they approve passports from Social Security except under extenuating circumstances."[152]

GAO has previously made recommendations similar to those of the 2009 report, but the State Department has failed to implement many of these. Director Ford stated that the State Department

---

[146] Hearing of May 5, 2009, at 20 (statement of Jess Ford).

[147] Hearing of May 5, 2009, at 20 (statement of Jess Ford).

[148] Hearing of May 5, 2009, at 20 (statement of Jess Ford).

[149] Hearing of May 5, 2009, at 25 (statement of Jess Ford).

[150] GAO Rep. of March 13, 2009, at 3.

[151] Hearing of May 5, 2009, at 21-22 (statement of Jess Ford); Hearing of May 5, 2009, at 21-22, at 31-32 (written statement of Jess Ford).

[152] Hearing of May 5, 2009, at 21-22 (statement of Jess Ford); Hearing of May 5, 2009, at 31-32 (written statement of Jess Ford).

"continues to struggle with reducing fraud risk that we had previously identified . . . in 2005 and in 2007."[153] In 2005, GAO specifically reported that individuals often used stolen documents to obtain fraudulent passports.[154] Senator Cardin referenced the previous GAO reports and the State Department's own internal report from 2008, which both demonstrated that serious problems persist: "there have been previous GAO reports with similar findings and similar efforts and commitments made to correct the failures of the system . . . but [State Department officials] have failed to effectively address these vulnerabilities."[155] Mr. Ford cautioned that "some of the vulnerabilities will be closed," but "we have been down this road before with [the State Department]."[156]

Although the State Department has a poor record of taking corrective action in the passport issuance process, Mr. Ford did applaud the State Department for taking GAO's most recent investigation seriously. According to Mr. Ford, State Department officials "sincerely indicated that [officials] needed to address the vulnerabilities that [GAO] found," and took the time to meet with GAO's investigators and audit officials.[157]

STATE DEPARTMENT TAKES IMMEDIATE ACTION

In response to GAO's report, the State Department took several steps designed to prevent passport fraud. It suspended the adjudication authority of the four passport specialists responsible for wrongly issuing passports to GAO's investigator.[158] It provided refresher courses in counterfeit document detection to all passport specialists and their managers[159] and modified its performance standards for passport specialists to place further emphasis on fraud prevention.[160] The State Department also eliminated production targets,[161] requirements for how many passports a specialist should process in a certain period of time.[162] The State Department conducted

---

[153] Hearing of May 5, 2009, at 23 (statement of Jess Ford).

[154] Hearing of May 5, 2009, at 20 (statement of Jess Ford).

[155] Hearing of May 5, 2009, at 2 (statement of Benjamin Cardin).

[156] Hearing of May 5, 2009, at 23 (statement of Jess Ford).

[157] Hearing of May 5, 2009, at 23 (statement of Jess Ford).

[158] Hearing of May 5, 2009, at 6 (statement of Brenda Sprague).

[159] Hearing of May 5, 2009, at 6 (statement of Brenda Sprague).

[160] Hearing of May 5, 2009, at 6 (statement of Brenda Sprague).

[161] Hearing of May 5, 2009, at 21 (statement of Jess Ford).

[162] Hearing of May 5, 2009, at 23 (statement of Jess Ford).

an audit of all current applications, and the "[p]assport specialists were only released from the audit when they had demonstrated to their supervisors that they were processing work in full compliance with adjudication standards."[163] The State Department also began to require passport acceptance facilities to photocopy all identification documentation submitted by applicants in order to create a permanent record.[164] In addition, all passport acceptance facilities are now required to use a traceable delivery method when transmitting passport applications to the Department.[165]

Additionally, the State Department increased the level of supervisory oversight required for "Will Call" or same-day applications.[166] Same-day passport issuances have been restricted "to truly life-and-death emergencies."[167] All other applications can no longer move through the system in fewer than 24-hours, thereby ensuring that the results from the Social Security database are returned in time to stop an application if a SSN discrepancy is found.[168]

STATE DEPARTMENT ADDRESSES LONG-TERM CHANGES TO REDUCE FRAUD

The State Department is working to implement long-term changes to reduce passport fraud. To facilitate this process, the Department created an "Adjudication Policy and Process Review Working Group" in March 2009 to help identify additional failures in the passport application process and recommend solutions for all identified issues.[169] The working group consists of five subgroups: (1) Restructuring of Adjudication Process and Oversight, which will review "the current adjudication program" and consider restructuring various aspects of the program as well as consider modifying the program's "managerial oversight function";[170] (2) Adjudication Requirements and Standards, which will develop standardized adjudication procedures and develop procedures specifically pertaining to the Social Security database as well as commercial databases;[171] (3) Post-Issuance Audit,

[163] Hearing of May 5, 2009, at 6 (statement of Brenda Sprague).

[164] Hearing of May 5, 2009, at 3 (statement of Brenda Sprague).

[165] Hearing of May 5, 2009, at 3 (statement of Brenda Sprague).

[166] Hearing of May 5, 2009, at 6 (statement of Brenda Sprague).

[167] Hearing of May 5, 2009, at 17 (statement of Brenda Sprague).

[168] Hearing of May 5, 2009, at 10 (statement of Brenda Sprague).

[169] Hearing of May 5, 2009, at 6 (statement of Brenda Sprague).

[170] Hearing of May 5, 2009, at 6 (statement of Brenda Sprague).

[171] Hearing of May 5, 2009, at 7 (statement of Brenda Sprague).

which will develop "a statistically valid audit process for previously issued passports" to be used for training future passport specialists;[172] (4) Training Initiatives, which will identify "enhancements for fraud training for all passport specialists, supervisors, and fraud prevention managers";[173] and (5) Technology, which will identify "technical and procedural vulnerabilities" in the application process and work on improving the State Department's automated systems, specifically access to more databases.[174] These subgroups have submitted formal recommendations to the State Department.[175] In response to those recommendations, the Department has instituted a number of improvements in the adjudication process. For instance, the Department now conducts comprehensive post-issuance audits of statistically-valid sample groups of DS-11 passport applications to detect any fraud or identify specialist error trends.[176] In addition, the Department has adopted the uniform passport adjudication procedures and production standards developed by the Adjudication Requirements Standards subgroup, which have been incorporated into passport specialist performance plans for the new rating cycle.[177] Furthermore, the Department established a new Office of Adjudication responsible for adjudication policy, standardization, and oversight based on the recommendation of the Restructuring of Adjudication Process and Oversight subgroup.[178]

The State Department also identified a number of specific changes it is implementing in response to GAO's concerns. The State Department is attempting to gain access to, and set up verification systems with, a number of outside databases on the state and federal levels. The State Department purchased a subscription to the Social Security Death Master File, which will provide weekly updates of deaths recorded by the Social Security Administration.[179]

On the state level, the State Department is working to obtain access to driver's license records through the American Association of Motor Vehicles.[180] Additionally, the Bureau of Diplomatic Security is

---

[172] Hearing of May 5, 2009, at 7 (statement of Brenda Sprague).

[173] Hearing of May 5, 2009, at 7 (statement of Brenda Sprague).

[174] Hearing of May 5, 2009, at 7 (statement of Brenda Sprague).

[175] Hearing of May 5, 2009, at 1 (statement of Brenda Sprague).

[176] Hearing of May 5, 2009, at 1 (statement of Brenda Sprague).

[177] Hearing of May 5, 2009, at 2 (statement of Brenda Sprague).

[178] Hearing of May 5, 2009, at 2 (statement of Brenda Sprague).

[179] Hearing of May 5, 2009, at 21 (statement of Jess Ford).

[180] Hearing of May 5, 2009, at 21 (statement of Brenda Sprague).

assisting the Bureau of Consular Affairs (the State Department's passport agency) in obtaining access to an unspecified national law enforcement database.[181] Finally, the Department has asked all state registrars for assistance in providing birth and death records.[182] The State Department has gained access to the National Association of Public Health Statistics Information Systems, an incomplete but growing database of all states' birth records.[183] While fewer than half of the states are tied into that database, all 50 states plus the District of Columbia should be included by December 2010.[184]

The State Department is also working to create a facial recognition system to prevent passport fraud.[185] Passport services recently began using a facial recognition system as part of a pilot program at the Colorado and Dallas passport agencies.[186] The system is capable of comparing applicants' photos against multiple "galleries" of images.[187] By utilizing the facial recognition system, the State Department will be able to prevent the issuance of passports to individuals using false identities and those who should be denied passports for other legal reasons.[188] The pilot program, which may ultimately involve up to five agencies, is scheduled to run until the end of 2010.[189] The Department plans to eventually deploy the technology to all agencies and centers.[190] The full system will compare applicants' photos to all previously issued passport photos, approximately 92 million altogether.[191] Senator Kyl expressed a desire to have the system automatically compare applicants' photos to driver's license records,[192] but Ms. Sprague does not believe the State Department could obtain that level of access to the records.[193] The Department would, however,

---

[181] Hearing of May 5, 2009, at 13 (statement of Brenda Sprague).

[182] Hearing of May 5, 2009, at 7 (statement of Brenda Sprague).

[183] Hearing of May 5, 2009, at 16 (statement of Brenda Sprague).

[184] Hearing of May 5, 2009, at 16 (statement of Brenda Sprague).

[185] Hearing of May 5, 2009, at 7 (statement of Brenda Sprague).

[186] Subcomm. on Terrorism and Homeland Security of the Senate Comm. on the Judiciary, *Questions Relating to Improvements to Passport Issuance Process*, May 5, 2009, at 2 (response by the State Department).

[187] Hearing of May 5, 2009, at 2 (statement of Brenda Sprague).

[188] Hearing of May 5, 2009, at 2 (statement of Brenda Sprague).

[189] Hearing of May 5, 2009, at 2 (statement of Brenda Sprague).

[190] Hearing of May 5, 2009, at 2 (statement of Brenda Sprague).

[191] Hearing of May 5, 2009, at 15 (statement of Brenda Sprague).

[192] Hearing of May 5, 2009, at 15 (statement of Jon Kyl).

[193] Hearing of May 5, 2009, at 15 (statement of Brenda Sprague).

like the passport specialists to be able to manually compare the driver's license photos with the photo submitted with the application.[194]

The State Department is also working to improve several other areas of the application process. As recommended by GAO, the Department is setting up its own undercover tests to verify that its systematic weaknesses are being eliminated.[195] It is also working to standardize the adjudication system platforms that passport specialists currently use domestically and overseas into one universal and more consistent platform.[196] Finally, the State Department is also working to increase the oversight of passport acceptance facilities. To that end, it established the Acceptance Facility Oversight (AFO) office, a division of the Office of Passport Integrity and Internal Affairs.[197] The AFO office conducts site visits to acceptance facilities and is currently in the process of developing an integrated statistics database to evaluate, track, and monitor acceptance facility performance.[198]

FULL IMPLEMENTATION OF REAL ID REQUIREMENTS MAY HELP TO AVERT FRAUD

Since the REAL ID Act[199] was passed in 2005, some have argued that the requirements placed on driver's licenses are too stringent.[200] However, Senator Kyl warned that "weakening the REAL ID driver's license requirements [might] . . . end up making it possible for more criminals, terrorists, and others to get fraudulent passports and thereby pose an additional risk to the country."[201] Ms. Sprague concurred with Senator Kyl and stated that she was "very enthusiastic about tougher standards for driver's licenses" and opposed loosening the REAL ID requirements.[202]

Mr. Ford also stated that, in general, GAO would share the "view that weakening the REAL ID driver's license requirements would

---

[194] Hearing of May 5, 2009, at 15 (statement of Brenda Sprague).

[195] Hearing of May 5, 2009, at 11 (statement of Brenda Sprague).

[196] Hearing of May 5, 2009, at 7 (statement of Brenda Sprague).

[197] Hearing of May 5, 2009, at 3 (statement of Brenda Sprague).

[198] Hearing of May 5, 2009, at 3 (statement of Brenda Sprague).

[199] REAL ID Act of 2005, Pub.L. No. 109-13, 119 Stat. 302 (2005).

[200] Jaikumar Vijayan, *Real ID opposition sparks revisions to national driver's license standard*, COMPUTERWORLD, June 15, 2009, *available at* http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9134404&intsrc=news_ts_head.

[201] Hearing of May 5, 2009, at 3 (statement of Jon Kyl).

[202] Hearing of May 5, 2009, at 13 (statement of Brenda Sprague).

be a bad thing."[203] He highlighted the ease with which, in the recent undercover tests, a GAO investigator had used a counterfeit D.C. identification to obtain an official government identification document that the GAO investigator in turn used to obtain a passport.[204]

CONCLUSION

The State Department and Congress must work together to eliminate existing weaknesses in the passport adjudication process.[205] Senators Cardin and Kyl requested a memo from Ms. Sprague detailing how action in Congress, such as legislation designed to support the REAL ID program, could help prevent the issuance of fraudulent passports.[206] The Subcommittee also requested the results of State Department's internal tests of passport issuance, and Ms. Sprague agreed to provide those results.[207] The Subcommittee again investigated the passport adjudication process in a hearing on July 29, 2010.

---

[203] Hearing of May 5, 2009, at 22 (statement of Jess Ford).

[204] Hearing of May 5, 2009, at 22 (statement of Jess Ford).

[205] Hearing of May 5, 2009, at 25 (statement of Benjamin Cardin).

[206] Hearing of May 5, 2009, at 14 (statement of Jon Kyl), at 16 (statement of Benjamin Cardin).

[207] Hearing of May 5, 2009, at 11.

PROSECUTING TERRORISTS: CIVILIAN AND MILITARY TRIALS FOR GUANTANAMO AND BEYOND

INTRODUCTION

On July 28, 2009, the Subcommittee held a hearing entitled "Prosecuting Terrorists: Civilian and Military Trials for Guantanamo and Beyond" to consider the preliminary report prepared by the Detention Policy Task Force under the guidance of the Departments of Justice and Defense.[208] As part of the preliminary report, the Detention Policy Task Force issued a protocol for the determination of Guantanamo cases referred for prosecution. The protocol laid out factors the Departments of Justice and Defense would consider in deciding whether to try a case in an Article III court or in a reformed military commission.

Two panels of witnesses testified at the hearing. Representing the Administration were David Kris, Assistant Attorney General, National Security Division, Department of Justice, and Jeh Charles Johnson, General Counsel, Department of Defense. The second panel consisted of three expert witnesses: (1) David Laufman, former Assistant U.S. Attorney for the Eastern District of Virginia and chief of staff to the Deputy Attorney General; (2) Deborah Pearlstein, Woodrow Wilson School for Public and International Affairs, Princeton University, founding director of law and security programs at Human Rights First, member of American Bar Association Advisory Committee on Law and National Security; and (3) Michael Edney, Gibson, Dunn & Crutcher, former White House legal advisor to the National Security Council.

THE PROTOCOL DEVELOPED BY THE DETENTION POLICY TASK FORCE

The protocol developed by the Detention Policy Task Force provides that there is "a presumption that, where feasible, . . . cases should be prosecuted in Article III federal courts. Nonetheless, where other compelling factors make it more appropriate to prosecute a case in a reformed military commission, it may be prosecuted there."[209]

---

[208] *Prosecuting Terrorists: Civilian and Military Trials for GTMO and Beyond: Hearing Before the Subcomm. on Terrorism and Homeland Security of the Senate Comm. on the Judiciary*, 111th Cong., 1st Sess. (July 28, 2009) [hereinafter "Hearing of July 28, 2009"].

[209] Hearing of July 28, 2009, at 120 (written statement of Jeh Johnson).

According to Assistant Attorney General Kris, the decision to prosecute in Article III courts or military commissions will be made on a case-by-case basis by joint teams of officials from the Department of Justice (DOJ) and the Department of Defense (DOD).[210] The protocol "recognizes the existence of two prosecution fora," both considered by this Administration to be effective and legitimate, and "provides that the choice between them needs to be made by professionals looking closely at the facts of each case, using flexible criteria established by policymakers."[211] Kris listed three main groups of factors that would govern the forum selection: (1) strength of interest in the forum; (2) efficiency; and (3) the ability to display or convey the full misconduct of the accused.[212] The decision to prosecute in an Article III court will be made by the Attorney General after consultation with the Secretary of Defense.[213]

The witnesses agreed that, in many terrorism cases, either Article III courts or military commissions could be used to obtain convictions.[214] They raised concerns, however, about evidentiary issues, including the necessity of *Miranda* warnings; the ability to protect classified information and sources; the risk of loss of credibility due to a two-tier system; and the potential complications of trying detainees on U.S. soil.

THE ABILITY OF ARTICLE III COURTS TO TRY TERRORISM CASES

Kris stated that Article III courts could handle terrorism cases.[215] David Laufman, former Assistant U.S. Attorney for the Eastern District of Virginia and chief of staff to the Deputy Attorney General, added that, while trying terrorism cases in federal courts does impose additional logistical and security demands on courthouse personnel and the U.S. Marshals Service, the demands are not unreasonable.[216]

On the question of whether terrorists could be successfully incarcerated in civilian detention facilities in the United States,

---

[210] Hearing of July 28, 2009, at 7 (statement of David Kris).

[211] Hearing of July 28, 2009, at 17 (statement of David Kris).

[212] Hearing of July 28, 2009, at 14 (statement of David Kris).

[213] Hearing of July 28, 2009, at 9 (statement of David Kris).

[214] Hearing of July 28, 2009, at 11.

[215] Hearing of July 28, 2009, at 10 (statement of David Kris).

[216] Hearing of July 28, 2009, at 135 (written statement of David Laufman).

Laufman stated that the United States has successfully detained terrorists in facilities in the United States.[217] He stated the government's current authority to detain persons prior to charging them in terrorism-related cases, outside of the military detention model, is limited to the material witness statute, pretrial detention under the Bail Reform Act, and immigration detention, in the case of foreign nationals.[218] Nevertheless, the rules for the detention of a person who has been charged with a federal crime are favorable to the government in terrorism cases, because in terrorism cases a rebuttable presumption in favor of detention exists if there is probable cause that the defendant committed a "federal crime of terrorism."[219] He added that "[m]ore often than not in terrorism cases, courts have either ordered pre-trial detention or authorized release subject to restrictive conditions."[220] Michael Edney, former White House legal advisor to the National Security Council, cautioned that "[i]f imprisoned in the United States, Guantanamo detainees can be expected to seek judicial review of decisions about isolation from other prisoners, the quality and quantity of food, and the amount of daily exercise."[221] In particular, the Religious Freedom Restoration Act would apply to detainees held in the United States, limiting restrictions that could be placed on a detainee's ability to gather with other detainees to worship.[222]

EVIDENTIARY ISSUES

Senators questioned whether existing rules of evidence and criminal procedure in Article III courts are adequate to handle terrorism trials. In particular, questions were asked about *Miranda* rights, chain of custody, hearsay, and confidential information. On the issue of whether *Miranda* warnings are ever permitted to interfere with American military or intelligence gathering operations, Kris assured the senators that no new policy existed as to *Miranda* warnings and that the decision to mirandize continued to be decided on a case-by-case basis.[223] According to Kris, less than one percent of interviews are preceded by a *Miranda* warning.[224] Kris further stated that *Miranda*

---

[217] Hearing of July 28, 2009, at 33 (statement of David Laufman).

[218] Hearing of July 28, 2009, at 135 (written statement of David Laufman).

[219] Hearing of July 28, 2009, at 136 (written statement of David Laufman).

[220] Hearing of July 28, 2009, at 137 (written statement of David Laufman).

[221] Hearing of July 28, 2009, at 60 (Michael Edney's response to written questions).

[222] Hearing of July 28, 2009, at 60-61 (Michael Edney's response to written questions).

[223] Hearing of July 28, 2009, at 15 (statement of David Kris).

[224] Hearing of July 28, 2009, at 15 (statement of David Kris).

warnings are not used by soldiers on the battlefield and are not allowed to interfere with force protection and intelligence collection.[225] Jeh Johnson, General Counsel, Department of Defense, clarified that the only circumstance in which *Miranda* warnings are given is where the law enforcement prosecution option is one that is being considered and military intelligence collection options have been exhausted.[226]

Senator Sessions inquired whether more *Miranda* warnings must be given if a presumption exists that suspected terrorists are going to be tried in civilian courts.[227] Kris responded that giving a *Miranda* warning keeps the option of criminal prosecution in Article III courts open, but, since intelligence costs may be involved, it will be necessary to strike a balance one case at a time.[228] In addition, Kris pointed out that *Quarles*[229] provides exceptions to *Miranda* for public safety, so it is not always necessary to give *Miranda* warnings.[230]

Edney agreed that a statement used in court must be "mirandized," but he raised a further concern as to the introduction of a voluntariness standard into military commissions.[231] Edney argued that introducing a voluntariness standard would result in the same inquiry as in *Miranda*[232] and would, therefore, put the military under pressure to choose between gathering intelligence and making sure that suspects are not released because the statement was not taken properly on the battlefield.[233]

Senator Kyl asked whether the presumption for Article III courts "would . . . increase the situations in which *Miranda* warnings are given"[234] and, therefore, directly conflict "with the first priority, which is getting good military intelligence . . . ."[235] Kris testified that

---

[225] Hearing of July 28, 2009, at 15, 63-64 (statement of David Kris).

[226] Hearing of July 28, 2009, at 25 (statement of Jeh Johnson).

[227] Hearing of July 28, 2009, at 22 (statement of Jeff Sessions).

[228] Hearing of July 28, 2009, at 22-23 (statement of David Kris).

[229] New York v. Quarles, 467 U.S. 649 (1984) (holding that there is a "public safety" exception to the requirement that *Miranda* warnings be given before a suspect's answers may be admitted).

[230] Hearing of July 28, 2009, at 22 (statement of David Kris).

[231] Hearing of July 28, 2009, at 49 (statement of Michael Edney).

[232] Miranda v. Arizona, 384 U.S. 436 (1966).

[233] Hearing of July 28, 2009, at 49 (statement of Michael Edney); Hearing of July 28, 2009, at 62-65 (Michael Edney's response to written questions).

[234] Hearing of July 28, 2009, at 28 (statement of Jon Kyl).

[235] Hearing of July 28, 2009, at 29 (statement of Jon Kyl).

gathering intelligence and protecting troops would be the paramount concern.[236] He added that, in cases where *Miranda* warnings have not been given, an Article III trial might still be possible given a sufficiency of other evidence, but conceded that it would be ideal to try to anticipate the endgame of the process at the earliest possible stage.[237]

Senator Hatch expressed concerns about chain of custody, noting that in battlefield situations it could be difficult to preserve the chain of custody.[238] Senator Hatch asked how the government intended to address the fact that much of the evidence that will be introduced in federal criminal prosecutions of detainees was obtained for intelligence purposes and the government might be unwilling or unable to produce the source.[239] Kris responded that there are "some differences in the rules that govern between the Article III courts and military commissions," and the protocol recognizes that choice of forum may be influenced by legal or evidentiary problems.[240]

As far as the ability of Article III courts to protect classified information, both Kris and Laufman touted the Classified Information Procedures Act (CIPA) as the main mechanism for protecting sensitive information from disclosure.[241] Despite concerns expressed by Senator Kyl that intelligence information had been compromised in earlier criminal trials of terrorists,[242] Laufman asserted that there were "no proven examples of disclosures at trial resulting in the compromise of sensitive intelligence sources and methods."[243] Edney disagreed that CIPA provided adequate safeguards; he urged the government to take a critical look at CIPA if it wants to try detainees in federal court.[244] According to Edney, CIPA was not designed for the situation at hand; it was not tailored to a standing armed conflict:[245] "CIPA was designed for trials against those suspected of espionage . . . to protect classified information already possessed by the defendant from further public

---

[236] Hearing of July 28, 2009, at 28 (statement of David Kris).

[237] Hearing of July 28, 2009, at 30 (statement of David Kris).

[238] Hearing of July 28, 2009, at 16 (statement of Orrin Hatch).

[239] Hearing of July 28, 2009, at 17 (statement of Orrin Hatch).

[240] Hearing of July 28, 2009, at 16-17 (statement of David Kris).

[241] Hearing of July 28, 2009, at 17 (statement of David Kris); Hearing of July 28, 2009, at 132 (written statement of David Laufman); Hearing of July 28, 2009, at 90 (David Laufman's response to written questions).

[242] Hearing of July 28, 2009, at 3 (statement of Jon Kyl).

[243] Hearing of July 28, 2009, at 133 (written statement of David Laufman).

[244] Hearing of July 28, 2009, at 37 (statement of Michael Edney).

[245] Hearing of July 28, 2009, at 37 (statement of Michael Edney).

disclosure."[246] Edney stated that CIPA "does not change the standard for disclosure and has been construed to require that the defendant be provided access to classified information that is relevant and helpful to the defense."[247] In addition, said Edney, unlike the Military Commissions Act (MCA), CIPA contains no mechanism for a trial judge to make an independent *ex parte* assessment of the reliability of intelligence sources and methods underlying otherwise admissible evidence.[248] Edney stressed that it is important to avoid forcing the government into the difficult choice between revealing classified information and holding people accountable for violations of law or war.[249]

CHOICE OF FORUM: CASE-BY-CASE ASSESSMENT RISKS LOSS OF CREDIBILITY

Laufman, Edney, and Pearlstein all raised concerns that the *ad hoc* system for determining whether defendants would be tried in Article III courts or military commissions could lead to a perception that military commissions are an inferior choice resorted to only when a conviction is not attainable in Article III courts.[250] In addition, Senator Feingold expressed his concern about any suggestion that military courts would be better because it is easier to get a conviction.[251]

Edney and Laufman both agreed that by beginning with a presumption in favor of Article III prosecutions, the case-by-case assessment will turn on whether the government can meet its burden and sustain a conviction under civilian principles of prosecution.[252] Edney added that it cheapens the federal criminal justice system when protections are cast aside on a case-by-case basis, and he suggested that the case-by-case approach may be a threat to the integrity of both systems.[253] According to Edney, the case-by-case approach sends the message that military commissions are a type of secondary justice and

---

[246] Hearing of July 28, 2009, at at 71 (Michael Edney's response to written questions).

[247] Hearing of July 28, 2009, at 107 (written statement of Michael Edney).

[248] Hearing of July 28, 2009, at 107 (written statement of Michael Edney).

[249] Hearing of July 28, 2009, at 37 (statement of Michael Edney).

[250] Hearing of July 28, 2009, at 47 (statement of David Laufman); Hearing of July 28, 2009, at 38 (statement of Michael Edney); Hearing of July 28, 2009, at 36 (statement of Deborah Pearlstein).

[251] Hearing of July 28, 2009, at 13-14 (statement of Russ Feingold).

[252] Hearing of July 28, 2009, at 47 (statement of David Laufman); Hearing of July 28, 2009, at 37-38 (statement of Michael Edney).

[253] Hearing of July 28, 2009, at 38, 47 (statement of Michael Edney).

could be viewed that way by judges when the decisions are reviewed in appellate court.[254]

Edney recommended that the government designate a class of cases for one system or the other to enhance the legitimacy of both systems.[255] For example, he suggested that the Administration could designate that all members of Al Qaeda who are aliens, have violated the laws of war, and have been captured outside the United States be tried in military commissions.[256] "Differential treatment for U.S. citizens or alien members of an enemy force captured on U.S. soil could be justified by the distinct constitutional rules applicable to those groups."[257] The least preferable option, according to Edney, is to sort on the strength of the evidence.[258]

POTENTIAL ISSUES IF DETAINEES ARE BROUGHT INTO THE UNITED STATES

Concerns were raised about the authority to bring detainees into the United States, the scope of constitutional rights that detainees would have once in the United States, and the possible risk of detainees being released into the United States before or after adjudication. Senator Kyl emphasized that "any plan to bring detainees into the United States would likely require congressional action."[259] He then asked whether the 2001 Authorization for the Use of Military Force[260] provides congressional authority for transferring individuals to the United States for trial and detention or whether that would require further congressional authorization.[261] Johnson responded that the Authorization for the Use of Military Force provides the adequate legal authority for the detention of the current population of Guantanamo irrespective of where they are held, including the United States, without further authorization from Congress.[262] Edney disagreed with Johnson, arguing that only "an aggressive interpretation of current statutory

---

[254] Hearing of July 28, 2009, at 38 (statement of Michael Edney).

[255] Hearing of July 28, 2009, at 38 (statement of Michael Edney); Hearing of July 28, 2009, at 14 (written statement of Michael Edney).

[256] Hearing of July 28, 2009, at 38 (statement of Michael Edney); Hearing of July 28, 2009, at 69 (Michael Edney's response to written questions).

[257] Hearing of July 28, 2009, at 111 (written statement of Michael Edney).

[258] Hearing of July 28, 2009, at 38 (statement of Michael Edney).

[259] Hearing of July 28, 2009, at 4 (statement of Jon Kyl).

[260] Authorization for Use of Military Force, S.J. Res. 23, 107th Cong. (2001).

[261] Hearing of July 28, 2009, at 12 (statement of Jon Kyl).

[262] Hearing of July 28, 2009, at 12 (statement of Jeh Johnson).

immigration law in favor of the Executive Branch would authorize the contemplated transfer of Guantanamo detainees to the United States."[263]

Edney raised concerns about bringing suspected terrorists from Guantanamo into the United States for prosecution. He suggested that senators needed to consider the legal consequences of where military commission trials would be held and the scope of the constitutional rights that would apply if the trials were held in the United States.[264] Edney contended that the discretion of the political branches in crafting rules for military commissions would be narrowed if the trials were held in the territorial United States.[265] He argued that special rules for hearsay might not withstand constitutional challenge: the Supreme Court decision in *Crawford*,[266] which confirmed the constitutional right to confront witnesses, suggests that a hearsay standard that "depends on reliability assessments by a trial judge would be invalid."[267]

Edney further addressed the potential problems involving detainees who become eligible for release after trial or after serving their sentence. According to Edney, Congress could lose its exclusive discretion as to whether Guantanamo detainees are released inside the United States.[268] Senator Cardin disagreed with Edney's assertion and affirmed that under the immigration laws detainees can be required to leave the country.[269] Edney responded that, once detainees are in the United States, under the torture statute,[270] the United States has a legal obligation not to return an individual to a place where he will be mistreated.[271] Laufman stated that in *Zadvydas*,[272] "the Supreme Court construed the law to limit the period of detention to the time reasonably necessary to secure the alien's removal — with six months

---

[263] Hearing of July 28, 2009, at 51-52 (Michael Edney's response to written questions).

[264] Hearing of July 28, 2009, at 38 (statement of Michael Edney).

[265] Hearing of July 28, 2009, at 115 (written statement of Michael Edney).

[266] Crawford v. Washington, 541 U.S. 36 (2004) (holding that where testimonial statements are at issue, the only *indicium* of reliability sufficient to satisfy constitutional demands is confrontation).

[267] Hearing of July 28, 2009, at 38 (statement of Michael Edney).

[268] Hearing of July 28, 2009, at 38 (statement of Michael Edney).

[269] Hearing of July 28, 2009, at 39 (statement of Benjamin Cardin).

[270] 8 C.F.R. § 208.18 (2010).

[271] Hearing of July 28, 2009, at 39-40 (statement of Michael Edney).

[272] Zadvydas v. Davis, 533 U.S. 678 (2001) (holding that the post-removal-period detention statute, read in light of the Constitution's demands, implicitly limits an alien's detention to a period reasonably necessary to bring about that alien's removal from the United States, and does not permit indefinite detention).

presumed to be a reasonable limit."[273] Once an alien enters the United States, the Due Process Clause applies and the risk of a constitutional claim for release in the United States exists.[274]

DETAINEES NOT ELIGIBLE FOR TRIAL OR RELEASE

Mr. Johnson stated that, at the end of the review process for the Guantanamo detainees, there may be a category of people who, for reasons of national security, must remain detained.[275] Kris added that the decision to put someone in that category would likely be a Cabinet-level or Presidential decision.[276] Mr. Johnson stated the Administration is in the process of developing a system of periodic review for dealing with that segment of the Guantanamo population.[277]

Senator Leahy expressed concern that the Administration has not yet offered details about how a system of prolonged detention would operate, adding that he wants to ensure the system provides constitutional protections and that the judicial review contemplated meets standards of fair treatment under law.[278]

CONCLUSION

This hearing looked at the Administration's protocol for trying Guantanamo detainees. The protocol expressed a preference for trying detainees in Article III courts, but retained the possibility of using military commissions where necessary. Senators raised concerns about *Miranda* rights; evidentiary issues; the risk of release of suspected terrorists into the United States, either before or after adjudication; and the procedures for safeguarding classified information and intelligence sources. The witnesses disagreed on these issues, and questions remained unanswered about the United States' ability to prevent released detainees from remaining in the United States, the application of a voluntariness standard in military commission trials, the ability of CIPA to safeguard intelligence, and the application of *Miranda* rights. There did, however, appear to be general agreement among the senators and witnesses that a two-tier system, where the decision of forum depends on the quality of the evidence, risks delegitimizing both Article III trials and military commissions.

---

[273] Hearing of July 28, 2009, at 140 (written statement of David Laufman).

[274] Hearing of July 28, 2009, at 57 (Michael Edney's response to written questions).

[275] Hearing of July 28, 2009, at 20 (statement of Jeh Johnson).

[276] Hearing of July 28, 2009, at 27 (statement of David Kris).

[277] Hearing of July 28, 2009, at 20 (statement of Jeh Johnson).

[278] Hearing of July 28, 2009, at 145 (written statement of Patrick Leahy).

STRENGTHENING SECURITY AND OVERSIGHT AT BIOLOGICAL RESEARCH LABORATORIES

INTRODUCTION

On September 22, 2009, the Subcommittee held a hearing entitled "Strengthening Security and Oversight at Biological Research Laboratories" to examine (1) current security measures at U.S. laboratories; (2) best practices in both the government and private sector; (3) various government agencies that have oversight responsibilities for security programs; and (4) recommendations on how to strengthen and improve lab security while maintaining innovative research and collaborative efforts with international allies.[279]

Two panels provided testimony. The first panel examined the Executive branch's efforts to strengthen bio-security and consisted of (1) Daniel Roberts, Criminal Justice Information Services (CJIS), Federal Bureau of Investigation (FBI); (2) Jean Reed, Deputy Assistant to the Secretary of Defense, Chemical and Biological Defense / Chemical Demilitarization, Department of Defense (DOD); and (3) Brandt Pasco, Compliance Assurance Program Manager, Department of Homeland Security (DHS). The second panel included outside experts and consisted of (1) the Honorable Robert Graham, former U.S. Senator from Florida, Chairman, Commission for the Prevention of Weapons of Mass Destruction Proliferation and Terrorism; (2) Dr. Nancy Kingsbury, Managing Director, Applied Research and Methods, Government Accountability Office (GAO); and (3) Michael Greenberger, Director, Center for Health and Homeland Security, University of Maryland.

CURRENT BIOLOGICAL RESEARCH LABORATORY SECURITY MEASURES

Security measures relating to U.S. laboratories include personnel screening, adherence to safety guidelines and various compliance programs, and, in some cases, on-sight inspections. However, the lack of a central governmental authority to oversee security implementation has resulted in disparate and inefficient security measures between laboratories. As Senator Cardin noted, "[t]here are about 15 Federal agencies that deal with labs and no one

[279] *Strengthening Security and Oversight at Biological Research Laboratories: Hearing Before the Subcomm. on Terrorism and Homeland Security of the Senate Comm. on the Judiciary*, 111th Cong., 1st Sess. (Sept. 22, 2009) at 1, 2 (statement of Benjamin Cardin) [hereinafter "Hearing of Sept. 22, 2009"].

agency has primary or full responsibility . . . ."[280] As a result, each government agency has its own safety protocols in place to secure biological research laboratories, resulting in excessive measures in some contexts and the need for more stringent measures in others.

In explaining the role of DOJ, Mr. Roberts, Criminal Justice Information Services, Federal Bureau of Investigation, testified that CJIS maintains oversight of the Bioterrorism Risk Assessment Group (BRAG) whose role is to "enhance national security and public safety by providing the timely and accurate determination of an individual's eligibility to use, possess, or transfer select agents and toxins."[281] BRAG uses Security Risk Assessments (SRAs) to evaluate access to select agents and toxins "against criteria delineated within the Public Health, Security, and Bio-Terrorism Preparedness and Response Act of 2002, and against prohibitive categories defining a restricted person within the USA Patriot Act."[282] SRAs are conducted "not less frequently than once every 5 years on individuals requiring access to select agents and toxins."[283]

BRAG collaborates with the Department of Health and Human Services (HHS) and the United States Department of Agriculture (USDA) to conduct SRAs on "public accredited academic institutions" and "any individual who owns or controls the entity . . . every 3 years."[284] SRAs take about one month to complete[285] and include fingerprint processing and searches of BRAG's "stand-alone bioterrorism data base maintained by CJIS."[286] BRAG has completed 32,742 SRAs since April 2003, and 208 individuals have been given restricted access to agents and toxins.[287] Senator Cardin pointed out, however, that in some circumstances more extensive searches would be necessary. For example, if a person is hospitalized for a mental condition, that information would likely not be revealed from a database check, but would be highly relevant to an individual's security assessment.[288] Although Mr. Greenberger, Director, Center for Health and Homeland Security, University of Maryland, did not support the

---

[280] Hearing of Sept. 22, 2009, at 9 (statement of Benjamin Cardin).

[281] Hearing of Sept. 22, 2009, at 3 (statement of Daniel Roberts).

[282] Hearing of Sept. 22, 2009, at 3 (statement of Daniel Roberts).

[283] Hearing of Sept. 22, 2009, at 3 (statement of Daniel Roberts).

[284] Hearing of Sept. 22, 2009, at 3 (statement of Daniel Roberts).

[285] Hearing of Sept. 22, 2009, at 3 (statement of Daniel Roberts).

[286] Hearing of Sept. 22, 2009, at 4 (statement of Daniel Roberts).

[287] Hearing of Sept. 22, 2009, at 4 (statement of Daniel Roberts).

[288] Hearing of Sept. 22, 2009, at 12 (statement of Benjamin Cardin).

use of psychological profiling, he acknowledged that it may be appropriate for a single regulator to report individuals experiencing psychological difficulties.[289] Senator Cardin suggested that Congress has the responsibility to scrutinize those seeking access to highly dangerous biological agents at a much higher level, "including their psychological make-up . . . ."[290]

Jean Reed, Deputy Assistant to the Secretary of Defense, Chemical and Biological Defense, testified that "[t]he term 'select agent' refers to a specific group of chemical or biological agents that historically have been evaluated and developed for use in weapons."[291] The current DOD framework for safeguarding select agents is based on DOD regulations for chemical and nuclear programs and consists of bio-safety, bio-security, personal reliability, and agent accountability.[292] Though current DOD measures exceed the prescribed select agent rules set forth by Congress, some studies have suggested that certain elements of the DOD framework "may be too extreme and could not be implemented by other agencies or the civilian sector without severe impact."[293] For example, the use of single-scope background investigations precludes foreign nationals or personnel with financial difficulties or prior non-criminal legal actions from working with select agents.[294] Mr. Reed testified that "[s]everal recent studies highlight the lack of data to demonstrate that . . . detailed background investigations provide substantial value" over SRAs.[295]

DHS ensures that research conducted on its behalf is compliant with existing regulatory standards.[296] DHS's regulatory compliance program is driven primarily by DHS's treaty compliance efforts.[297] The Compliance Review Group, chaired by the deputy secretary, ensures that all biological research conducted by DHS is compliant with U.S. law and international obligations.[298] DHS's select agent research is subject to regulatory control by the Center for Disease Control (CDC)

---

[289] Hearing of Sept. 22, 2009, at 29-30 (statement of Michael Greenberger).

[290] Hearing of Sept. 22, 2009, at 29 (statement of Benjamin Cardin).

[291] Hearing of Sept. 22, 2009, at 6 (statement of Jean Reed).

[292] Hearing of Sept. 22, 2009, at 6 (statement of Jean Reed).

[293] Hearing of Sept. 22, 2009, at 6 (statement of Jean Reed).

[294] Hearing of Sept. 22, 2009, at 6 (statement of Jean Reed).

[295] Hearing of Sept. 22, 2009, at 7 (statement of Jean Reed).

[296] Hearing of Sept. 22, 2009, at 10 (statement of Brandt Pasco).

[297] Hearing of Sept. 22, 2009, at 9 (statement of Brandt Pasco).

[298] Hearing of Sept. 22, 2009, at 8 (statement of Brandt Pasco).

and the USDA's Animal and Plant Health Inspection Service (APHIS).[299]

Projects funded by DHS fall within one of three categories: (1) those that do not raise compliance concerns; (2) those that raise compliance concerns but do not involve the National Science Advisory Board; and (3) those that raise compliance concerns and likely involve research of concern.[300] Though labs conducting Category 2 or 3 projects, mentioned above, are subject to on-site inspections,[301] when funds are allocated to projects that involve collaboration with partners outside of the United States, DHS usually performs document based review rather than on-site inspections.[302]

SECURITY PROGRAM OVERSIGHT

The lack of a central agency with the authority to oversee and promulgate security measures remains a critical concern at the nation's biological research laboratories. None of the agencies that have an interest in the question of oversight believe that they have "the authority to take a leadership role."[303] As a result, agencies make efforts to coordinate and maintain an interagency approach and varying standards result.[304] Dr. Kingsbury, Managing Director, Applied Research and Methods, Government Accountability Office, noted that "some aspects of the current oversight programs provided by the CDC and the USDA are dependent upon entities monitoring themselves and reporting incidents to federal regulators."[305] CDC, HHS, and APHIS have the responsibility for inspecting all facilities for compliance with select agent programs.[306]

RECOMMENDATIONS TO IMPROVE SECURITY

Improvements in biological research laboratory security are critical to national security and public health. Experts concur that a strong need exists for a single regulatory body to coordinate and

---

[299] Hearing of Sept. 22, 2009, at 8 (statement of Brandt Pasco).

[300] Hearing of Sept. 22, 2009, at 8 (statement of Brandt Pasco).

[301] Hearing of Sept. 22, 2009, at 9 (statement of Brandt Pasco).

[302] Hearing of Sept. 22, 2009, at 15 (statement of Brandt Pasco).

[303] Hearing of Sept. 22, 2009, at 28 (statement of Nancy Kingsbury).

[304] Hearing of Sept. 22, 2009, at 28 (statement of Nancy Kingsbury).

[305] Hearing of Sept. 22, 2009, at 22 (statement of Nancy Kingsbury).

[306] Hearing of Sept. 22, 2009, at 10 (statement of Jean Reed).

oversee bio-safety measures and to instruct agencies on best practices in order to balance security with open and collaborative research.

Mr. Reed suggested that the National Security Council use its interagency policy committee process in conjunction with input from industry and academia to review the recommendations and policy options from collective reports and develop a national approach that optimizes the balance between science and security.[307] He further suggested that the prudent approach would be to apply information gathered from the last two years to develop a series of policies and practices that balance safety and security with the pursuit of a robust biological research and development program.[308]

Senator Graham advised that Congress take three steps: (1) demand that the Executive establish a comprehensive biological weapons strategy; (2) promote global preparation at the 2011 Biological Weapons Convention; and (3) act swiftly due to the greater than 50 percent chance that a weapon of mass destruction will be used by the end of 2013.[309] The Commission for the Prevention of Weapons of Mass Destruction Proliferation and Terrorism advocated implementing an interagency approach with HHS as the lead agency.[310]

Dr. Kingsbury recommended that HHS be the lead agency[311] in developing national standards for high-containment lab operations.[312] He emphasized that, since biological agent inventories cannot be completely controlled, HHS and USDA should review existing inventory control systems and technologies to minimize the potential for misuse.[313] Dr. Kingsbury expressed reservations about the tiered approach and suggested that more information would be necessary to properly assess such an approach,[314] as the more stringent background checks might be prohibitively expensive.[315]

---

[307] Hearing of Sept. 22, 2009, at 7 (statement of Jean Reed).

[308] Hearing of Sept. 22, 2009, at 7 (statement of Jean Reed).

[309] Hearing of Sept. 22, 2009, at 18-20 (statement of Robert Graham) ("The [Commission] assessed that, as of December 2008, it was better than a 50/50 chance that there would be a weapon of mass destruction used between that date and the end of 2013.").

[310] Hearing of Sept. 22, 2009, at 28 (statement of Robert Graham).

[311] Hearing of Sept. 22, 2009, at 29 (statement of Nancy Kingsbury).

[312] Hearing of Sept. 22, 2009, at 28 (statement of Nancy Kingsbury).

[313] Hearing of Sept. 22, 2009, at 22 (statement of Nancy Kingsbury).

[314] Hearing of Sept. 22, 2009, at 26 (statement of Nancy Kingsbury).

[315] Hearing of Sept. 22, 2009, at 30-31 (statement of Nancy Kingsbury).

Echoing the comments of other panelists, Mr. Greenberger advised that a single regulator using guidelines from the CDC and National Institutes of Health should be set up to address security concerns and execute policy.[316] Greenberger recommended designating HHS as the lead agency,[317] with the CDC specifically taking responsibility for setting up safety and security standards, maintaining inventory, reporting, and setting up an accreditation process.[318]

CONCLUSION

The lack of a single regulator responsible for oversight of the nation's biological research laboratories raises concerns about the location of labs, inventory levels, and security implementation.[319] Without a single regulator, agencies have been left to regulate their own activities, and many believe that they lack the authority to take a leadership role.[320] Recognizing this problem, several commissions and agencies have undertaken an assessment to determine best practices.[321]

Outside experts agree that HHS should be the lead regulator for biological research laboratory security because it is in the best position to coordinate and oversee bio-safety measures. Establishing a single regulator would also allow agencies to better coordinate safety measures and would lower costs through improved efficiency.[322] Ultimately, any regulating body must aim to strengthen and improve lab security while maintaining innovative research and collaborative efforts with international allies.[323]

---

[316] Hearing of Sept. 22, 2009, at 28 (statement of Michael Greenberger).

[317] Hearing of Sept. 22, 2009, at 27 (statement of Michael Greenberger).

[318] Hearing of Sept. 22, 2009, at 27-28 (statement of Michael Greenberger).

[319] Hearing of Sept. 22, 2009, at 9-10 (statement of Benjamin Cardin).

[320] Hearing of Sept. 22, 2009, at 28 (statement of Nancy Kingsbury).

[321] Hearing of Sept. 22, 2009, at 7 (statement of Jean Reed).

[322] Hearing of Sept. 22, 2009, at 31 (statement of Benjamin Cardin).

[323] Hearing of Sept. 22, 2009, at 2 (statement of Benjamin Cardin).

CYBERSECURITY: PREVENTING TERRORIST ATTACKS AND PROTECTING PRIVACY IN CYBERSPACE

INTRODUCTION

Shortly after taking office, President Obama ordered a "review to assess U.S. policies and structures for cybersecurity."[324] In May 2009, the review concluded that "the federal government is not organized to address the growing problems of cybersecurity," government agencies have overlapping responsibilities, and "the status quo is no longer acceptable."[325] The study also "pointed out the need to appoint a cyber-security policy officer responsible for coordination of the national cyber-security policies and activities" and the "need to designate a privacy and civil liberties official to the National Security Cyber Security Directorate."[326]

On November 17, 2009, the Subcommittee held a hearing to examine both governmental and private sector efforts to prevent cyber-attacks, the proper role of government in promoting cybersecurity, and "the proper balance between improving cybersecurity and protecting the privacy rights and civil liberties of Americans."[327] Two panels provided testimony. Panel one consisted of (1) James Baker, Associate Deputy Attorney General, Department of Justice; (2) Philip Reitinger, Deputy Under Secretary, National Protection and Programs Directorate, Department of Homeland Security; (3) Richard Schaeffer, Information Assurance Director, National Security Agency; and (4) Steven Chabinsky, Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation. Panel two consisted of (1) Gregory Nojeim, Senior Counsel and Director, Project on Freedom, Security & Technology, Center for Democracy & Technology; (2) Larry Clinton, President and Chief Executive Officer, Internet Security Alliance; and (3) Larry Wortzel, Vice Chairman, United States-China Economic and Security Review Commission.

---

[324] Cyberspace Policy Review, at iii, *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[325] *Cybersecurity: Preventing Terrorist Attacks And Protecting Privacy In Cyberspace: Hearing Before the Subcomm. on Terrorism and Homeland Security of the Senate Comm. on the Judiciary*, 111th Cong., 1st Sess. (Nov. 17, 2009) at 3 (written statement of Benjamin Cardin) [hereinafter "Hearing of Nov. 17, 2009"].

[326] Hearing of Nov. 17, 2009, at 3 (statement of Benjamin Cardin).

[327] Hearing of Nov. 17, 2009, at 2 (written statement of Benjamin Cardin).

GROWING THREATS TO U.S. CYBERSECURITY

At the hearing, both Senators Cardin and Kyl noted that as cyberspace has played an increasingly significant role in our daily activities, the lack of effective standards and controls in cyberspace pose significant and growing dangers to the nation's cybersecurity.[328] Senator Cardin explained that cybersecurity intrusions allow criminals, hackers, and terrorists to gain access to confidential and classified information through weaknesses in the internet in order to "manipulate, corrupt, or alter data that is being used to run critical information systems inside the government or private businesses."[329] Senator Kyl gave an example of the magnitude of the cybersecurity threat: "[T]he U.S. faced a so-called electronic Pearl Harbor in 2007 when an unknown foreign power broke into the computer systems at the Departments of Defense, State, Commerce, and Energy, and probably NASA, and downloaded the equivalent of a Library of Congress worth of information."[330] Senator Kyl also expressed concern that, according to a report by the United States-China Economic and Security Review Commission, China has become a significant cyber-threat.[331]

GOVERNMENT AND PRIVATE SECTOR EFFORTS TO PREVENT A TERRORIST CYBER-ATTACK

The Department of Justice (DOJ) works with various federal agencies, including the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and the Department of Defense (DOD) "to support cybersecurity efforts and inform policy discussions . . . ."[332] DOJ investigates cybersecurity threats, prosecutes

---

[328] Hearing of Nov. 17, 2009, at 1 (written statement of Benjamin Cardin); Hearing of Nov. 17, 2009, at 6-8 (statement of Jon Kyl).

[329] Hearing of Nov. 17, 2009, at 1 (written statement of Benjamin Cardin).

[330] Hearing of Nov. 17, 2009, at 7 (statement of Jon Kyl quoting *60 Minutes: Cyber War: Sabotaging the System* (CBS television broadcast Nov. 8, 2009) *available at* http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml?tag=contentMain;contentBody).

[331] Hearing of Nov. 17, 2009, at 6-7 (statement of Jon Kyl) (stating that "Increasingly, Chinese military strategists have come to view information dominance as the precursor for overall success in a conflict. China is likely using its maturing computer network exploitation capability to support intelligence collection against the U.S. Government. . . . In a conflict with the U.S., China will likely use its computer network operations capabilities to attack unclassified DOD and civilian contractor logistics networks in the continental United States and allied countries in the Asia-Pacific Region. The stated goal in targeting these systems is to delay U.S. deployments and impact combat effectiveness of troops already in theater.").

[332] Hearing of Nov. 17, 2009, at 2 (written statement of James Baker).

cyber-criminals in federal court, conducts training for investigators and prosecutors on cyber threats, and engages in information sharing and coordination across federal agencies through its efforts in the National Cyber Investigative Joint Task Force.[333] In addition, DOJ engages with "foreign law enforcement partners to deny safe havens to cyber criminals and to bring them to justice . . . ."[334]

DHS collaborates with the private sector to ensure the resilience of the nation's critical infrastructures[335] and is developing an "international framework" to build relationships with allies in order to secure cyberspace internationally.[336] DHS has reorganized the government's cybersecurity and communications watch centers in response to advice from both Congress and the private sector in order to improve cross-government coordination and response-efficiency to significant cybersecurity intrusions.[337] DHS is also responsible for creating the National Cybersecurity Protection System, known as EINSTEIN.[338]

The National Security Agency (NSA) protects government systems that "process, store, and transmit classified information or [are] otherwise critical to military or intelligence activities"[339] by "compil[ing] and publish[ing] security checklists for hardening computers and networks against a variety of threats."[340] NSA also participates in joint efforts with the private sector to protect the nation's cybersecurity.[341]

On the enforcement side, the FBI is composed of "the largest cadre of cyber trained law enforcement officers in the United States"

---

[333] Hearing of Nov. 17, 2009, at 10-11 (statement of James Baker); Hearing of Nov. 17, 2009, at 2-3 (written statement of James Baker).

[334] Hearing of Nov. 17, 2009, at 11 (statement of James Baker).

[335] Hearing of Nov. 17, 2009, at 1 (written statement of Philip Reitinger).

[336] Hearing of Nov. 17, 2009, at 56 (statement of Philip Reitinger).

[337] Hearing of Nov. 17, 2009, at 16-17 (statement of Philip Reitinger).

[338] Hearing of Nov. 17, 2009, at 4 (written statement of Philip Reitinger) (explaining that EINSTEIN 1 is a network flow monitoring system; EINSTEIN 2 is an intrusion detection system; EINSTEIN 3 will be "an intrusion prevention system for federal executive branch civilian networks and systems" and will provide "improved early warning and an enhanced situational awareness; the ability to automatically detect malicious activity; and the capability to prevent malicious intrusions before harm is done.").

[339] Hearing of Nov. 17, 2009, at 21 (statement of Richard Schaeffer).

[340] Hearing of Nov. 17, 2009, at 22 (statement of Richard Schaeffer).

[341] Hearing of Nov. 17, 2009, at 22-23 (statement of Richard Schaeffer).

and is "uniquely positioned to combine counterterrorism, counterintelligence, and criminal domestic investigative authorities to address the cyber threat."[342] The FBI's "highest criminal priority" is to protect the nation against "cyber-based attacks and high-technology crimes."[343] To that end, the FBI is investigating individuals "who are affiliated with or sympathetic to Al Qaeda, who have recognized and discussed the vulnerabilities of the United States infrastructure to cyber attack, who have demonstrated an interest in elevating their computer hacking skills, and who are seeking more sophisticated capabilities from outside of their close-knit circles."[344]

SETTING CYBERSECURITY STANDARDS ACROSS GOVERNMENT AND INDUSTRY

Because most of the nation's cyber infrastructure is found within the private domain and because government networks are either "heavily dependent on commercial products and infrastructure or interconnect with systems that are,"[345] it is critical that the government proceed in setting standards cooperatively with the private sector.[346] The panelists agreed that the effort to protect cybersecurity requires participation across government and the private sector as well as increasing awareness of cybersecurity issues, developing new standards, improving cyber-education, expanding information sharing, establishing uniform practices, and improving technology.[347]

Mr. Schaeffer, Information Assurance Director, National Security Agency, stressed that fortifying systems with "good configuration management," "good patch management," and "good access control" greatly increases the "overall assurance of the operating environment"[348] because, under these conditions, intruders must resort to much more sophisticated means and consequently increase their risk of detection.[349] Adopting these quality assurance practices "enable[s] information about computer vulnerabilities to be more easily catalogued and exchanged and ultimately the vulnerabilities themselves

---

[342] Hearing of Nov. 17, 2009, at 3 (written statement of Steven Chabinsky).

[343] Hearing of Nov. 17, 2009, at 3 (written statement of Steven Chabinsky).

[344] Hearing of Nov. 17, 2009, at 26 (statement of Steven Chabinsky).

[345] Hearing of Nov. 17, 2009, at 21 (statement of Richard Schaeffer).

[346] Hearing of Nov. 17, 2009, at 16 (statement of Philip Reitinger).

[347] Hearing of Nov. 17, 2009, at 20 (statement of Richard Schaeffer); Hearing of Nov. 17, 2009, at 33 (statement of Philip Reitinger).

[348] Hearing of Nov. 17, 2009, at 40 (statement of Richard Schaeffer).

[349] Hearing of Nov. 17, 2009, at 49 (statement of Richard Schaeffer).

to be automatically patched" across national security, government, critical infrastructure and other commercial or private systems.[350]

LEADERSHIP FOR CYBERSECURITY POLICIES AND ACTIVITIES

Despite a recommendation by the President's Cybersecurity Policy Review to appoint "a cybersecurity policy official,"[351] at the time of the hearing the government had yet to establish a leadership authority for cybersecurity matters.[352] Mr. Baker, Associate Deputy Attorney General, Department of Justice, testified that a "director-level person" from NSA currently sets the agenda for cybersecurity meetings with the White House.[353] In addition, the Joint Interagency Cyber Task Force monitors and coordinates activities within the Comprehensive National Cybersecurity Initiatives and reports back to the President quarterly.[354] In the event of a significant incident, the National Cyber Instant Response Plan is working on "a highly actionable set of policies and procedures that will enable all of the different government agencies to work effectively with the private sector" to ensure a unified response by the nation.[355]

Senator Kyl expressed concern about this lack of defined leadership in the area of cybersecurity within the government.[356] Mr. Wortzel, Vice Chairman, United States-China Economic and Security Review Commission, underscored this concern, noting that while a fully coordinated government and industry response to cyber intrusions or espionage is necessary, this effort is stalled without senior leadership in the form of a "permanent cybersecurity coordinator."[357]

---

[350] Hearing of Nov. 17, 2009, at 22 (statement of Richard Schaeffer).

[351] Cyberspace Policy Review, at vi, *available at* http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[352] Hearing of Nov. 17, 2009, at 78 (statement of Larry Wortzel); Macon Phillips, *Introducing the New Cybersecurity Coordinator*, THE WHITE HOUSE BLOG, (Dec. 22, 2009), *available at* http://www.whitehouse.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator.

[353] Hearing of Nov. 17, 2009, at 43 (statement of James Baker).

[354] Hearing of Nov. 17, 2009, at 44 (statement of Steven Chabinsky).

[355] Hearing of Nov. 17, 2009, at 42 (statement of Philip Reitinger).

[356] Hearing of Nov. 17, 2009, at 38 (statement of Jon Kyl).

[357] Hearing of Nov. 17, 2009, at 78 (statement of Larry Wortzel).

SHOULD GOVERNMENT HAVE AUTHORITY TO TAKE OVER PRIVATE SYSTEMS?

Senator Cardin expressed concern that, particularly in the private sector, the technology in use does not alert users that their software has been compromised,[358] and despite progress in alerting end users to signs of a compromised system, "it is too hard for individual users and even small and medium businesses to secure their systems."[359] Mr. Nojeim, Senior Counsel and Director, Project on Freedom, Security & Technology, testified that "pursuit of cybersecurity must not include governmental monitoring of private networks"; that monitoring should be left to the "private sector communications providers."[360] Mr. Nojeim noted that though authorities exist to allow the private sector to disclose information under certain circumstances, "[t]hese provisions do not authorize ongoing or routine disclosure of traffic by the private sector to the government . . . ."[361] Instead, Mr. Nojeim advocated continuing policy that allows "providers to invite in the government to intercept the communications of computer trespassers."[362]

Senator Whitehouse expressed concern that "the relationship between the providers and [government could] be anything but ongoing and routine when cyber attacks are constant and unremitting."[363] Senator Whitehouse added that it is impractical for the government to rely on an invitation from the private sector because a government agency probably "has technical capabilities beyond those of providers," making providers less likely to know that a sophisticated attack is under way.[364]

BALANCING CYBERSECURITY PROTECTIONS WITH PRIVACY RIGHTS AND CIVIL LIBERTIES

Senators Cardin and Kyl agreed that steps toward improving cybersecurity must address both the cyber threats of today and protection of privacy and civil liberties.[365] To that end, DOJ is actively

---

[358] Hearing of Nov. 17, 2009, at 32 (statement of Benjamin Cardin).

[359] Hearing of Nov. 17, 2009, at 33-34 (statement of Philip Reitinger).

[360] Hearing of Nov. 17, 2009, at 66 (statement of Gregory Nojeim).

[361] Hearing of Nov. 17, 2009, at 66 (statement of Gregory Nojeim).

[362] Hearing of Nov. 17, 2009, at 66 (statement of Gregory Nojeim).

[363] Hearing of Nov. 17, 2009, at 85 (statement of Sheldon Whitehouse).

[364] Hearing of Nov. 17, 2009, at 85 (statement of Sheldon Whitehouse).

[365] Hearing of Nov. 17, 2009, at 1-4 (statement of Benjamin Cardin); Hearing of Nov. 17, 2009, at 8 (statement of Jon Kyl).

engaged "in an interagency process" to bring proposals to Congress designed to properly balance cybersecurity, privacy, and civil rights;[366] the President's Cyberspace Policy Review "identified a number of legal issues" that are "under examination, including the various authorities that agencies have";[367] and DHS is working to establish the procedures, "training, oversight mechanisms and transparency" that are necessary to ensure that cybersecurity efforts "are compliant with and actually advance privacy rather than impair it."[368]

Senator Cardin expressed concern about the EINSTEIN program's capacity to obtain private information about innocent Americans.[369] Mr. Baker testified that "an extensive legal analysis of the EINSTEIN II initiative"[370] was completed and two Office of Legal Counsel opinions were made available on the OLC website.[371] Mr. Baker acknowledged however, that "not all of the privacy issues with respect to EINSTEIN II have been resolved."[372] Mr. Reitinger added that oversight mechanisms to ensure the initiative's compliance have been instituted by the Office of Privacy, the Office of Civil Rights and Civil Liberties, Office of Cybersecurity and Communications, and other DHS offices.[373]

CONCLUSION

There is no simple solution to America's cybersecurity threats exists and efforts must continue across both the government and private sector to secure the nation's critical infrastructures.[374] Government agencies and the private sector must work together to promote cybersecurity and develop strategies to effectively deal with

---

[366] Hearing of Nov. 17, 2009, at 53-55 (statement of James Baker).

[367] Hearing of Nov. 17, 2009, at 54-55 (statement of Philip Reitinger).

[368] Hearing of Nov. 17, 2009, at 18 (statement of Philip Reitinger).

[369] Hearing of Nov. 17, 2009, at 57-58 (statement of Benjamin Cardin).

[370] Hearing of Nov. 17, 2009, at 57-58 (statement of James Baker).

[371] *Legal Issues Relating To The Testing, Use, And Deployment Of An Intrusion-Detection System (EINSTEIN 2.0) To Protect Unclassified Computer Networks In The Executive Branch* (January 9, 2009), Op. Off. Legal Counsel, *available at* http://www.justice.gov/olc/2009/e2-issues.pdf; *Legality Of Intrusion-Detection System To Protect Unclassified Computer Networks In The Executive Branch* (August 14, 2009), Op. Off. Legal Counsel, *available at* http://www.justice.gov/olc/2009/legality-of-e2.pdf.

[372] Hearing of Nov. 17, 2009, at 61 (statement of James Baker).

[373] Hearing of Nov. 17, 2009, at 60 (statement of Philip Reitinger).

[374] Hearing of Nov. 17, 2009, at 2 (written statement of Benjamin Cardin); Hearing of Nov. 17, 2009, at 6-9 (statement of Jon Kyl).

cybersecurity threats from foreign nations, cyber-terrorists and other cyber-criminals.[375]

[375] Hearing of Nov. 17, 2009, at 35, 37 (statement of Benjamin Cardin); Hearing of Nov. 17, 2009, at 38 (statement of Jon Kyl).

THE ESPIONAGE STATUTES: A LOOK BACK AND A LOOK FORWARD

INTRODUCTION

On May 12, 2010, the Subcommittee held a hearing on the nation's current espionage laws.[376] The hearing, entitled "The Espionage Statutes: A Look Back and A Look Forward," focused on understanding how the nation's espionage laws work, identifying problems in the laws, and potentially modernizing the laws.[377] Three witnesses testified at the hearing: (1) Stephen Vladeck, a law professor at American University Washington College of Law, who specializes in the role of the federal courts in the war on terrorism; (2) Jeffrey Smith, a partner at Arnold and Porter, former general counsel to the Senate Armed Services Committee, and a member of the CIA Director's External Advisory Board; and (3) Kenneth Wainstein, a partner at O'Melveny and Myers, former Assistant Attorney General for National Security, former United States Attorney for the District of Columbia, and former general counsel and chief of staff to FBI Director Robert Mueller.[378]

POTENTIAL DEFICIENCIES IN THE ESPIONAGE ACT

According to law professor Stephen Vladeck, the Espionage Act[379] is a law plagued by "profound and frustrating ambiguities and internal inconsistencies."[380] Senators Cardin and Kyl agreed that the Espionage Act may need to be modernized.[381] The witnesses in their testimonies identified specific weaknesses in the Espionage Act and suggested various ways to modernize it.

---

[376] *The Espionage Statutes: A Look Back and A Look Forward: Hearing Before the Subcomm. on Terrorism and Homeland Security of the Senate Comm. on the Judiciary*, 111th Cong., 2nd Sess. (May 12, 2010) [hereinafter "Hearing of May 12, 2010"].

[377] Hearing of May 12, 2010, at 3-4 (statement of Benjamin Cardin).

[378] Hearing of May 12, 2010, at 6-8 (statement of Benjamin Cardin).

[379] 18 U.S.C. § 793 (1917) (prohibiting the collection and/or distribution of national defense information with the purpose of or reason to believe that the information will be used to injure the United States and advantage a foreign nation)

[380] Hearing of May 12, 2010, at 9 (statement of Stephen Vladeck).

[381] Hearing of May 12, 2010, at 28 (statement of Benjamin Cardin); Hearing of May 12, 2010, at 36 (statement of Jon Kyl).

Mr. Vladeck, in his testimony, cited a number of issues with the Espionage Act.[382] First, the scope of the Espionage Act is ambiguous.[383] The plain text of the Act does not require a showing of an individual's specific intent to harm the national security of the United States or benefit a foreign power, so the Act could potentially apply to cases "bearing little resemblance to classic espionage."[384] The second problem, in Mr. Vladeck view, was the ambiguity in how the Act applies to whistleblowers because there is no specific reference to the Espionage Act in any of the whistleblower statutes.[385] Third, it is unclear how the Act applies to the press.[386] Fourth, the effect of non-disclosure agreements on the Act is unclear.[387] Finally, the Act does not address any potential defenses to prosecution — for example, the improper classification of information. [388] For these reasons, Mr. Vladeck testified that that the Espionage Act hinders enforcement and "deter[s] perfectly legitimate expression and debate."[389]

Mr. Vladeck recommended a number of ways to modernize the Espionage Act.[390] Because the Act predates the modern classification system, Mr. Vladeck first recommended substituting a prohibition on the disclosure of "classified information" for the current prohibition on more ambiguous types of governmental materials.[391] Next, he recommended amending the espionage statutes to allow an "improper classification" defense.[392] Finally, if Congress sought to limit the reach of the espionage statutes to only classic espionage, Mr. Vladeck recommended requiring proof of specific harmful intent.[393] To do so would "eliminate the possibility that individuals could be subject to liability under the Espionage Act for non-espionage-motivated (albeit still prohibited) disclosures."[394]

---

[382] Hearing of May 12, 2010, at 10 (statement of Stephen Vladeck).

[383] Hearing of May 12, 2010, at 10 (statement of Stephen Vladeck).

[384] Hearing of May 12, 2010, at 10 (statement of Stephen Vladeck).

[385] Hearing of May 12, 2010, at 11 (statement of Stephen Vladeck).

[386] Hearing of May 12, 2010, at 13 (statement of Stephen Vladeck).

[387] Hearing of May 12, 2010, at 31 (statement of Stephen Vladeck).

[388] Hearing of May 12, 2010, at 13 (statement of Stephen Vladeck).

[389] Hearing of May 12, 2010, at 14 (statement of Stephen Vladeck).

[390] Letter from Stephen Vladeck, American University Professor of Law, to Patrick Leahy, U.S. Senator, Chairman of the Senate Committee on the Judiciary (June 3, 2010) [hereinafter "Letter from Stephen Vladeck, June 3, 2010"].

[391] Letter from Stephen Vladeck, June 3, 2010, at 1.

[392] Letter from Stephen Vladeck, June 3, 2010, at 1.

[393] Letter from Stephen Vladeck, June 3, 2010, at 2.

[394] Letter from Stephen Vladeck, June 3, 2010, at 2.

Mr. Smith, former general counsel to the Senate Armed Services Committee and a member of the CIA Director's External Advisory Board, identified additional problems with the Espionage Act.[395] Specifically, Mr. Smith identified problems with some of the terms and definitions used in the Act.[396] First, many of the terms for items of classified information such as "signal books," are out-dated.[397] Mr. Smith recommended replacing this list with "'information in whatever form'" or updating the list to include electronic information.[398] Furthermore, the terms "national defense" and "foreign nation" are too narrow to protect against modern day disclosures.[399] Mr. Smith recommended replacing the term "national defense" with the term "national security" and the term "foreign nation" with the term "foreign power" to more broadly protect the nation's interests.[400]

AUTHORIZED GOVERNMENT DISCLOSURES

Authorized government disclosure of classified information is another area of concern.[401] An authorized government disclosure occurs when a senior government official approves the disclosure of information to the press that is still technically classified.[402] Mr. Smith testified that it is important for senior officials to be able to release information so that the public is informed.[403] But, officials do not always want to release information in a way that specifically ties the Administration to the statement.[404]

Mr. Smith explained that authorized disclosures can be legitimate, but argued that it is troubling when Administration officials try to have it both ways: prosecuting individuals only when leaks do not suit the Administration's needs.[405] Mr. Smith testified that authorized disclosures generally undermine the effectiveness of the nation's

---

[395] Hearing of May 12, 2010, at 17 (statement of Jeffery Smith).

[396] Hearing of May 12, 2010, at 17 (statement of Jeffery Smith).

[397] Hearing of May 12, 2010, at 17-18 (statement of Jeffery Smith).

[398] Hearing of May 12, 2010, at 18 (statement of Jeffery Smith).

[399] Hearing of May 12, 2010, at 18 (statement of Jeffery Smith).

[400] Hearing of May 12, 2010, at 18-19 (statement of Jeffery Smith).

[401] Hearing of May 12, 2010, at 43-44 (statement of Benjamin Cardin).

[402] Hearing of May 12, 2010, at 19 (statement of Jeffery Smith).

[403] Hearing of May 12, 2010, at 44 (statement of Jeffery Smith).

[404] Hearing of May 12, 2010, at 44 (statement of Jeffery Smith).

[405] Hearing of May 12, 2010, at 44 (statement of Jeffery Smith).

espionage laws[406] and suggest that the government is not serious about protecting its secrets.[407] Senator Kyl expressed his concern that authorized leaks undermine "the rule of law and their expectation of deterrence."[408] Mr. Smith went on to point out that the central problem with authorized disclosures is that it is extremely difficult under current espionage laws to draw the line between authorized and unauthorized disclosures.[409]

Senator Kyl suggested adapting in the law a brighter line between authorized and unauthorized disclosures.[410] Mr. Wainstein, former Assistant Attorney General for National Security, expressed his support for clarifying this issue.[411] Senator Cardin and Mr. Smith agreed that without a clear line between authorized and unauthorized disclosures it is difficult to know where criminal culpability lies.[412] Senator Cardin also argued for a transparent process for authorizing leaks because members of Congress and others need to know what they can comment on and discuss openly.[413]

Senator Kyl suggested two potential changes to the law that would more effectively address the problem of authorized leaks.[414] First, Senator Kyl suggested that a new bill could authorize only certain officials to make the decision to leak classified information.[415] That way, someone could be held accountable.[416] Mr. Smith, on the other hand, testified that such an approach would prove unmanageable in practice.[417] Senator Kyl also suggested creating a simple, quick process by which information could be declassified immediately before disclosure, so that officials only discuss unclassified information with the public.[418]

---

[406] Hearing of May 12, 2010, at 29 (statement of Jeffery Smith).

[407] Hearing of May 12, 2010, at 19-20 (statement of Jeffery Smith).

[408] Hearing of May 12, 2010, at 36 (statement of Jon Kyl).

[409] Hearing of May 12, 2010, at 29 (statement of Jeffery Smith).

[410] Hearing of May 12, 2010, at 39 (statement of Jon Kyl).

[411] Hearing of May 12, 2010, at 39 (statement of Kenneth Wainstein).

[412] Hearing of May 12, 2010, at 41-42 (statements of Benjamin Cardin and Jeffery Smith).

[413] Hearing of May 12, 2010, at 44 (statement of Benjamin Cardin).

[414] Hearing of May 12, 2010, at 36 (statement of Jon Kyl).

[415] Hearing of May 12, 2010, at 36 (statement of Jon Kyl).

[416] Hearing of May 12, 2010, at 36 (statement of Jon Kyl).

[417] Hearing of May 12, 2010, at 38 (statement of Jeffery Smith).

[418] Hearing of May 12, 2010, at 36, 38 (statement of Jon Kyl).

UNAUTHORIZED GOVERNMENT DISCLOSURES

Mr. Wainstein, in his testimony, discussed two types of unauthorized disclosures by government officials: the disclosure of sensitive information to a foreign agent for money or a traitorous reason and the disclosure of sensitive information to the media for self-interest or to expose wrongdoing.[419] He explained that the key to stopping both types of unauthorized disclosures is prosecuting those responsible.[420] Several obstacles stand in the way of prosecuting unauthorized disclosure cases, including difficulty in identifying the leaker, limits on the Department of Justice's ability to subpoena and get information to identify the leaker, reluctance of the compromised agency to cooperate, and defendants' use of wide varieties of legal challenges.[421] These difficulties are even greater in media leak cases, which hinders DOJ's ability to prosecute these cases. [422]

To overcome some of these obstacles, Mr. Wainstein suggested that the Subcommittee consider exploring how the espionage laws apply to private contractors employed by the government, amending the Classified Information Procedures Act[423] to better protect classified and sensitive information in criminal trials, and encouraging a general respect for the United States' classified and sensitive information by sending a clear message that the government does not condone unauthorized disclosures of classified information.[424]

WHISTLEBLOWER PROTECTION ACT

During the hearing, Senator Cardin initiated a discussion about the Whistleblower Protection Act.[425] Mr. Wainstein recommended that Congress update the Whistleblower Protection Act[426] to perfect the mechanism and procedures by which whistleblowers can report government wrongdoing.[427] According to Mr. Wainstein, perfecting

---

[419] Hearing of May 12, 2010, at 23 (statement of Kenneth Wainstein).

[420] Hearing of May 12, 2010, at 23-24 (statement of Kenneth Wainstein).

[421] Hearing of May 12, 2010, at 24-25 (statement of Kenneth Wainstein).

[422] Hearing of May 12, 2010, at 24, 25 (statement of Kenneth Wainstein).

[423] 18 U.S.C. App. III. §§ 1-16.

[424] Hearing of May 12, 2010, at 25-26 (statement of Kenneth Wainstein).

[425] Hearing of May 12, 2010, at 44 (statement of Benjamin Cardin).

[426] 5 U.S.C. § 1213 (1989)

[427] Hearing of May 12, 2010, at 46 (statement of Kenneth Wainstein).

the mechanisms and procedures for whistleblowers would discredit justifications for unilateral leaks to the media.[428] Mr. Vladeck added that because the Espionage Act is silent as to its interaction with the Whistleblower Protection Act, Congress should amend the Espionage Act to exclude disclosures protected under the whistleblower statutes.[429]

GOOD MOTIVE LEAKS

A good motive leak occurs when an individual leaks classified information with a motive other than to harm the United States.[430] Senator Kyl found it difficult to justify a good motive as a defense for an unlawful disclosure when under current law the government is already required to establish knowledge of potential harm to the United States.[431] Mr. Vladeck disagreed.[432] He believes that a government employee should be permitted to argue good faith even if he knew his disclosure could cause harm to national defense.[433] Mr. Smith, on the other hand, argued that a good faith defense should not apply to those with authorized access or those that disclose information to a foreign power, but he does support a good faith defense for those who, without authorized access, seek to publish classified information to generate public discussion.[434] Because of this distinction, Mr. Smith argues that we may "need to have a statute with different types of action, different intents, and different punishments, depending on the actor and the intent."[435]

CONCLUSION

The Subcommittee discovered that all witnesses identified weaknesses in the current laws and supported modernizing and clarifying the espionage statutes. The hearing provided the Subcommittee with a heightened sense of awareness in regard to deficiencies within the Espionage Act, and provided the Subcommittee

---

[428] Hearing of May 12, 2010, at 46 (statement of Kenneth Wainstein).

[429] Hearing of May 12, 2010, at 47 (statement of Stephen Vladeck).

[430] Hearing of May 12, 2010, at 48 (statement of Jon Kyl).

[431] Hearing of May 12, 2010, at 56 (statement of Jon Kyl).

[432] Hearing of May 12, 2010, at 56 (statement of Stephen Vladeck).

[433] Hearing of May 12, 2010, at 56 (statement of Stephen Vladeck).

[434] Hearing of May 12, 2010, at 57-58 (statement of Jeffrey Smith).

[435] Hearing of May 12, 2010, at 58 (statement of Jeffrey Smith).

with information necessary to move forward in addressing these deficiencies.

THE PASSPORT ISSUANCE PROCESS: CLOSING THE DOOR TO FRAUD, PART II

INTRODUCTION

On July 29, 2010, the Subcommittee convened its second hearing to investigate the results of the Government Accountability Office's (GAO) most recent undercover investigation of the State Department's passport issuance system.[436] Two witnesses provided testimony at the hearing: Greg Kutz, Managing Director, Forensic Audits and Special Investigation Unit, U.S. Government Accountability Office; and Brenda Sprague, Deputy Assistant Secretary for Passport Services, Bureau of Consular Affairs, U.S. State Department. GAO's 2010 investigation revealed that "significant concerns remain about [the State Department's] ability to prevent passport fraud."[437]

GAO'S 2010 UNDERCOVER TESTS REVEAL SOME PROGRESS, BUT SIGNIFICANT FLAWS REMAIN

After the GAO successfully used counterfeit and/or fraudulent documents to obtain four U.S. passports in 2009,[438] Senators Cardin, Kyl, Feinstein, Lieberman, and Collins requested a follow-up investigation.[439] During the follow-up investigation, GAO investigators applied for seven U.S. passports using counterfeit and/or fraudulently obtained driver's licenses, birth certificates, and Social Security numbers.[440] Five passports were issued.[441] Some of the red flags missed by those processing the applications were a 62-year-old applicant using a Social Security number issued in 2009, applications with counterfeit driver's licenses and birth certificates, a significant age difference between an applicant's passport and driver's license photo, and an applicant who provided documents with various addresses in

---

[436] The Passport Issuance Process: Closing the Door to Fraud, Part II: *Hearing Before the Subcomm. on Terrorism and Homeland Security of the Senate Comm. on the Judiciary*, 111th Cong., 2nd Sess. (July 29, 2010) at 4 [hereinafter "Hearing of July 29, 2010"].

[437] Hearing of July 29, 2010, at 15 (statement of Greg Kutz).

[438] Hearing of July 29, 2010, at 2-3 (statement of Benjamin Cardin).

[439] Hearing of July 29, 2010, at 4 (statement of Benjamin Cardin).

[440] Hearing of July 29, 2010, at 12-13 (statement of Greg Kutz).

[441] Hearing of July 29, 2010, at 13 (statement of Greg Kutz).

different states.[442] Two of the five passports issued were recovered before delivery because facial recognition technology matched photos used in the applications with photos used in previous applications.[443] Concerns about the Social Security numbers of two applicants and subsequently discovered driver's license and birth certificate defects resulted in the denial of two applications.[444]

Senator Cardin expressed disappointment "that there was . . . success in again compromising our [passport issuance] system."[445] Brenda Sprague, Deputy Assistant Secretary for Passport Services within the Bureau of Consular Affairs, the agency within the State Department responsible for the passport issuance system, stressed that her agency was "fully committed to continually improving our system."[446] Ms. Sprague stated that improvements in the passport issuance system implemented after the 2009 investigation enabled the Bureau to detect the most recent GAO tests and respond appropriately.[447] Despite these improvements, Ms. Sprague testified that the Bureau of Consular Affairs "need(s) additional tools and stronger authority" to effectively perform its function.[448] Greg Kutz, Managing Director of GAO's Forensic Audits and Special Investigation Unit, agrees that some progress has been made, but he is still concerned about the Bureau's inability to detect "counterfeit breeder documents."[449] Even though Senator Cardin recognized that there are "dedicated people working very hard to correct these problems," he stressed that "we must do better, much better."[450]

VERIFICATION USING SOCIAL SECURITY NUMBERS: A WORK IN PROGRESS

The Social Security number database is a "tremendous resource" in processing passport applications.[451] Currently, the

---

[442] Hearing of July 29, 2010, at 13 (statement of Greg Kutz).

[443] Hearing of July 29, 2010, at 14, 21 (statement of Greg Kutz).

[444] Hearing of July 29, 2010, at 14 (statement of Greg Kutz).

[445] Hearing of July 29, 2010, at 26 (statement of Senator Cardin).

[446] Hearing of July 29, 2010, at 16 (statement of Brenda Sprague).

[447] Hearing of July 29, 2010, at 18 (statement of Brenda Sprague).

[448] Hearing of July 29. 2010, at 18 (statement of Brenda Sprague).

[449] Hearing of July 29, 2010, at 30 (statement of Greg Kutz).

[450] Hearing of July 29, 2010, at 5 (statement of Benjamin Cardin).

[451] Hearing of July 29, 2010, at 38 (statement of Brenda Sprague).

response time for a Social Security number check is 24 hours.[452] The Bureau of Consular Affairs is working with the Social Security Administration to achieve real-time access to this information.[453] Both Senator Kyl and Mr. Kutz stressed the importance of real-time access, and Senator Kyl saw this as an opportunity for the Bureau of Consular Affairs to improve its system through agency collaboration.[454] Mr. Kutz did report that the State Department is making progress in validating deceased and regular Social Security numbers.[455]

Because of the progress made in verifying Social Security numbers, Ms. Sprague requested, with the support of Mr. Kutz, the authority from Congress to require applicants to provide their Social Security numbers.[456] Senator Hatch expressed concerns with a Social Security number requirement because of the danger of misuse.[457] Ms. Sprague conceded misuse is a concern, but she highlighted a Social Security number's importance in the verification process.[458] A Social Security number can, in a fairly short period of time, provide the Bureau of Consular Affairs with the name, birth date, gender, and death status of the individual associated with the number.[459] Ms. Sprague also reported that the Bureau's current procedures require acceptance facilities to send all applications by traceable mail.[460]

One lingering concern with the verification process is the inaccessibility of data on the issuance date of Social Security numbers.[461] The issuance date for Social Security numbers in the past could be determined by a specific algorithm, but soon the Social Security Administration will abandon that algorithm, so it will be impossible to determine the issuance date of newly issued Social Security numbers.[462]

---

[452] Hearing of July 29, 2010, at 48 (statement of Brenda Sprague).

[453] Hearing of July 29, 2010, at 48 (statement of Brenda Sprague).

[454] Hearing of July 29, 2010, at 9 (statement of Senator Kyl); Hearing of July 29, 2010, at 50 (Statement of Greg Kutz).

[455] Hearing of July 29, 2010, at 50 (statement of Greg Kutz).

[456] Hearing of July 29, 2010, at 19 (statement of Brenda Sprague); Hearing of July 29, 2010, at 31 (statements of Greg Kutz).

[457] Hearing of July 29, 2010, at 38 (statement of Orrin Hatch).

[458] Hearing of July 29, 2010, at 38-39 (statement of Brenda Sprague).

[459] Hearing of July 29, 2010, at 38-39 (statement of Brenda Sprague).

[460] Hearing of July 29, 2010, at 39 (statement of Brenda Sprague).

[461] Hearing of July 29, 2010, at 49 (statement of Brenda Sprague).

[462] Hearing of July 29, 2010, at 49 (statement of Brenda Sprague).

FACIAL RECOGNITION: A PROMISING BUT LIMITED TOOL

When GAO conducted its recent tests, the Bureau had not fully implemented facial recognition technology, but once GAO's investigation was discovered by the Bureau of Consular Affairs, the technology was used by the Bureau to successfully prevent the delivery of two wrongfully issued passports.[463] Currently, the facial recognition technology is available to all fraud managers and all domestic Bureau agencies.[464]

The Bureau will use facial recognition technology in a two-tiered approach.[465] Initially, all incoming passport photographs for domestic applications will be run through the facial recognition system.[466] If later in the application process fraud is suspected, the technology will again be used to run the applicant's photograph against the Bureau's entire database.[467] In using this technology, the Bureau of Consular Affair's can detect a fraudulent application by matching an applicant's photograph with photographs from previous passport applications, previously issued passports, or the Bureau's Visa lookout file.[468]

DRIVER'S LICENSE AND BIRTH CERTIFICATE VERIFICATION

In his testimony, Greg Kutz stressed the importance of validating an applicant's driver's license and birth certificate.[469] Senator Cardin specifically expressed concern about the current state of the driver's license verification process.[470] A driver's license is such a common instrument for identification that, according to Senator Cardin, "there needs to be a capacity . . . to identify fraudulent driver's licenses."[471] Senator Cardin classified this capacity as "a basic security issue."[472]

---

[463] Hearing of July 29, 2010, at 23 (statement of Brenda Sprague).

[464] Hearing of July 29, 2010, at 25-26 (statement of Brenda Sprague).

[465] Hearing of July 29, 2010, at 24 (statement of Brenda Sprague).

[466] Hearing of July 29, 2010, at 25 (statement of Brenda Sprague).

[467] Hearing of July 29, 2010, at 24 (statement of Brenda Sprague).

[468] Hearing of July 29, 2010, at 25 (statement of Brenda Sprague).

[469] Hearing of July 29, 2010, at 30 (statement Greg Kutz).

[470] Hearing of July 29, 2010, at 27 (statement of Benjamin Cardin).

[471] Hearing of July 29, 2010, at 27 (statement of Benjamin Cardin).

[472] Hearing of July 29, 2010, at 27 (statement of Benjamin Cardin).

In GAO's 2010 tests, investigators used counterfeit driver's licenses and birth certificates,[473] none of which were "initially detected."[474] Verifying a driver's license or birth certificate is difficult because it requires ensuring a document is neither counterfeit nor fraudulently obtained. The State Department has difficulty determining whether a document is either.

In detecting counterfeit driver's licenses, the State Department faces two hurdles: it has limited access to data banks, and acceptance agencies are ill-equipped to detect counterfeit driver's licenses. In detecting counterfeit birth certificates, limited access to data banks is also a concern, but the lack of standardization poses greater problems.[475] Senator Kyl expressed concern that the Department of Homeland Security was moving slowly in its digitization of birth certificates.[476] Ms. Sprague indicated that the digitization of birth certificates would assist her agency in detecting counterfeit birth certificates.[477]

Currently, the State Department only has limited access to the nationwide verification system that is used to verify driver's license information.[478] The State Department can verify the information of applicants in 43 states, but only has a small number of accounts, thus access to this tool is limited to the State Department's fraud offices.[479] Ms. Sprague suggested that these limitations stem from the State Department's lack of law enforcement authority,[480] so she encouraged Congress to provide the State Department with that law enforcement authority.[481] Senator Cardin, along with Senators Feinstein and Lieberman, introduced the Passport Identity Verification Act, which would provide the State Department with the authority it needs to access federal, state, and local data banks.[482] Even if the State

---

[473] Hearing of July 29, 2010, at 12 (statement of Greg Kutz).

[474] Hearing of July 29, 2010, at 21 (statement of Greg Kutz) (according to Greg Kutz driver's license defects were not discovered, until after Social Security number defects raised fraud concerns).

[475] Hearing of July 29, 2010, at 19, 30 (statements of Brenda Sprague and Greg Kutz) (according to both Brenda Sprague and Greg Kutz, standardization is a significant concern).

[476] Hearing of July 29, 2010, at 9 (statement of Jon Kyl).

[477] Hearing of July 29, 2010, at 32 (statement of Brenda Sprague).

[478] Hearing of July 29, 2010, at 27 (statement of Brenda Sprague).

[479] Hearing of July 29, 2010, at 27-28 (statement of Brenda Sprague).

[480] Hearing of July 29, 2010, at 37 (statement of Brenda Sprague).

[481] Hearing of July 29, 2010, at 18 (statement of Brenda Sprague).

[482] Hearing of July 29, 2010, at 5-6 (statement of Benjamin Cardin).

Department gains access to this information, however, a significant issue with detecting counterfeit licenses persists: acceptance agencies are the first line of defense for counterfeit detection.

Nine out of every ten passport applications are submitted through acceptance agencies, most of which are post offices,[483] so acceptance agencies are the "the first line of defense" in detecting counterfeit driver's licenses.[484] In fact, because acceptance agencies send only photocopies of driver's licenses to the State Department, Mr. Kutz and Senator Cardin agreed the role of acceptance agencies is essential to the detection counterfeit driver's licenses.[485] Ms. Sprague could not envision giving acceptance agencies access to data banks because of the sensitivity of the information involved, but she did propose an alternative solution.[486] According to Ms. Sprague, there are commercially available machines that have the ability to detect counterfeit driver's licenses.[487] Ms. Sprague did concede that the postal service is currently under "financial strains,"[488] so she did not believe that the postal service is "in a position to invest in this technology."[489]

Improving detection of fraudulently obtained documents is significantly more difficult than improving the detection of counterfeit documents. Specifically, it is almost impossible based on a driver's license alone to determine whether it was fraudulently obtained.[490] Thus, the burden shifts to the states to ensure fraudulent driver's licenses are not issued.[491] Ms. Sprague argued that changes in the policies of some states would not be enough to resolve this issue because such action would only shift activity to states with less stringent restrictions.[492]

---

[483] Hearing of July 29, 2010, at 28 (statement of Brenda Sprague).

[484] Hearing of July 29, 2010, at 42 (statement of Greg Kutz).

[485] Hearing of July 29, 2010, at 42-43 (statements of Benjamin Cardin and Greg Kutz).

[486] Hearing of July 29, 2010, at 43 (statement of Brenda Sprague).

[487] Hearing of July 29, 2010, at 43 (statement of Brenda Sprague).

[488] Hearing of July 29, 2010, at 40 (statement of Brenda Sprague).

[489] Hearing of July 29, 2010, at 28 (statement of Brenda Sprague).

[490] Hearing of July 29, 2010, at 29 (statement Brenda Sprague).

[491] Hearing of July 29, 2010, at 29, 33 (statement of Brenda Sprague).

[492] Hearing of July 29, 2010, at 34 (statement of Brenda Sprague).

CONCLUSION

The Subcommittee hearing resulted in a clearer picture of what is needed to improve the passport issuance system: more information and a comprehensive detection system. Senator Kyl requested a State Department report on the passport issuance system, including what is needed for the system to work effectively, any action required by Congress or the Executive branch, and the State Department's response to the concerns and suggestions of GAO.[493] Ms. Sprague agreed to produce the report.[494]

Senator Cardin concluded that a system with multiple safeguards was the best solution: "it seems to me you have to combine all these issues in the most efficient way and by doing this, the net will be tight enough that you're going to increase dramatically the denial of those fraudulent applications."[495] Specifically, the first safeguard is a two-tiered counterfeit detection system, which involves a driver's license check by acceptance agencies using commercially available technology and a second check by agents of the Bureau of Consular Affairs using information in state data banks.[496] The next safeguard is verification using death records and Social Security numbers.[497] The final safeguard is verification of birth certificates, which requires collaboration between the federal government and local governments in order to find a better way to verify these documents because currently this information is not available in a useful way. [498] Senator Kyl stressed the importance of creating a better system: "If there is another 9/11 and people obtain fraudulent documents as they did in that case like drivers licenses, for example, and people ask why it happened, I think every one of us has to be able to say we did everything we could to prevent it from happening."[499]

---

[493] Hearing of July 29, 2010, at 50-51 (statement of Jon Kyl).

[494] Hearing of July 29, 2010, at 51 (statement of Brenda Sprague).

[495] Hearing of July 29, 2010, at 52-53 (statement of Benjamin Cardin).

[496] Hearing of July 29, 2010, at 43-44 (statement of Brenda Sprague); Hearing of July 29, 2010, at 52 (statement of Benjamin Cardin). Greg Kutz also supported this two-tiered approach: "[i]f you had the machines to authenticate the drivers license and . . . the ability to validate or authenticate with the DMVs, to me those two together would work in this environment." Hearing of July 29, 2010, at 45-46 (statement of Greg Kutz).

[497] Hearing of July 29, 2010, at 52 (statement of Benjamin Cardin).

[498] Hearing of July 29, 2010, at 52 (statement of Benjamin Cardin).

[499] Hearing of July 29, 2010, at 54 (statement of Jon Kyl).

GOVERNMENT PREPAREDNESS AND RESPONSE TO A TERRORIST ATTACK USING WEAPONS OF MASS DESTRUCTION.

INTRODUCTION

The Subcommittee held a hearing on August 4, 2010 to assess government preparedness and response to terrorist attacks using weapons of mass destruction (WMD).[500]

Two panels provided testimony at the hearing. Panel one consisted of (1) Glenn Fine, Inspector General, Department of Justice; (2) James Barker, Associate Deputy Attorney General, Department of Justice; and (3) Steward Beckham, Director, Office of National Capital Regional Coordination, Federal Emergency Management Agency, Department of Homeland Security. Panel two consisted of (1) Colonel Randall J. Larsen, USAF (Retired), Executive Director, Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism; and (2) Michael J. Frankel, Ph.D., Executive Director, Commission to Assess the Threat to the U.S. from Electromagnetic Pulse (EMP) Attack.

THE THREAT OF WEAPONS OF MASS DESTRUCTION GENERALLY: STATE OF PREPAREDNESS

A weapon of mass destruction attack can occur through the use of chemical, biological, radiological, or nuclear weapons.[501] The potential use of a WMD poses a serious threat to the United States.[502] One of our nation's greatest concerns is that a WMD could fall into the hands of terrorists or that terrorists will develop a WMD of their own.[503] As Senator Cardin noted at the hearing, "if there were a successful terrorist attack using [WMDs], it could not only cause a significant number of casualties, but it could very well compromise our infrastructure and ability to respond to the crisis. It would create fear and panic within the community. It is critical to have clear leadership

---

[500] *Government Preparedness and Response to a Terrorist Attack Using Weapons of Mass Destruction: Hearing before the Subcomm. on Terrorism and Homeland Security of the Senate Comm. on the Judiciary*, 111th Cong., 1st Sess. (Aug. 4, 2010) at 1 (statement of Benjamin Cardin) [hereinafter "Hearing of Aug. 4, 2010"].

[501] Hearing of Aug. 4, 2010, at 3 (statement of Benjamin Cardin).

[502] Hearing of Aug. 4, 2010, at 8 (statement of Glenn Fine).

[503] Hearing of Aug. 4, 2010, at 8 (statement of Glenn Fine).

and clear control of the resources that are available for the response."[504] It is of paramount importance that a terrorist attack of any kind against this country be prevented, particularly one involving a WMD.[505]

Senator Kyl expressed concern about the state of our preparedness, noting that it receives too little attention[506] and pointed out that "unfriendly nations have had the ability to inflict great damage with WMDs and that terrorist groups have sought the capacity to do so for some time, yet our government is not sufficiently prepared for such an attack."[507] Senator Cardin echoed this concern, stating, "quite frankly, it is rather disturbing . . . to see that 9 years after the 9/11 attack, we still do not have in place the proper functioning plans in the event of a successful attack using [WMDs] in the United States."[508]

DEPARTMENT OF JUSTICE: STATE OF PREPAREDNESS

DOJ's Office of Inspector General found that while the FBI has taken appropriate steps to prepare to respond to a WMD attack,[509] DOJ as a whole, with a response program that is uncoordinated and fragmented, has not.[510] Under the National Response Framework, ESF-13, DOJ is designated as the lead agency for coordinating the use of federal law enforcement resources to maintain public safety and security if local and state resources are overwhelmed during an incident.[511] ESF-13 staff, when questioned, said, "we are totally unprepared . . . right now, being totally effective would never happen. Everybody would be winging it."[512]

The OIG report made recommendations to help DOJ better prepare to respond to a WMD incident: designating a person or office at the Department level with the authority to manage DOJ's WMD response program, updating WMD response policies and plans, and establishing effective oversight to ensure that DOJ maintains WMD response plans and participates in training exercises.[513] Glenn Fine,

---

[504] Hearing of Aug. 4, 2010, at 22 (statement of Benjamin Cardin).

[505] Hearing of Aug. 4, 2010, at 2 (statement of Benjamin Cardin).

[506] Hearing of Aug. 4, 2010, at 3 (statement of Jon Kyl).

[507] Hearing of Aug. 4, 2010, at 4 (statement of Jon Kyl).

[508] Hearing of Aug. 4, 2010, at 22 (statement of Benjamin Cardin).

[509] Hearing of Aug. 4, 2010, at 8 (statement of Glenn Fine).

[510] Hearing of Aug. 4, 2010, at 9 (statement of Glenn Fine).

[511] Hearing of Aug. 4, 2010, at 9 (statement of Glenn Fine).

[512] Hearing of Aug. 4, 2010, at 9 (statement of Glenn Fine).

[513] Hearing of Aug. 4, 2010, at 11 (statement of Glenn Fine).

Inspector General, Department of Justice, testified that DOJ is taking the report seriously,[514] as can be seen by the creation of DOJ Emergency Preparedness Committee and five subcommittees aimed at addressing emergency response issues.[515] The Associate Deputy Attorney General within DOJ, James Baker, testified that DOJ is in the process of implementing the recommendations of the OIG.[516]

BIOLOGICAL ACTS OF TERRORISM: STATE OF PREPAREDNESS

The WMD Commission Report Card released on January 26, 2010 gave a failing grade to America for preparedness to respond to a bioterrorism attack.[517] Colonel Randall J. Larsen, Executive Director, Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, set forth two primary reasons why America earned a failing grade. First, Larsen stated, "[t]he underlying cause for this failing grade is exactly the same across the board in all departments and agencies — leadership, to be precise, lack of leadership."[518] Larsen pointed out that "[t]here is not a single Presidentially-appointed, Senate-confirmed individual with fulltime responsibility for leading America's biodefense efforts."[519] Larsen suggested that to remedy this issue, "the Vice President should be the top WMD coordinator for the nation."[520]

The second reason, according to Larsen, that America received a failing grade is a lack of understanding of the threat of bioterrorism.[521] Larsen argued that "for the nation to effectively deal with the biological threats facing us, it is imperative that those responsible for shaping the strategy understand the true nature of the threats,"[522] and he suggested that all members of the Subcommittee receive the Population Threat Assessment briefing prepared by Dr. Elizabeth George at DHS's Office of Science and Technology.[523] Larsen urged that "at the least we need to have the Biodefense Policy

---

[514] Hearing of Aug. 4, 2010, at 11 (statement of Glenn Fine).

[515] Hearing of Aug. 4, 2010, at 11 (statement of Glenn Fine).

[516] Hearing of Aug. 4, 2010, at 15 (statement of James Baker).

[517] Hearing of Aug. 4, 2010, at 32 (statement of Randall Larsen).

[518] Hearing of Aug. 4, 2010, at 2 (written statement of Randall Larsen).

[519] Hearing of Aug. 4, 2010, at 3 (written statement of Randall Larsen).

[520] Hearing of Aug. 4, 2010, at 43 (statement of Randall Larsen).

[521] Hearing of Aug. 4, 2010, at 3 (written statement of Randall Larsen).

[522] Hearing of Aug. 4, 2010, at 4 (written statement of Randall Larsen).

[523] Hearing of Aug. 4, 2010, at 4 (written statement of Randall Larsen).

Coordinating Committee back, bringing the very senior leaders into the White House to look at this. [It] was there in the Clinton . . . and Bush Administration[s] and it went away in the Obama Administration."[524]

ELECTROMAGNETIC PULSE: STATE OF PREPAREDNESS

If a nuclear weapon is detonated hundreds of miles above the Earth, the resulting radiation would interact with the Earth's atmosphere to produce an electromagnetic pulse (EMP).[525] The resulting EMP waves could cause severe damage to electronic devices and a single weapon could affect much of the United States.[526] An EMP event could potentially cause the power grid to collapse entirely.[527] Recovery could take months, even years.[528] Our low orbit satellite infrastructure would be in danger as well.[529] That these types of events could occur is not theoretical. In 1962, the United States conducted a high-altitude nuclear test 400 kilometers above Johnston Island, 825 miles southwest of Hawaii. The resulting nuclear blast knocked out street lights across Hawaii, tripped circuit breakers, triggered burglar alarms, and damaged a telecommunications relay facility on the island of Kauai.[530] Colonel Larsen pointed out that the sun poses the most likely EMP threat to America and noted that preparing the nation to withstand an EMP event will protect the country from either a man-made or a solar event.[531]

Dr. Frankel, Executive Director, Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, testified that while the response of the military infrastructure to the findings and recommendations of the Commission was very positive, the response of the civilian infrastructure was not.[532] Frankel testified that DHS has given no thought to the notion that a nuclear device might be launched and used in EMP mode, and, therefore, there is a component of the

---

[524] Hearing of Aug. 4, 2010, at 46 (statement of Randall Larsen).

[525] Hearing of Aug. 4, 2010, at 4 (statement of Jon Kyl).

[526] Hearing of Aug. 4, 2010, at 4 (statement of Jon Kyl).

[527] Hearing of Aug. 4, 2010, at 39 (statement of Michael Frankel).

[528] Hearing of Aug. 4, 2010, at 39 (statement of Michael Frankel).

[529] Hearing of Aug. 4, 2010, at 39 (statement of Michael Frankel).

[530] Matthew Harwood, *DHS Need to Take Threat of EMP Attack Seriously, Physicist Warns*, SEC. MGMT, Aug. 5, 2010, *available at* http://www.securitymanagement.com/news/dhs-needs-take-threat-emp-attack-seriously-physicist-warns-007500.

[531] Hearing of Aug. 4, 2010, at 50 (statement of Randall Larsen).

[532] Hearing of Aug. 4, 2010, at 40 (statement of Michael Frankel).

nuclear problem that DHS is simply not addressing.[533] Frankel stated that "protection of the nation's critical infrastructures from an EMP threat is both feasible and well within the Nation's means and resources to accomplish."[534] Senator Kyl expressed concern that the government is particularly ill-equipped to respond to the threat posed by an EMP attack[535] and asked for recommendations for solving this issue.[536] Frankel noted that direction coming down from the top is indispensable,[537] and he suggested that the Secretary of DHS should have a reporting requirement that would force him to appoint someone to a leadership position at the confirmed level.[538]

OFFICE OF NATIONAL CAPITAL REGION COORDINATION: STATE OF PREPAREDNESS

The Office of National Capital Region Coordination (NCRC) is located in the Department of Homeland Security's (DHS) Federal Emergency Management Agency (FEMA).[539] Congress created NCRC to, among other things, oversee and coordinate federal programs for, and relationships with, state, local, and regional authorities within the National Capital Region (NCR) to enhance domestic preparedness.[540]

Unlike other agencies discussed at the hearing, NCRC seemed well prepared to respond to a WMD attack. According to NCRC Director Steward Beckham, NCRC has established a course of action to mobilize and coordinate a "well-organized response and recovery"[541] in the event of a WMD attack. NCRC has fostered strong partnerships and collaboration with state, local, and regional authorities in the NCR[542] and has developed or is in the process of developing a number of projects that Beckham cites as examples of NCRC's commitment to concerted action.[543] These include data and information sharing systems, the Metrorail Tunnel Response Operations, disease

---

[533] Hearing of Aug. 4, 2010, at 41 (statement of Michael Frankel).

[534] Hearing of Aug. 4, 2010, at 41 (statement of Michael Frankel).

[535] Hearing of Aug. 4, 2010, at 4 (statement of Jon Kyl).

[536] Hearing of Aug. 4, 2010, at 44 (statement of Jon Kyl).

[537] Hearing of Aug. 4, 2010, at 44 (statement of Michael Frankel).

[538] Hearing of Aug. 4, 2010, at 44 (statement of Michael Frankel).

[539] Hearing of Aug. 4, 2010, at 17 (statement of Steward Beckham).

[540] Hearing of Aug. 4, 2010, at 17 (statement of Steward Beckham).

[541] Hearing of Aug. 4, 2010, at 21 (statement of Steward Beckham).

[542] Hearing of Aug. 4, 2010, at 17 (statement of Steward Beckham).

[543] Hearing of Aug. 4, 2010, at 19 (statement of Steward Beckham).

surveillance systems, exercises and drills, and various equipment purchases.[544] Senator Cardin expressed concern about the coordination between NCRC and local governments, asking, for example, how NCRC's response would be coordinated if a WMD attack occurred in Maryland.[545] Beckham replied with the steps that would be taken, including reaching out to the homeland security adviser for Maryland and giving him the appropriate, available information, as well as involving the Secretary of DHS and even the President himself.[546]

CONCLUSION

The Subcommittee agreed that the government, as a whole, is insufficiently prepared to respond to the threat of WMDs being used against the United States.[547] All present at the hearing seemed to agree that the lack of clear working chains of command is a significant factor in the nation's unpreparedness. Senator Cardin noted that "in addition to the agencies being adequately prepared, you need the force and authority of the Administration and the President behind this issue. You need chain of command and you need training."[548]

[544] Hearing of Aug. 4, 2010, at 19-20 (statement of Steward Beckham).

[545] Hearing of Aug. 4, 2010, at 27 (statement of Benjamin Cardin).

[546] Hearing of Aug. 4, 2010, at 28 (statement of Steward Beckham).

[547] Hearing of Aug. 4, 2010, at 47 (statement of Benjamin Cardin).

[548] Hearing of Aug. 4, 2010, at 47 (statement of Benjamin Cardin).

APPENDIX:
HEARINGS DURING THE 111TH CONGRESS

PROTECTING NATIONAL SECURITY AND CIVIL LIBERTIES:
STRATEGIES FOR TERRORISM INFORMATION SHARING

21 April 2009

WITNESSES

Ms. Zoe Baird
President, Markle Foundation
Co-Chair, Markle Foundation Task Force on National Security in the Information Age
New York, NY

The Honorable Slade Gorton
Former United States Senator from Washington
Member, Markle Foundation Task Force on National Security in the Information Age
Seattle, WA

Mr. J. Thomas Manger
Chief of Police
Montgomery County, MD
Chairman, Legislative Committee, Major Cities Chiefs Association
Rockville, MD

Ms. Caroline Fredrickson
Director, Washington Office
American Civil Liberties Union
Washington, DC

THE PASSPORT ISSUANCE PROCESS:
CLOSING THE DOOR TO FRAUD

5 May 2009

WITNESSES

Ms. Brenda Sprague
Deputy Assistant Secretary for Passport Services
Bureau of Consular Affairs
United States Department of State
Washington, DC

Mr. Jess T. Ford
Director, International Affairs and Trade Team
United States Government Accountability Office
Washington, DC

PROSECUTING TERRORISTS:
CIVILIAN AND MILITARY TRIALS FOR GUANTANAMO AND BEYOND

28 July 2009

WITNESSES

PANEL 1:

The Honorable David Kris
Assistant Attorney General
National Security Division
United States Department of Justice
Washington, DC

The Honorable Jeh C. Johnson
General Counsel
United States Department of Defense
Arlington, VA

PANEL 2:

David Laufman
Partner
Kelley Drye & Warren LLP
Washington, DC

Deborah Pearlstein
Associate Research Scholar
Woodrow Wilson School of Public and International Affairs
Princeton, NJ

Michael Edney
Gibson, Dunn & Crutcher LLP
Washington, DC

STRENGTHENING SECURITY AND OVERSIGHT
AT BIOLOGICAL RESEARCH LABORATORIES

22 September 2009

WITNESSES

PANEL 1:

Mr. Daniel D. Roberts
Criminal Justice Information Services
Federal Bureau of Investigation
United States Department of Justice
Washington, DC

Ms. Jean Reed
Deputy Assistant to the Secretary of Defense
Chemical and Biological Defense / Chemical Demilitarization
United States Department of Defense
Arlington, VA

Mr. Brandt Pasco
Compliance Assurance Program Manager
United States Department of Homeland Security
Washington, DC

PANEL 2:

The Honorable Robert Graham
Former United States Senator from Florida
Chair, Commission for the Prevention of Weapons of Mass Destruction
Proliferation and Terrorism
Washington, DC

Dr. Nancy Kingsbury
Managing Director, Applied Research and Methods
United States Government Accountability Office
Washington, DC

Mr. Michael Greenberger
Director, Center for Health and Homeland Security
University of Maryland, Baltimore
Baltimore, MD

CYBERSECURITY:
PREVENTING TERRORIST ATTACKS AND PROTECTING PRIVACY IN CYBERSPACE

17 November 2009

WITNESSES

PANEL 1:

Mr. James Baker
Associate Deputy Attorney General, Deputy Attorney General Office
United States Department of Justice
Washington, DC

Mr. Philip Reitinger
Deputy Under Secretary, National Protection and Programs Directorate
Director, National Cyber Security Center
United States Department of Homeland Security
Washington, DC

Mr. Richard Schaeffer
Director, Information Assurance Directorate
National Security Agency
United States Department of Defense
Fort Meade, MD

Mr. Steven R. Chabinsky
Deputy Assistant Director, Cyber Division
Federal Bureau of Investigation
United States Department of Justice
Washington, DC

PANEL 2:

Mr. Gregory T. Nojeim
Senior Counsel and Director,
Project on Freedom, Security & Technology,
Center for Democracy and Technology
Washington, DC

Mr. Larry Clinton
President, Internet Security Alliance
Arlington, VA

Larry M. Wortzel, Ph.D.
Vice Chairman, United States - China Economic and Security Review Commission
Washington, DC

THE ESPIONAGE STATUTES: A LOOK BACK AND A LOOK FORWARD

12 May 2010

WITNESSES

Stephen Vladeck
Professor of Law
American University Washington College of Law
Washington, DC

Jeffrey H. Smith
Partner
Arnold and Porter
Washington, DC

Kenneth L. Wainstein
Partner
O'Melveny and Myers
Washington, DC

THE PASSPORT ISSUANCE PROCESS: CLOSING THE DOOR TO FRAUD, PART II

29 July 2010

WITNESSES

Ms. Brenda Sprague
Deputy Assistant Secretary for Passport Services
Bureau of Consular Affairs
United States Department of State
Washington, DC

Mr. Gregory D. Kutz
Managing Director, Forensic Audits and Special Investigations Unit
United States Government Accountability Office
Washington, DC

GOVERNMENT PREPAREDNESS AND RESPONSE TO A TERRORIST ATTACK

4 August 2010

WITNESSES

The Honorable Glenn A. Fine
Inspector General
United States Department of Justice
Washington, DC

Mr. James A. Baker
Associate Deputy Attorney General
United States Department of Justice
Washington, DC

Mr. Steward D. Beckham
Director, Office of National Capital Region Coordination
Federal Emergency Management Agency
United States Department of Homeland Security
Washington, DC

Colonel Randall J. Larsen, USAF (Retired)
Executive Director, Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism
Washington, DC

Michael J. Frankel, Ph. D.
Executive Director, Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack
McLean, VA