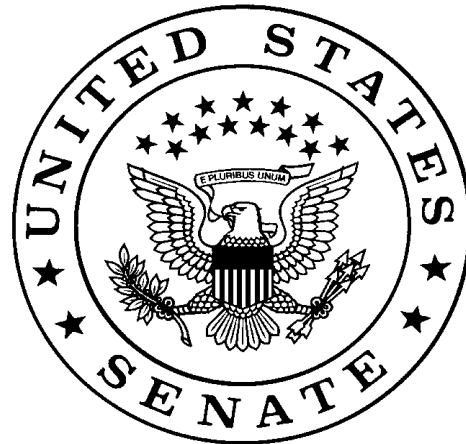


**UNITED STATES SENATE  
COMMITTEE ON THE JUDICIARY  
SUBCOMMITTEE ON TERRORISM, TECHNOLOGY, AND HOMELAND SECURITY**

**SENATOR JON KYL  
CHAIRMAN**

**SENATOR DIANNE FEINSTEIN  
RANKING DEMOCRAT**



**Three Years After September 11:  
Keeping America Safe**

---

**108<sup>TH</sup> CONGRESS**

**March 2005**

**Report Submitted by Majority and Minority Staff**

**W**e 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*<sup>1</sup>  
November 2001

**T**his new enemy seeks to destroy our freedom and impose its views. We value life; the terrorists ruthlessly destroy it. We value education; the terrorists do not believe women should be educated or should have health care, or should leave their homes. We value the right to speak our minds; for the terrorists, free expression can be grounds for execution. We respect people of all faiths and welcome the free practice of religion; our enemy wants to dictate how to think and how to worship even to their fellow Muslims.

— *President George W. Bush*<sup>2</sup>  
November 8, 2001

**W**e have come together with a unity of purpose because our nation demands it. September 11, 2001, was a day of unprecedented shock and suffering in the history of the United States. The nation was unprepared. How did this happen, and how can we avoid such tragedy again? . . . We learned about an enemy who is sophisticated, patient, disciplined, and lethal. The enemy rallies broad support in the Arab and Muslim world by demanding redress of political grievances, but its hostility toward us and our values is limitless. Its purpose is to rid the world of religious and political pluralism, the plebiscite, and equal rights for women. It makes no distinction between military and civilian targets. *Collateral damage* is not in its lexicon.

— *The 9/11 Commission Report*<sup>3</sup>  
July 2004

---

<sup>1</sup> “*I Was the Most Optimistic*”; *Transcript of the Osama bin Laden Videotape*, NEWSWEEK, Dec. 24, 2001, at 14.

<sup>2</sup> *President’s Address to the Nation on Homeland Security from Atlanta*, 37 WKLY. COMP. PRES. DOC. 1614 (Nov. 8, 2001).

<sup>3</sup> THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, 108TH CONG., THE 9/11 COMMISSION REPORT vx-vxi (2004) (emphasis in original).

---

## CONTENTS

---

**Introduction by Chairman Jon Kyl and Ranking Democrat Dianne Feinstein.....vii**

**Overview.....1**

**Executive Summary .....3**

### HOMELAND SECURITY

#### **“Lone-Wolf”**

**Fix.....10**

    “Lone-Wolf” Terrorists .....10  
    Changed World Requires a Change in FISA .....11  
    Islamist Terrorist Threat .....11  
    Development of a “Lone-Wolf” Fix .....13

#### **Pretrial Detention of Terrorists**

**.....14**

    Filling Gaps in the Law

**.....14**

    Pretrial Detention .....14

    Post-Release Supervision .....15

**Tools To Fight Terrorism Act.....16**

    A Three-Year Gap in Anti-Terror Legislation .....16

    Knitting Together Years of Legislation .....16

    Prevention of Terrorist Access to Special Weapons .....18

    Providing Material Support and Receiving Military Training From Terrorists .....19

    Improving TFTA So It Will Pass Constitutional Muster .....21

**Crime Victims’ Rights .....22**

    Passing the Crime Victims’ Rights Act .....22

### TECHNOLOGICAL SECURITY

**Document Security and Identity Theft .....24**

    Identity Theft: A “Key Catalyst” for Terrorist Groups .....24

    GAO Report Finds Vulnerabilities .....25

Key Methods for Terrorist Infiltration .....	26
Identity Theft Penalty Enhancement Act .....	27
Mandatory Penalty Enhancements .....	27
Removal of Judicial Discretion .....	28
Bank Officers and Social Security Fraud .....	28
New Tools of Prevention .....	29
Making Full Use of the Identity Theft Penalty Enhancement Act .....	29
The Future of Identity Theft and Phishing .....	30
<b>Virtual Threat, Real Terror: Cyberterrorism .....</b>	<b>32</b>
Virtual Threat, Real Terror .....	32
Tracking Down Cyber Intruders and the Importance of the Patriot Act .....	34
Lacking a Cyberterrorism Threat Assessment .....	35
Interagency Responsibility .....	37
Public/Private Cooperation Has a Long Way to Go .....	38
Making Combating Cyberterrorism a Priority .....	38
<b>Database Security .....</b>	<b>41</b>
Preventing Unauthorized Access .....	41
The Notification of Risk to Personal Data Act .....	43
Cyber-Crooks Gaining the Upper Hand .....	44

## **SEAPORT SECURITY**

<b>Seaport Security .....</b>	<b>45</b>
The Importance of America's Seaports and the Dangers of Attack .....	45
Extending the Security Net: Identifying and Interpreting Threats Before They Happen .....	47
Improving Security at the Ports: Targeted Screening, Security Plans, and Pilot Programs .....	48
Working with the Private Sector: Improving Security Without Hindering Trade .....	49
Follow-Up Hearing and Future Legislation .....	50

## **BORDER SECURITY**

<b>Role of Technology in Border Security.....</b>	<b>51</b>
Border Technology .....	51
The Enhanced Border Security and Visa Reform Act .....	52
Border Security Challenges .....	52
Looking Ahead .....	54

<b>Securing the United States through Biometrics .....</b>	<b>55</b>
The Biometric Passport Deadline .....	55
The Visa Waiver Program .....	56
Why Biometrics? .....	57
Biometric Deadline Challenges .....	58
A Plan to Ensure Compliance .....	59
Other Concerns About Biometrics and the Visa Waiver Program .....	59
Hearing Aftermath .....	60

<b>Drug Trafficking and Terrorism — A Dangerous Mix .....</b>	<b>61</b>
Link Between International Drug Traffickers and Terrorists .....	61
Global Phenomenon .....	62
Narcoterror Problem Also an Opportunity .....	64

**“AFTER-ATTACK” SECURITY**

<b>First Responders.....</b>	<b>64</b>
Responding to Terrorist Attacks .....	64
Faster and Smarter Funding .....	65
<b>Rapid Bioterrorism Detection and Response: Project Zebra .....</b>	<b>66</b>
The Current State of Affairs .....	66
What is Project Zebra? .....	67
Creation of National Database .....	69
Data Transmitting Network and Training Protocol .....	70
Laboratory Security .....	70
A Vast Undertaking .....	71

**DOMESTIC SECURITY**

<b>Wahhabism.....</b>	<b>72</b>
An Extremist Ideology .....	72
The Spread of Wahhabism and the Threat from Al Qaeda .....	73
Epicenter of Terrorist Financing .....	74

<b>Saudi Arabia .....</b>	<b>75</b>
Connecting the Dots .....	75
Saudis Playing a Double Game .....	77
Ending the Double Game .....	78

<b>Radical Islamist Influence of the Chaplaincy of the U.S. Military and Prisons .....</b>	<b>79</b>
--	-----------

Terrorist Exploitation of a Free Society .....	79
Bureau of Prisons and Department of Defense .....	80
<b>Bureau of Prisons’ Response to the Subcommittee Hearing .....</b>	<b>82</b>
Deficiencies in the Chaplaincy Program .....	82
Looking Ahead .....	84
<b>Department of Defense’s Response to the Subcommittee Hearing .....</b>	<b>84</b>
Deficiencies in the Chaplaincy Program .....	84
Chaplains of Any Faith .....	85
Strengthening the Department of Defense’s Oversight Role .....	86
Establishing Screening Procedures and Strengthening Information-Sharing .....	86
Procedures for Removing Chaplains for Cause .....	88
Internal Procedures to Formalize Policy .....	89
Implementation of All Inspector General Recommendations .....	89
<b>Appendix A: Hearings During the 108<sup>th</sup> Congress .....</b>	<b>90</b>
<b>Appendix B: Information for Victims of Identity Theft .....</b>	<b>97</b>
<b>Appendix C: Avoid Becoming a Victim of “Phishing” .....</b>	<b>99</b>
<b>Appendix D: Tools to Fight Terrorism Act of 2004 .....</b>	<b>101</b>

---

## 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, which crashed into the North Tower of the World Trade Center; United Airlines Flight 175, which crashed into the South Tower of the World Trade Center; American Airlines Flight 77, which crashed into the Pentagon; and United Airlines Flight 93, which crashed in Somerset County, Pennsylvania.<sup>4</sup> Masterminded by Osama bin Laden and his Al Qaeda terrorist network, the attacks killed 3,016 people,<sup>5</sup> and wounded thousands more.<sup>6</sup>

On that day, we were, in President Bush's words, "a country awakened to danger and called to defend freedom."<sup>7</sup> 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 — then we would be forever on the defensive, and the primary battlefield would not be in Iraq or Afghanistan, but right here at home. One obvious sign of the success of our actions over the past three years is that, defying many predictions, we have not had another terrorist attack on our soil. Terrorists have instead gone after easier targets abroad. Nonetheless, our actions thus far are insufficient; there is much to be done. The magnitude of the challenge is illustrated by the 1984 assassination attempt on Prime Minister Margaret Thatcher by IRA terrorists. Their warning — and one that remains

---

<sup>4</sup> *A Nation Challenged; Indictment Chronicles "Overt Acts" That It Says Led to Sept. 11 Attacks*, N.Y. TIMES, Dec. 12, 2001, at B6.

<sup>5</sup> James Barron, *Two Years Later: Ceremonies; Another 9/11, and a Nation Mourns Again*, N.Y. TIMES, Sept. 12, 2003, at A1.

<sup>6</sup> David Chen, *Man Behind Sept. 11 Fund Describes Effort as a Success, With Reservations*, N.Y. TIMES, Jan. 1, 2004, at B1.

<sup>7</sup> 147 CONG. REC. S9553 (daily ed. Sept. 20, 2001) (Address by President George W. Bush to Joint Session of Congress).

relevant today — was: “Remember, we only have to get lucky once; you have to be lucky always.”<sup>8</sup> As Vice President Cheney has said, “if we’re 99 percent successful, the one percent that gets through can still kill you.”<sup>9</sup> We have done much to turn the odds in our favor — but terrorists remain a grave threat to national security and public safety.

Believing that we could not effectively fight terrorists unless we understood them, the Subcommittee focused its efforts during the 108<sup>th</sup> Congress on learning what motivates them, where they derive their support, and how they operate. To this end, hearings were held on the growing Wahhabi influence in the United States, the terrorist links to Saudi Arabia, and the radical Islamist influence in the United States, including in the chaplaincy of the U.S. military and in U.S. prisons. Other hearings examined ways to respond to terrorist attacks, bioterrorism, border security technology, links between terrorist and drug traffickers, seaport security, cyberterrorism, and law-enforcement tools to fight terrorism. The attached report is a summary of the Subcommittee’s efforts to understand the terrorist threats to the United States and what remains to be done to win the war on terrorism.

JON KYL  
Chairman  
Subcommittee on Terrorism, Technology,  
and Homeland Security  
Committee on the Judiciary  
United States Senate

DIANNE FEINSTEIN  
Ranking Democrat  
Subcommittee on Terrorism, Technology,  
and Homeland Security  
Committee on the Judiciary  
United States Senate

---

<sup>8</sup> See, e.g., Paul Brown, *Cabinet Survives IRA Hotel Blast*, SUNDAY UK GUARDIAN, Oct. 13, 1984.

<sup>9</sup> Mark Leibovich, *The Strong, Silent Type*, WASH. POST, Jan. 18, 2004, at D01.

---

## THREE YEARS AFTER SEPTEMBER 11: KEEPING AMERICA SAFE

---

### Overview

In the 108<sup>th</sup> Congress, the Senate Judiciary Committee's Subcommittee on Terrorism, Technology, and Homeland Security was the most active Judiciary Committee subcommittee, holding thirteen hearings.<sup>10</sup> The Subcommittee held a series of three hearings to investigate the roots of terrorist ideology, terrorist support networks, and state sponsorship of terrorism. Additionally, the Subcommittee pursued ways to respond to terrorist attacks; combat bioterrorism; keep terrorists out of the country; fight the plague of narcoterrorism; ensure document security and cyber security; investigate "lone-wolf" terrorists; detain suspected terrorists before trial; provide law enforcement with tools to fight terrorism; and ensure rights for crime victims.

The Subcommittee's hearings bore great fruit, leading (among other things) to the introduction of a bill on seaport security;<sup>11</sup> reports by the Inspectors General of the Department of Justice<sup>12</sup> and the Department of Defense;<sup>13</sup> and the enactment of the Identity Theft Penalty Enhancement Act,<sup>14</sup> the "Lone-Wolf Fix" to the Foreign Intelligence Surveillance Act,<sup>15</sup> the pre-

---

<sup>10</sup> Number of hearings listed in parentheses after subcommittee name: Terrorism, Technology, and Homeland Security (13, including two hearings held at the full Committee but run by the Subcommittee); Immigration, Border Security, and Citizenship (8); Antitrust, Competition Policy, and Consumer Rights (6); Constitution, Civil Rights, and Property Rights (6); Administrative Oversight and the Courts (3); and Crime, Corrections, and Victims' Rights (2). *All Hearings, at U.S. Senate, Comm. on the Judiciary Home*: [http://judiciary.senate.gov/schedule\\_all.cfm](http://judiciary.senate.gov/schedule_all.cfm) (last visited Jan. 28, 2005).

<sup>11</sup> S. 2653, 108<sup>th</sup> Cong. (2004).

<sup>12</sup> U.S. Dep't of Just., Off. of the Inspector Gen., *A Review of Federal Bureau of Prisons' Selection of Muslim Religious Services Providers*, prepared April 2004 [hereinafter "DOJ OIG Report, April 2004"].

<sup>13</sup> U.S. Dep't of Def., Off. of the Inspector Gen., *Crystal Focus: DoD Chaplain Program*, prepared November 2004 [hereinafter "DoD OIG Report, Nov. 2004"].

<sup>14</sup> Pub. L. No. 108-275 (July 15, 2004).

<sup>15</sup> Pub. L. No. 108-458 (Dec. 17, 2004).

trial detention of terrorists,<sup>16</sup> and provisions to (1) allow sharing of grand jury information with state and local governments, (2) punish and deport persons who receive military-type training from a terrorist group, (3) expand and clarify the material support statute, (4) punish concealment of terrorist financing, (5) punish military and terrorist hoaxes, (6) increase penalties for obstruction of justice in a terror case, (7) expand weapons of mass destruction prohibitions and punish aiding rogue states' weapons of mass destruction efforts, and (8) severely punish possession of shoulder-fired anti-aircraft rockets, atomic, radiological bombs, and smallpox virus.<sup>17</sup>

The Subcommittee's efforts to provide both oversight and legislative improvement 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 has directed significant resources to this end, receiving briefings, reports, and engaging in independent research, all designed to complement the hearing process as a mechanism for understanding the successes and failures of policies designed to combat terrorism.

The Subcommittee's efforts in this respect have generally met with success. The Subcommittee has been able to craft a bi-partisan approach to oversight, as is illustrated by this joint report. While the Departments of Justice and Homeland Security have provided information to the Subcommittee, requests to the Department of Justice to provide a comprehensive report assessing the effect and efficacy of the sixteen provision of the Patriot Act subject to "sunset" remain unfulfilled. Such a report is a critical element in the Subcommittee's, and indeed the entire Committee's, responsibility to provide meaningful oversight before determining whether to change the law with respect to these provisions.

Many of the issues within the Subcommittee's jurisdiction are among the most controversial in American public life. What is the best way to balance effective counter-terrorism against civil liberties? How does the government ensure that adequate intelligence is acquired and disseminated to allow effective strategic and tactical decisions that can keep us safer? Such questions must be answered, and it is one of the critical functions of the Subcommittee to ensure that they can be answered in a credible way, based on careful and thorough oversight.

In the 109<sup>th</sup> Congress, the Subcommittee intends to pursue the answers to such questions and to provide effective oversight of the functions of government within its jurisdiction.

---

<sup>16</sup> Pub. L. No. 108-458 (Dec. 17, 2004).

<sup>17</sup> Pub. L. No. 108-458 (Dec. 17, 2004).

## Executive Summary

Key findings and accomplishments:

### HOMELAND SECURITY

- ▶ **“Lone-Wolf” terrorists represent a new threat.** According to testimony by the Attorney General, “[s]ingle, lone-wolf terrorists act and can act in ways that are very, very damaging.”<sup>18</sup> Legislation introduced by Chairman Kyl, S. 113, updated the Foreign Intelligence Surveillance Act to permit surveillance of individual foreign visitors to the United States who appear to be involved in international terrorism, without regard to whether such persons are affiliated with a foreign government or terrorist group.<sup>19</sup> Both the FBI Director and the Attorney General testified in support of this bill.<sup>20</sup> It passed the Senate on May 8, 2003 and was enacted in December 2004 as Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (S. 2845).<sup>21</sup>
- ▶ **Legal sanctions were less stringent for terrorism than drug-related crimes.** While there is a statutory presumption in favor of denying bail to defendants accused of some crimes, such as those involving drugs, the presumptive detention did not apply to acts of terrorism. This inconsistency prompted Chairman Kyl to introduce S. 1606 to amend the criminal code to presumptively deny pre-trial release to persons charged with acts of terrorism.<sup>22</sup> This provision was enacted in December 2004 as Section 6952 of the Intelligence Reform and Terrorism Prevention Act.<sup>23</sup>
- ▶ **Law-enforcement must be given the correct tools to fight terrorism.** Before the Intelligence Reform and Terrorism Prevention Act of 2004, no major anti-terror legislation had been enacted since the USA Patriot Act in the weeks following September 11, despite numerous gaps discovered in the U.S. anti-terror

---

<sup>18</sup> *The War Against Terrorism: Working Together to Protect America: Hearing Before the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 1<sup>st</sup> Sess. (Mar. 4, 2003) (S. Hrg. 108-137, Serial No. J-108-3), at 19 (statement of John Ashcroft) [hereinafter “Hearing of Mar. 4, 2003”].

<sup>19</sup> S. 113, 108<sup>th</sup> Cong. (2003).

<sup>20</sup> Hearing of Mar. 4, 2003, at 19 (statements of John Ashcroft and Robert Mueller).

<sup>21</sup> Pub. L. No. 108-458 (Dec. 17, 2004).

<sup>22</sup> S. 1606, 108<sup>th</sup> Cong. (2003).

<sup>23</sup> Pub. L. No. 108-458 (Dec. 17, 2004).

system. Chairman Kyl's Tools to Fight Terrorism Act (S. 2679) combines 11 different bills introduced over the past several years in order to close loopholes in existing law and provide law-enforcement with constitutionally sound tools to prevent, disrupt, and prosecute terrorism.<sup>24</sup> In addition to the "lone-wolf" and pretrial detention provisions of TFTA (discussed above), the IRTPA enacted about half of TFTA. Specifically, the IRTPA includes TFTA's provisions to allow sharing of grand jury information with state and local governments; punish and deport persons who receive military-type training from a terrorist group; expand and clarify the material support statute; punish concealment of terrorist financing; punish military and terrorist hoaxes; increase penalties for obstruction of justice in a terror case; expand WMD prohibitions and punish aiding rogue states' WMD efforts; and severely punish possession of shoulder-fired anti-aircraft rockets, atomic, radiological bombs, and the smallpox virus.<sup>25</sup>

- ▶ **Victims of terrorism and of all crimes acquire desperately needed rights.** The Oklahoma City bombing was one of the worst acts of domestic terrorism in American history: the bombing of the Alfred P. Murrah Federal Building in Oklahoma City killed 168 people and injured more than 500 others.<sup>26</sup> In October 2004, the Justice for All Act, which includes a guarantee of crime victims' rights, was signed into law.<sup>27</sup> The Act recognizes the right of victims of terrorism and of all crime to receive notice of public criminal-justice events, to be present during those proceedings, to be heard at the proceedings, to be protected from unreasonable delays, and to have their safety taken into account.

## TECHNOLOGICAL SECURITY

- ▶ **Nearly 10 million Americans were victims of identity theft in 2003.**<sup>28</sup> As witnesses testified at a Subcommittee hearing, terrorists have "long utilized identity theft as well as Social Security Number fraud to enable them to obtain . . . cover employment and access to secure locations."<sup>29</sup> In response to the growing

---

<sup>24</sup> S. 2679, 108<sup>th</sup> Cong. (2004).

<sup>25</sup> Pub. L. No. 108-458 (Dec. 17, 2004).

<sup>26</sup> Lois Romano & Tom Kenworthy, *McVeigh Guilty on All 11 Counts*, WASH. POST, June 3, 1997, at A01.

<sup>27</sup> Pub. L. No. 108-405 (Oct. 30, 2004).

<sup>28</sup> Attorney General John Ashcroft, Remarks at the Department of Justice (Aug. 26, 2004), at <http://www.usdoj.gov/ag/speeches/2004/82604ag.htm>.

<sup>29</sup> *Identity Theft Penalty Enhancement Act of 2002: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (July 9, 2002) (S. Hrg. 107-900, Serial No. J-107-68), at 89-90 (written statement of Dennis Lormel) [hereinafter "Hearing of July

threat of identity theft, Chairman Kyl and Senator Feinstein introduced S. 153, which significantly enhances law-enforcement tools necessary both to prevent identity theft when possible and to vigorously prosecute the crime when deterrence fails.<sup>30</sup> The bill became law on July 15, 2004.<sup>31</sup>

- ▶ **Identity theft is the fastest growing crime in the United States.**<sup>32</sup> Preventing terrorists and other criminals from hacking into databases to obtain sensitive personal data is essential. When databases have been so compromised, there must be prompt victim notification; however, such notification is the exception to the rule, not the norm.<sup>33</sup> Recognizing this fact and the gravity of the threat, Senator Feinstein introduced S. 1350, which requires businesses to inform customers of hacking incidents that could compromise their sensitive personal data.<sup>34</sup> Action on the bill was not completed on the bill before the end of the 108<sup>th</sup> Congress.
- ▶ **Cyber attacks have increased in both frequency and effectiveness.**<sup>35</sup> Terrorists are using cyber tools to raise funds and organize physical attacks, and they can use these same tools to conduct cyber warfare. A Subcommittee hearing made clear that while the USA Patriot Act has played a vital role in detecting and prosecuting cyberterrorism,<sup>36</sup> there must be better cooperation among government agencies to develop a clear assessment of the threat and to clarify their respective roles in preventing cyberterrorism.

## SEAPORT SECURITY

---

9, 2002”].

<sup>30</sup> S. 153, 108<sup>th</sup> Cong. (2003).

<sup>31</sup> Pub. L. No. 108-275 (July 15, 2004).

<sup>32</sup> *Database Security: Finding Out When Your Information Has Been Compromised: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 1<sup>st</sup> Sess. (Nov. 4, 2003) (S. Hrg. 108-520, Serial No. J-108-52), at 8 (statement of Evan Hendricks) [hereinafter “Hearing of Nov. 4, 2003”].

<sup>33</sup> Hearing of Nov. 4, 2003, at 8 (statement of Evan Hendricks).

<sup>34</sup> S. 1350, 108<sup>th</sup> Cong. (2003).

<sup>35</sup> CERT Coordination Center, *CERT/CC Statistics 1988-2003*, available at [http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html) (last visited Jan. 21, 2005).

<sup>36</sup> *Virtual Threat, Real Terror: Cyberterrorism in the 21<sup>st</sup> Century: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (Feb. 24, 2004) (S. Hrg. 108-516, Serial No. J-108-58), at 64 (written statement of John Malcolm) [hereinafter “Hearing of Feb. 24, 2004”].

- ▶ **Seaport security remains dangerously deficient.** The effects of a terrorist attack on a U.S. seaport could be catastrophic. By one estimate, a nuclear weapon detonated in a major seaport or Washington, D.C., would kill 50,000 to one million people, would result in direct property damage of \$50 billion to \$500 billion, would cause trade disruption of \$100 billion to \$200 billion, and would create indirect costs of \$300 billion to \$1.2 trillion.<sup>37</sup> After a Subcommittee hearing on this topic, Chairman Kyl and Senator Feinstein introduced S. 746 to close loopholes in current law and toughen sanctions, including criminal charges, for certain offenses related to seaport security and international shipping.<sup>38</sup>

## **BORDER SECURITY**

- ▶ **Steps to prevent terrorists from entering the United States have been implemented.** According to testimony before the Subcommittee by the Department of Homeland Security (DHS) Under Secretary, Asa Hutchinson, “[t]echnology is a critical tool that enables the . . . Department of Homeland Security to balance our national security imperative with the free flow of goods and people across our Nation’s borders . . .”<sup>39</sup> After September 11, DHS implemented improvements in technology and infrastructure (such as the implementation of the National Security Entry-Exit Registration System and non-intrusive cargo inspection systems) to prevent terrorists and terrorist-related goods from entering the United States. Still, Congress must work to ensure that the Department of Homeland Security receives adequate funding to meet deadlines for implementing additional terrorism-prevention technology and infrastructure.
- ▶ **Biometric Identifiers are essential to ensure the integrity of the Visa Waiver Program.** The Visa Waiver Program (VWP) allows nationals of 27 countries to enter the United States for business or tourism purposes with only a valid passport. The Program is important for both economic and foreign diplomacy purposes, but contained very few security procedures when instituted in 1986. Thus in 2002, Congress passed legislation that required the VWP countries to issue machine-readable, tamper-resistant passports that contain a biometric identifier by October 26, 2004. In June 2004, the Judiciary Committee held a

---

<sup>37</sup> Abt Associates, *The Economic Impact of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability*, Apr. 30, 2003, at 7 (executive summary).

<sup>38</sup> S. 746, 108<sup>th</sup> Cong. (2003).

<sup>39</sup> *Border Technology: Keeping Terrorists Out of the United States: Joint Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security and the Subcomm. on Immigration, Border Security and Citizenship of the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 1<sup>st</sup> Sess., (Mar. 12, 2003) (S. Hrg. 108-148, Serial No. J-108-5), at 15 (statement of Asa Hutchinson) [hereinafter “Hearing of Mar. 12, 2003”].

hearing aimed at ensuring that the U.S. government is taking every possible step to protect the country against terrorism, explored the implementation of biometric passports, the status of compliance with biometric requirements by VWP countries, the United States' compliance with the October 2004 deadline, and the wisdom of a deadline extension.<sup>40</sup> In July 2004, Congress extended that deadline for one year. Diplomatic pressure must be used to ensure that the VWP countries comply with the biometric deadline and that there is no longer such an open avenue through which terrorists can enter the country.

- ▶ **The illegal drug trade provides terrorists with a significant source of funding.** Terrorists have turned to drug trafficking as a major source of funding. In so doing, they have become more susceptible to law-enforcement actions that target drug trafficking, money laundering, and smuggling. The federal government should enhance intelligence capabilities and training that supports these law-enforcement activities. The Subcommittee will continue to periodically reexamine the progress against narcoterrorist activity, and the suitability of federal laws to combat the evolving narcoterrorist threat.

#### “AFTER-ATTACK” SECURITY

- ▶ **Resources for first responders must be allocated based on a threat analysis.** At a Subcommittee hearing, former Senator Warren Rudman, a Senior Advisor to the Council on Foreign Relations, presented the Council's report on antiterrorism preparedness and its chilling conclusion: “the United States must assume that terrorists will strike again,” and “the United States remains dangerously ill-prepared to handle a catastrophic attack on American soil.”<sup>41</sup> To ensure that the nation is prepared for the event a terrorist attack, the government must allocate money wisely, based on accurate threat analysis, not on a political or formulaic basis. A targeted, needs-based system should be developed for high-risk states and counties; border counties and states, which are high-risk by definition, should receive a more equitable proportion of first responder funding.
- ▶ **Project Zebra presents a method to rapidly detect and treat exposure to biological agents.** Using highly precise DNA fingerprinting technology, scientists can determine whether a patient has been exposed to any biological

---

<sup>40</sup> *Biometric Passports: Hearing Before the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 2<sup>nd</sup> Sess., (June 15, 2004) (transcript), at 1 (statement of Orrin Hatch) [hereinafter “Hearing of June 15, 2004”].

<sup>41</sup> Council on Foreign Relations, Independent Task Force on Emergency Responders, *Drastically Underfunded, Dangerously Unprepared*, prepared June 2003, at 1 [hereinafter “Emergency Responders Report, June 2003”], available at <http://www.cfr.org/pubs.php?year=2003&type-reports>.

pathogen.<sup>42</sup> This method of disease detection would revolutionize medical diagnoses as it could quickly, accurately, and, in many cases, pre-symptomatically identify the precise illness from which a patient suffers. The technology is vital in the war on terror. As Deputy Secretary of Defense Paul Wolfowitz stated, “As horrible as it was to have thousands of innocent Americans killed on our own territory . . . that is nothing compared to what terrorists could do with . . . biological weapons.”<sup>43</sup>

## DOMESTIC SECURITY

- ▶ **Wahhabism sows the seeds of terror.** In hearings examining the international terrorist movement, the Subcommittee examined Wahhabism, a separatist, exclusionary, and violent form of Islam that provides the ideological inducement, recruitment, training, and support infrastructure for international terrorists and terrorist groups such as Al Qaeda. All 19 of the terrorists who committed the horrific September 11 attacks were Wahhabi followers. Saudi Arabia has a deep historical and symbiotic relationship with the radical Islamic ideology of Wahhabism, which has impeded Saudi government cooperation with the United States in the war against terrorism.
- ▶ **The Saudis provide financing to the Al Qaeda terrorist network.** According to the testimony of a senior Treasury Department official before the Subcommittee, Saudi Arabia is the “epicenter” of terrorist financing.<sup>44</sup>
- ▶ **Wahhabism recruits support in U.S. prisons and the military.** Wahhabi activity in the United States has included efforts to influence the selection of Muslim clerics in U.S. prisons and the U.S. military. The chaplaincy programs of these institutions were in the past vulnerable to infiltration, but action has been

---

<sup>42</sup> *Rapid Bio-terrorism Detection and Response: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 2<sup>nd</sup> Sess., (May 11, 2004) (S. Hrg. 108-559, Serial No. J-108-74), at 9 (statement of David Relman) [hereinafter “Hearing of May, 11, 2004”].

<sup>43</sup> Deputy Secretary of Defense Paul Wolfowitz, Joint Press Conference with the Department of Health and Human Services and the Department of Homeland Security, at 5 (Apr. 28, 2004), available at <http://www.defenselink.mil/transcripts/2004/tr20040428-depsecdef1383.html>.

<sup>44</sup> *Terrorism: Growing Wahhabi Influence in the United States: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 1<sup>st</sup> Sess. (June 26, 2003) (S. Hrg. 108-267, Serial No. J-108-21), at 12 (statement of David Aufhauser) [hereinafter “Hearing of June 26, 2003”].

recommended by the Inspector Generals at the Departments of Justice and Defense to reduce the opportunity for such influence.<sup>45</sup>

- ▶ **Islamic chaplains present a continuing security risk in U.S. prisons.** As one Wahhabi prison chaplain stated, “prison is the perfect recruitment and training ground for radicalism and the Islamic religion.”<sup>46</sup> The Office of Inspector General has concluded that the Bureau of Prisons has taken specific action to fully address all 16 of the Inspector General’s recommendations.<sup>47</sup>
  
- ▶ **Religious organizations with links to terrorism endorse military chaplains.** The military will remain vulnerable to Wahhabist and terrorist infiltration until it imposes greater oversight of religious organizations with whom it cooperates and creates non-religious criteria to prevent organizations with links to terrorism from endorsing chaplains.

---

<sup>45</sup> U.S. Dep’t of Def., Off. of the Inspector Gen., *Crystal Focus: DoD Chaplain Program*, prepared November 2004, at 1 [hereinafter “DoD OIG Report, Nov. 2004”]; U.S. Dep’t of Just., Off. of the Inspector Gen., *A Review of Federal Bureau of Prisons’ Selection of Muslim Religious Services Providers*, prepared April 2004 [hereinafter “DOJ OIG Report, April 2004”].

<sup>46</sup> Paul Barrett, *Criminal Fifth Column*, WALL ST. J., Feb. 5, 2003, available at <http://www.frontpagemag.com/Articles/ReadArticle.asp?ID=5984>.

<sup>47</sup> U.S. Dep’t of Just., Off. of the Inspector Gen., *Office of the Inspector General (OIG) Analysis of Second Response by the Federal Bureau of Prisons to Recommendations in the OIG’s April 2004 Report on the Selection of Muslim Religious Services Providers*, prepared Oct. 26, 2004 (on file with the Senate Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary).

## HOMELAND SECURITY

### “Lone-Wolf” Fix

#### *“Lone-Wolf” Terrorists*

In the 108<sup>th</sup> Congress, the Subcommittee secured the enactment of numerous laws to bolster the security of the homeland. One of these laws is the “Lone-Wolf” fix to the Foreign Intelligence Surveillance Act (FISA).<sup>48</sup>

The case of suspected September 11 conspirator Zacarias Moussaoui is discussed extensively in the 9/11 Commission Report.<sup>49</sup> Moussaoui, an Al Qaeda operative, was arrested by Minneapolis FBI agents several weeks before the September 11 attacks. That summer, instructors at a Minnesota flight school became suspicious when Moussaoui, with little apparent knowledge of flying, asked to be taught to pilot a 747. The instructors contacted the Minneapolis office of the FBI, which immediately suspected that Moussaoui might be a terrorist. After the September 11 attacks, when FBI agents finally were allowed to search Moussaoui’s belongings, they discovered information that linked him to two of the actual September 11 hijackers, and to a high-level organizer of the attacks who was later arrested in Pakistan.<sup>50</sup>

The 9/11 Commissioners were right to ask whether more could have been done to pursue this case. Unfortunately, given the state of the law at the time, the answer to that question is probably no. In fact, given the state of the law until the end of 2004, the answer to the question still would have been no.

FBI agents were blocked from searching Moussaoui’s belongings because of an outdated requirement of the 1978 Foreign Intelligence Surveillance Act (FISA).<sup>51</sup> FISA sets rules for searches conducted for intelligence investigations. As the 9/11 Commission Report notes, the FBI field office was unable to obtain a FISA warrant for Moussaoui because it lacked information linking him to a known terror group.<sup>52</sup> As the Report states: Minneapolis agents sought a “special warrant under the Foreign Intelligence Surveillance Act to [search Moussaoui].

---

<sup>48</sup> Pub. L. No. 95-511 (Oct. 25, 1978).

<sup>49</sup> THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT, 108<sup>th</sup> Cong., 273-276 (2004).

<sup>50</sup> S. REP. NO. 108-40 (2003), at 3.

<sup>51</sup> Pub. L. No. 95-511 (Oct. 25, 1978).

<sup>52</sup> THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT, 108<sup>th</sup> Cong., 274 (2004).

To do so, however, the FBI needed to demonstrate probable cause that Moussaoui was an agent of a foreign power, a demonstration that [is] . . . a statutory requirement for a FISA warrant. The agent did not have sufficient information to connect Moussaoui to a foreign power.”<sup>53</sup> At the time, the law did not allow searches of apparent lone-wolf terrorists such as Zacarias Moussaoui — even if the FBI could show probable cause to believe that the person is involved in international terrorism.

It is inevitable that Islamist terrorists will try again to attack the United States. And as Chairman Kyl stated when he introduced legislation that includes a provision known as the “Lone-Wolf” fix or the “Moussaoui Fix,” “Imagine if another attack occurred — and another review commission found that critical FBI investigations again were undermined by the lack of FISA authority to monitor and search lone-wolf terrorists. We simply cannot let that happen. We must ensure that today’s FBI agents are not hampered by the same unnecessary barriers that hurt the efforts of the Minneapolis agents in August of 2001.”<sup>54</sup>

### *Changed World Requires a Change in FISA*

Requiring that targets of a FISA warrant be specifically linked to a foreign government or international terrorist organization may have made sense when FISA was enacted in 1978; in that year, the typical FISA target was a Soviet spy or a member of one of the hierarchical, military-style terror groups of that era. Today, however, the United States faces a much different threat. We are principally confronted not by specific groups or governments, but by a movement of Islamist extremists. This movement does not maintain a fixed structure or membership list, and its adherents do not always advertise their affiliation with this cause.

### *Islamist Terrorist Threat*

The origins and evolution of the Islamist terrorist threat, and the difficulties posed by FISA’s current framework, were described in detail by Spike Bowman, the Deputy General Counsel of the FBI, at a Senate Select Committee on Intelligence hearing.

When FISA was enacted, terrorism was very different from what we see today. In the 1970s, terrorism more often targeted individuals, often carefully selected. This was the usual pattern of the Japanese Red Army, the Red Brigades and similar organizations listed by name in the legislative history of FISA. Today we see terrorism far more lethal and far more indiscriminate than could have been imagined in 1978. It takes only the events of September 11, 2001, to fully comprehend the difference of a couple of decades. But there is another difference as well. Where we

---

<sup>53</sup> THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT, 108<sup>th</sup> Cong., 274 (2004).

<sup>54</sup> 150 CONG. REC. S10227 (daily ed. Oct. 1, 2004) (statement of Jon Kyl).

once saw terrorism formed solely around organized groups, today we often see individuals willing to commit indiscriminate acts of terror. It may be that these individuals are affiliated with groups we do not see, but it may be that they are simply radicals who desire to bring about destruction. . . .

[W]e are increasingly seeing terrorist suspects who appear to operate at a distance from these [terrorists] organizations. . . . [W]hat we see today are (1) agents of foreign powers in the traditional sense who are associated with some organization or discernible group (2) individuals who appear to have connections with multiple terrorist organizations but who do not appear to owe allegiance to any one of them, but rather owe allegiance to the International Jihad movement and (3) individuals who appear to be personally oriented toward terrorism but with whom there is no known connection to a foreign power.

This phenomenon, which we have seen . . . growing for the past two or three years, appears to stem from a social movement that began at some imprecise time, but certainly more than a decade ago. It is a global phenomenon which the FBI refers to as the International Jihad Movement. By way of background we believe we can see the contemporary development of this movement, and its focus on terrorism, rooted in the Soviet invasion of Afghanistan. . . .

The current FISA statute has served the nation well, but the International Jihad Movement demonstrates the need to consider whether a different formulation is needed to address the contemporary terrorist problem.<sup>55</sup>

When FISA was enacted in 1978, the Soviet invasion of Afghanistan had not yet occurred and both Iran and Iraq were considered allies of the United States. The world has changed — and, as the Attorney General testified in response to a question from Chairman Kyl, “single, lone-wolf terrorists act and can act in ways that are very, very damaging.”<sup>56</sup>

### *Development of a “Lone-Wolf” Fix*

---

<sup>55</sup> S. REP. NO. 108-40, at 4-5 (2003) (quoting statement of Spike Bowman, before a hearing of the Senate Select Comm. on Intelligence on the predecessor to S. 113).

<sup>56</sup> *The War Against Terrorism: Working Together to Protect America: Hearing Before the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 1<sup>st</sup> Sess. (Mar. 4, 2003) (S. Hrg. 108-137, Serial No. J-108-3) at 19 (statement of John Ashcroft) [hereinafter “Hearing of Mar. 4, 2003”].

It is the responsibility of Congress to adapt our laws to changed conditions, and to ensure that U.S. intelligence agents have at their disposal all of the tools that they need to combat the terrorist threat currently facing the United States. Chairman Kyl and Senator Schumer introduced S. 113 to update the Foreign Intelligence Surveillance Act of 1978 so that it permits surveillance of individual foreign visitors to the United States who appear to be involved in international terrorism, without regard to whether such persons are affiliated with a foreign government or terrorist group.<sup>57</sup>

In March 4, 2003, the Judiciary Committee held a hearing to examine critical changes in law-enforcement tools.<sup>58</sup> The witnesses were Attorney General Ashcroft, Homeland Security Secretary Ridge, and FBI Director Mueller. At the hearing, Director Mueller and Attorney General Ashcroft both expressed their support for S. 113.<sup>59</sup> In response to questions from Chairman Kyl, Director Mueller stated that the FBI has had difficulty obtaining sufficient information to permit surveillance of individuals who fit the lone-wolf profile.<sup>60</sup> He testified that S. 113 would allow the FBI to “overcome” some of these hurdles to tracking terrorists.<sup>61</sup> He added: “We have in our threat analyses and our summary of threats facing the United States identified the lone-wolf as an individual . . . we cannot dismiss and one that we would have to look out for, particularly when we know that Al Qaeda is a very loosely integrated organization, and quite often, you cannot, until sometime down the road, identify particular ties to that particular organization.”<sup>62</sup> Attorney General Ashcroft testified, “It’s a good bill. It’s what ought to be done.”

S. 113 was unanimously reported by the Judiciary Committee in March 2003, and was approved by the full Senate by a vote of 90 to 4 in May 2003.<sup>63</sup> A substantially identical provision was included in a House bill that was introduced by Chairman Sensenbrenner and former House Intelligence Committee Chairman Goss and was included in the House Intelligence Reform and Terrorism Prevention Act as Section 2001.<sup>64</sup> The “Moussaoui fix” was

---

<sup>57</sup> S. 113, 108<sup>th</sup> Cong. (2003).

<sup>58</sup> Hearing of Mar. 4, 2003. The “Moussaoui Fix” also has been the subject of two hearings — one in the Senate Intelligence Committee on July 31, 2002, and one in the House Crime Subcommittee on May 18, 2004.

<sup>59</sup> Hearing of Mar. 4, 2003, at 19 (statements of John Ashcroft and Robert Mueller).

<sup>60</sup> Hearing of Mar. 4, 2003, at 19 (statement of Robert Mueller).

<sup>61</sup> Hearing of Mar. 4, 2003, at 19 (statement of Robert Mueller).

<sup>62</sup> Hearing of Mar. 4, 2003, at 19 (statement of Robert Mueller).

<sup>63</sup> 150 CONG. REC. S5928 (daily ed. May 8, 2003).

<sup>64</sup> Hearing of Mar. 4, 2003, at 19 (statement of John Ashcroft).

finally enacted in December 2004 as Section 6001 of the Intelligence Reform and Terrorism Prevention Act.<sup>65</sup>

## **Pretrial Detention of Terrorists**

### *Filling Gaps in the Law*

In the aftermath of September 11, Congress passed several key pieces of legislation to improve homeland security, to give law enforcement a greater capacity to investigate potential terrorists, and to increase border security. At numerous hearings, the Subcommittee sought to find answers to some of the following questions: Are the new laws working? Are there things we left out? Are there improvements we should make? And most importantly, what progress is being made by the administration in implementing these new measures?

As part of the Subcommittee's effort to fill some of the gaps in the law, Chairman Kyl introduced the Pretrial Detention and Lifetime Supervision of Terrorists Act of 2003 (S. 1606).<sup>66</sup> The bill was, in part, a result of a 2002 Subcommittee hearing that reviewed the tools available to law-enforcement officers.<sup>67</sup>

### *Pretrial Detention*

Under federal law, there is a presumption in favor of denying bail to defendants accused of certain crimes, such as drug crimes that carry a potential sentence of 10 years or more. The Subcommittee noted, however, that at the time presumptive detention did not apply to terrorist activity. S. 1606 aimed to fix this oversight by amending the criminal code to presumptively deny pre-trial release to persons charged with acts of terrorism. The presumption would apply to federal crimes of terrorism, as enumerated in the criminal code, if the Attorney General certifies that the offense, by its nature and context, appears to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by an act of mass destruction, assassination, or kidnapping, or an offense involved in or related to domestic or international terrorism.

---

<sup>65</sup> Pub. L. No. 108-458.

<sup>66</sup> S. 1606, 108<sup>th</sup> Cong. (2003); *see also* 149 CONG. REC. S11353 (daily ed. Sept. 10, 2003) (statement of Jon Kyl).

<sup>67</sup> *Tools Against Terror: How the Administration is Implementing New Laws in the Fight to Protect Our Homeland: Hearing Before the Senate Comm. on the Judiciary*, 107<sup>th</sup> Cong., 1<sup>st</sup> Sess. (Oct. 9, 2002) (S. Hrg. 107-1043, Serial No. J-107-110) [hereinafter "Hearing of Mar. 4, 2003"].

This expansion is justified by the unparalleled magnitude of the threat posed to our nation by acts of terrorism. While drug crimes are serious, terrorists pose at least as much of a threat as drug dealers, and therefore, should be subject to the same presumption of pre-trial detention.

### *Post-Release Supervision*

S. 1606 would also broaden the list of offenses that render a convicted terrorist eligible for lifetime supervision after his release from prison. Current law allows lifetime post-release supervision for terrorist offenses only if they result in or create a foreseeable risk of death or serious injury.<sup>68</sup> This limitation could prevent the imposition of adequate supervision periods for persons convicted of non-violent terrorist offenses, such as a computer attack on the United States that results in tens of billions of dollars of economic damage.

Current law also limits supervision of persons who provide essential financial or other material support for terrorist acts, but who are not directly engaged in violent terrorist acts.<sup>69</sup> The continuing danger to our nation's security posed by such persons may be no less than that posed by the direct perpetrators of terrorist violence. The courts should have the same degree of discretion in prescribing post-release supervision for these terrorists as for others.

For this reason, S.1606 eliminates the foreseeable-risk-of-injury requirement and allows lifetime supervision for those convicted of all offenses in the standard list of crimes likely to be committed by terrorist felons and their supporters. This reform reflects the continuing danger posed by terrorists after the completion of their term of imprisonment. It recognizes that even those terrorists not directly involved in the use of violence may continue to harbor a commitment to terrorist goals and methods that will not dissipate within a few years of release from prison.

The pretrial detention provision of S. 1606 was enacted into law in December 2004 as Section 6952 of the Intelligence Reform and Terrorism Prevention Act.<sup>70</sup> In the 109<sup>th</sup> Congress, the Subcommittee will work to pass the remaining lifetime post-release supervision provisions of S. 1606.

### **Tools to Fight Terrorism Act**

---

<sup>68</sup> Pub. L. No. 98-473, *as amended* (Oct. 12, 1984).

<sup>69</sup> Pub. L. No. 98-473, *as amended* (Oct. 12, 1984).

<sup>70</sup> Pub. L. No. 108-458.

### *A Three-Year Gap in Anti-Terror Legislation*

Since September 11, congressional committees and executive agencies have conducted extensive reviews and investigations to uncover gaps in the nation's anti-terrorism safety net. Both the House and Senate Judiciary Committees have held numerous hearings. The Joint Intelligence Committee, the 9/11 Commission, and the Justice Department have all conducted evaluations of the nation's anti-terrorism capabilities.

These hearings and investigations have, as Chairman Kyl pointed out, “uncovered numerous flaws and gaps in our anti-terrorism system”<sup>71</sup> — flaws and gaps that urgently need to be addressed. Recent events indicate that the United States and its allies remain the targets of terrorists. Large quantities of chemicals used to make bombs were seized near London's Heathrow Airport; a car bomb in Riyadh killed five and wounded 147 others; Osama bin Laden's second in command, Ayman Al Zawahiri, rallied supporters for the third year in a row preceding the anniversary of September 11; and, of course, there are the tragic bombings in Madrid and Baghdad to remind the world that terrorists are intent on continuing their indiscriminate attacks on innocent people.<sup>72</sup>

Yet, as Chairman Kyl has pointed out, “It would undoubtedly surprise most Americans to know that despite countless congressional hearings, no major anti-terror legislation has been passed into law since President Bush signed the USA Patriot Act<sup>73</sup> on October 26, 2001 — six weeks after the fall of the Twin Towers in New York,”<sup>74</sup> the attack on the Pentagon, and the downing of Flight 93 in Pennsylvania.

### *Knitting Together Years of Legislation*

As a result of this legislative gap, the Subcommittee held a hearing on September 13, 2004 to review ongoing legislative efforts to strengthen law enforcement's ability to fight terrorism.<sup>75</sup> The witnesses at the hearing were Assistant Attorney General Daniel J. Bryant;

---

<sup>71</sup> *A Review of the Tools to Fight Terrorism Act: A Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (Sept. 13, 2004), at 2 (transcript) (statement of Jon Kyl) [hereinafter “Hearing of Sept. 13, 2004”].

<sup>72</sup> Hearing of Sept. 13, 2004, at 20 (transcript) (statement of Barry Sabin).

<sup>73</sup> For a more detailed discussion of the USA Patriot Act, see Dep't of Just., *Dispelling the Myths*, at [http://www.lifeandliberty.gov/subs/u\\_myths.htm](http://www.lifeandliberty.gov/subs/u_myths.htm) (last visited Oct. 19, 2004). For a description of how the Department of Justice is employing the Patriot Act, see U.S. Dep't of Just., *Report from the Field: The USA Patriot Act at Work*, July 2004.

<sup>74</sup> *Giving Law Enforcement Some Overdue Tools in the Fight Against Terrorism*, Senator Kyl's WKLY. COLUMN (Sept. 20, 2004), at <http://kyl.senate.gov/record.cfm?id=226389>.

<sup>75</sup> Hearing of Sept. 13, 2004.

Barry Sabin, Chief of the Counterterrorism Section of the Criminal Division at the Department of Justice; and Professor Jonathan Turley, the Shapiro Professor of Public Interest Law at the George Washington University Law School.

The Subcommittee focused on S. 2679, the Tools to Fight Terrorism Act (TFTA),<sup>76</sup> introduced by Chairman Kyl along with several other Members of the Subcommittee and the Senate Leadership. TFTA is composed of 11 bills that were pending in the House or Senate. Every provision had either been introduced previously as a bill in the House or Senate or had had a committee hearing. Also, every provision was fully supported by the Justice Department. Collectively, the provisions of TFTA had been the subject of nine separate hearings before House and Senate committees and had been the subject of four separate committee reports.<sup>77</sup> As of September 13, 2004 (the date of the hearing), the bills included in TFTA collectively had been pending before Congress for 14 years, seven months, and nine days.<sup>78</sup>

At the hearing, Assistant Attorney General Bryant stated that the bill was necessary to fill gaps in existing law<sup>79</sup> and further added that it is “critical to enact this common-sense reform.”<sup>80</sup> He stressed that the bill “contains significant, effective, constitutionally-sound tools that would help us prevent, disrupt and prosecute terrorism.”<sup>81</sup> Counterterrorism Chief Barry Sabin agreed wholeheartedly, stating that “if passed, [TFTA] would fill a number of holes in our homeland security blanket.”<sup>82</sup> Referring to the agreement between civil liberties advocates and national security advocates concerning TFTA, Professor Turley of George Washington University joked that the Visigoths and the Romans had finally found common ground.<sup>83</sup>

Among other things, the bill would:

- Allow FBI agents to seek warrants for surveillance of suspected “lone-wolf” terrorists, such as the alleged 20<sup>th</sup> hijacker Zacarias Moussaoui;

---

<sup>76</sup> S. 2679, 108<sup>th</sup> Cong. (2004); For a description of each section, see Appendix D.

<sup>77</sup> Hearing of Sept. 13, 2004, at 4 (transcript) (statement of Jon Kyl).

<sup>78</sup> Hearing of Sept. 13, 2004, at 4 (transcript) (statement of Jon Kyl).

<sup>79</sup> Hearing of Sept. 13, 2004, at 15 (transcript) (statement of Daniel Bryant).

<sup>80</sup> Hearing of Sept. 13, 2004, at 19 (transcript) (statement of Daniel Bryant).

<sup>81</sup> Hearing of Sept. 13, 2004, at 14 (transcript) (statement of Daniel Bryant).

<sup>82</sup> Hearing of Sept. 13, 2004, at 19 (transcript) (statement of Barry Sabin).

<sup>83</sup> Hearing of Sept. 13, 2004, at 27-28 (transcript) (statement of Jonathan Turley).

- Grant the FBI administrative subpoena power when investigating terrorism offenses, just as DEA agents can issue subpoenas when enforcing the Controlled Substances Act;
- Improve information-sharing among federal, state, and local authorities, avoiding the barriers between criminal and intelligence investigation that impeded pre-September 11 searches in the United States for Al Qaeda hijackers Khalid al-Midhar and Nawaf al-Hazmi;
- Punish hoaxes about terrorist crimes or about the death of a U.S. soldier by imposing penalties commensurate with disruptions and trauma inflicted by such hoaxes;
- Impose stiff mandatory-minimum penalties for possession of Man-Portable Air Defense systems (MANPADS); atomic weapons; radiological dispersal devices (“dirty bombs”); and the variola virus, which causes smallpox; and
- Create a set of criminal offenses tailored to the unique challenges of guaranteeing the security of our nation’s seaports.

#### *Prevention of Terrorist Access to Special Weapons*

The Assistant Attorney General commented on several key provisions of TFTA in his testimony. He discussed the dangers posed by Man-Portable Air Defense systems (MANPADS); atomic weapons; radiological dispersal devices (dirty bombs); and the variola virus which causes smallpox.<sup>84</sup> He testified that MANPADS are portable, easy to conceal, lightweight weapons that can kill hundreds of people in a single attack.<sup>85</sup> Atomic weapons and “dirty bombs” can inflict enormous casualties, as well as damage property and the environment. Finally, the variola virus has been classified by the Centers of Disease Control as “one of the biological agents posing the greatest potential threat to public health.”<sup>86</sup>

These weapons have no legitimate private use.<sup>87</sup> And while they have the capability to inflict unmeasurable death and destruction, the current penalties for unlawful possession of such weapons are inadequate. The maximum penalty for possession of MANPADS and atomic weapons is only 10 years.<sup>88</sup> In addition, Assistant Attorney General Bryant stated that “there is

---

<sup>84</sup> Hearing of Sept. 13, 2004, at 15 (transcript) (statement of Daniel Bryant).

<sup>85</sup> Hearing of Sept. 13, 2004, at 15 (transcript) (statement of Daniel Bryant).

<sup>86</sup> Hearing of Sept. 13, 2004, at 15 (transcript) (statement of Daniel Bryant).

<sup>87</sup> Hearing of Sept. 13, 2004, at 15-16 (transcript) (statement of Daniel Bryant).

<sup>88</sup> Hearing of Sept. 13, 2004, at 16 (transcript) (statement of Jon Kyl).

no statute that criminalizes the mere possession of [dirty bombs]” or the mere possession of nuclear materials.<sup>89</sup>

TFTA would change this by establishing and enforcing “a zero tolerance policy toward the unlawful importation, possession or transfer of these weapons by imposing very tough criminal penalties.”<sup>90</sup> Specifically, the bill would require imprisonment of 30 years to life for possession of these weapons. Use, attempted use, threats to use, or conspiracy to use would result in a mandatory life sentence. If the possession or use of these weapons results in death, capital punishment becomes a possible penalty.

In his testimony about these provisions before the Subcommittee, Professor Turley stated that Section 426, the WMD-statute provision, “would close current loopholes in the interest of national security and does not materially affect civil liberty interests.”<sup>91</sup> He also said “the obvious value of such a law would be hard to overstate.”<sup>92</sup>

A version of these provisions was enacted into law at the end of the 108<sup>th</sup> Congress as Section 6001 of the Intelligence Reform and Terrorism Prevention Act.<sup>93</sup>

#### *Providing Material Support and Receiving Military Training From Terrorists*

Counterterrorism Chief Sabin testified that the development of tools addressing material support for terrorism and terrorist financing is “critical to our daily counterterrorism efforts.”<sup>94</sup> The Anti-Terrorism and Effective Death Penalty Act of 1996 criminalized conduct several steps removed from a terrorist attack, including providing material support to terrorists and terrorist organizations. Several court decisions have, however, found the statute to be “unconstitutionally vague.”<sup>95</sup>

---

<sup>89</sup> Hearing of Sept. 13, 2004, at 16 (transcript) (statement of Jon Kyl).

<sup>90</sup> Hearing of Sept. 13, 2004, at 17 (transcript) (statement of Daniel Bryant).

<sup>91</sup> Hearing of Sept. 13, 2004, at 9 (written statement of Jonathan Turley).

<sup>92</sup> Hearing of Sept. 13, 2004, at 9 (written statement of Jonathan Turley).

<sup>93</sup> Pub. L. No. 108-458.

<sup>94</sup> Hearing of Sept. 13, 2004, at 20 (transcript) (statement of Barry Sabin).

<sup>95</sup> Hearing of Sept. 13, 2004, at 23 (transcript) (statement of Barry Sabin).

According to Mr. Sabin, TFTA remedies this vagueness while maintaining the statute's effectiveness.<sup>96</sup> The bill broadens the jurisdictional bases of the material support statute and more clearly defines the terms "training" and "expert advice or assistance" in order to avoid a perceived overreach. Professor Turley testified, "[TFTA] moves [the material support statute] out of one constitutional area of concern; that is, void for vagueness. I would think that that would be embraced by civil liberties advocates."<sup>97</sup> And even if such advocates did still object, Professor Turley noted that "the Government does have a legitimate interest in prosecuting people giving material support to terrorist organizations . . . I believe that this is an advance. It makes this statute better and brings it closer to conformity with the Constitution. Quite frankly, I believe this entire law would be upheld under even First Amendment and due process challenges as it stands."<sup>98</sup>

TFTA would also make it a crime to receive military-type training from a foreign terrorist group and would make aliens who have received such training inadmissible to and deportable from the United States. The need for a stronger material support statute was the subject of a hearing before the Senate Judiciary Committee on May 5, 2004.<sup>99</sup> The current prohibition on providing material support does not clearly prohibit receiving training from a terrorist organization; it only prohibits providing the training. But, as Mr. Sabin testified, "it is clear that persons who attend training camps violate the existing material support statutes by providing training to other trainees serving under the direction of the organization and performing guard duty or other tasks, providing money to the organization for the training, or for uniforms and provisions and the like."<sup>100</sup> It is difficult, however, to prove that these activities occurred, especially when the training occurs in a remote location. According to Mr. Sabin, TFTA could fill the gap by simply making it an offense to receive military-type training.<sup>101</sup> Professor Turley opined on the constitutionality of this provision: "I also agree . . . that Section 115 achieves an important purpose in making it a crime to receive military-type training from a

---

<sup>96</sup> Hearing of Sept. 13, 2004, at 23 (transcript) (statement of Barry Sabin). This view was affirmed by James B. Comey, Deputy Attorney General, in his testimony before the Senate Judiciary Committee on Sept. 22, 2004. He stated, "[TFTA] would, among other things, improve existing law by clarifying several aspects of the material support statutes." *A Review of Counter-Terrorism Legislation and Proposals: A Hearing Before the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 2<sup>nd</sup> Sess., at 9 (Sept. 22, 2004) (written statement of James Comey) [Hereinafter "Hearing of Sept. 22, 2004"].

<sup>97</sup> Hearing of Sept. 13, 2004, at 35 (transcript) (statement of Jonathan Turley).

<sup>98</sup> Hearing of Sept. 13, 2004, at 35-36 (transcript) (statement of Jonathan Turley).

<sup>99</sup> *Oversight Hearing: Aiding Terrorists — An Examination of the Material Support Statute: A Hearing Before the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (May 5, 2004) [hereinafter "Hearing of May 5, 2004"].

<sup>100</sup> Hearing of Sept. 13, 2004, at 25 (transcript) (statement of Barry Sabin).

<sup>101</sup> Hearing of Sept. 13, 2004, at 25 (transcript) (statement of Barry Sabin).

foreign terrorist organization. We have seen in recent years, particularly in cases like that of Jose Padilla, that these training camps are used to recruit and indoctrinate individuals.”<sup>102</sup>

The above-discussed provisions — Sections 114 and 115 of TFTA — were enacted into law as Sections 6602, 6603, and 5402 of the Intelligence Reform and Terrorism Prevention Act.<sup>103</sup>

### *Improving TFTA So It Will Pass Constitutional Muster*

Professor Turley recommended one change to a part of the bill in order to better protect civil liberties. He recommended that, if the FBI is given subpoena authority for terrorism investigations, it also be required to report on the use of that authority. Chairman Kyl later filed TFTA as an amendment (S.A. 3724)<sup>104</sup> to the Intelligence Reform and Terrorism Prevention Act (S. 2845)<sup>105</sup> on October 1, 2004. The amendment incorporated Professor Turley’s recommendation. The revised provision would require the FBI to report to Congress on the number of subpoenas that it issues pursuant to this new authority, and the circumstances under which those subpoenas are issued.<sup>106</sup>

In addition to the provisions described above, the following sections of TFTA were enacted into law as part of the Intelligence Reform and Terrorism Prevention Act:

1. TFTA Sec. 106 (IRTPA Sec. 6702): *Terrorist and Military Hoaxes*. This provision makes it a federal offense to perpetrate hoaxes concerning certain terrorist crimes or the deaths of U.S. soldiers in a war zone.
2. TFTA Sec. 107 (IRTPA Sec. 6703): *Increased Penalties for Obstruction of Justice*. This provision increases from 5 years to 8 years the penalty for obstruction of justice or making false statements in a terrorism investigation.
3. TFTA Sec. 113 (IRTPA Sec. 6501): *Grand-Jury Information Sharing*. This provision authorizes sharing of federal grand-jury information with state and local

---

<sup>102</sup> Hearing of Sept. 13, 2004, at 30 (transcript) (statement of Jonathan Turley).

<sup>103</sup> Pub. L. No. 108-458.

<sup>104</sup> S.A. 3724, 108<sup>th</sup> Cong. (2004).

<sup>105</sup> Pub. L. No. 108-458 (Dec. 17, 2004).

<sup>106</sup> 150 CONG. REC. S10227 (daily ed. Oct. 1, 2004) (statement of Jon Kyl).

governments. This provision also had been introduced in the Senate as part of S. 2599,<sup>107</sup> a Chambliss/Kyl bill, on June 24, 2004.

4. TFTA Sec. 116 (IRTPA Sec. 6802). *WMD Offenses*. This provision expands the jurisdictional bases and scope of existing prohibitions on use of weapons of mass destruction, and includes chemical weapons within the prohibition for the first time.

5. TFTA Sec. 117 (IRTPA Sec. 6803). *WMD Proliferation*. This section amends the Atomic Energy Act to more broadly prohibit participation in the development or production of any nuclear weapon outside of the United States, and also makes it a crime to participate in or provide material support to a WMD program of a terrorist organization or state sponsor of terrorism.

6. TFTA Sec. 506 (IRTPA Sec. 6604): *Concealment of Terrorist Financing*. This section amends current law to prohibit the concealment of financial support while knowing that it has been or will be provided to terrorists.

## **Crime Victims' Rights**

### *Passing the Crime Victims' Rights Act*

The Oklahoma City bombing was one of the worst acts of domestic terrorism in American history: the bombing of the Alfred P. Murrah Federal Building in Oklahoma City killed 168 people and injured more than 500 others.<sup>108</sup> On September 30, 2004, Chairman Kyl proposed an amendment to the Intelligence Reform and Terrorism Prevention Act (S. 2845)<sup>109</sup> — a bill implementing many of the 9/11 Commission recommendations. Chairman Kyl's amendment (S.A. 3881) would grant victims of terrorism certain rights, allowing for their notification and participation in the criminal justice process.<sup>110</sup> The amendment to the IRTPA was not accepted.

---

<sup>107</sup> S. 2599, 108<sup>th</sup> Cong. (2004).

<sup>108</sup> Lois Romano & Tom Kenworthy, *McVeigh Guilty on All 11 Counts*, WASH. POST, June 3, 1997, at A01.

<sup>109</sup> Pub. L. No. 108-458 (Dec. 17, 2004).

<sup>110</sup> S.A. 3881, 108<sup>th</sup> Cong. (2004).

On the same day that Chairman Kyl proposed the amendment for victims of terrorism, the House Judiciary Committee passed the Justice For All Act (H.R. 5107),<sup>111</sup> which included a version of the Kyl-Feinstein crime victims' act, S. 2329.<sup>112</sup> The full House passed the Justice For All Act without any changes. The Senate passed the bill after lengthy negotiations, resulting in a number of alterations to the crime victims' language. Finally, on October 20, 2004, the Justice For All Act of 2004 was presented to the President for his signature, and, on October 30, it was signed into law.<sup>113</sup> Victims of terrorism and of all crimes victims finally acquired desperately need rights.

The Justice for All Act grants the victims of federal crimes the following rights:

- (1) The right to be reasonably protected from the accused.
- (2) The right to reasonable, accurate, and timely notice of any public proceeding involving the crime or of any release or escape of the accused.
- (3) The right not to be excluded from any such public proceeding.
- (4) The right to be reasonably heard at any public proceeding involving release, plea, or sentencing.
- (5) The right to confer with the attorney for the government in the case.
- (6) The right to full and timely restitution as provided in law.
- (7) The right to proceedings free from unreasonable delay.
- (8) The right to be treated with fairness and with respect for the victim's dignity and privacy.

Federal law-enforcement officials are required to make their "best efforts to see that crime victims are notified of, and accorded" these rights.

In addition, the legislation contains provisions to ensure compliance with these new requirements: The Attorney General shall issue regulations to enforce these victims' rights in federal criminal cases, regulations that shall include proper Justice Department oversight, training, and disciplinary systems to ensure that the rights are being enforced. In addition, the Administrative Office of the United States Courts shall provide annual reports on how these

---

<sup>111</sup> H.R. 5107, 108<sup>th</sup> Cong. (2004).

<sup>112</sup> S. 2329, 108<sup>th</sup> Cong. (2004).

<sup>113</sup> Pub. L. No. 108-405 (Oct. 30, 2004).

statutory rights are being asserted and respected in the nation's federal courts. Finally, the General Accounting Office<sup>114</sup> shall conduct an independent progress report due three years from the enactment of this legislation.

## TECHNOLOGICAL SECURITY

### Document Security and Identity Theft

#### *Identity Theft: A "Key Catalyst" for Terrorist Groups*

One area of concern to the Subcommittee is document security and terrorist use of identity theft. For both Senator Feinstein and Chairman Kyl, combating identity theft has been a "top priority."<sup>115</sup> Senator Feinstein has explained the magnitude of the threat: "We know that the average loss of an identity theft is now about \$17,000. We know that fraud losses at individual financial institutions are running well over \$1 billion annually. And, on an average, it takes a full year and a half for someone who has had their identity stolen to regain it."<sup>116</sup> The Department of Justice reports that nearly 10 million Americans had their identities stolen in 2003.<sup>117</sup> Identity theft costs businesses "nearly \$50 billion a year in fraudulent transactions and often involves coordinated criminal conduct."<sup>118</sup>

---

<sup>114</sup> Now the Government Accountability Office.

<sup>115</sup> *Identity Theft Penalty Enhancement Act of 2002: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (July 9, 2002) (S. Hrg. 107-900, Serial No. J-107-68), at 81 (statement of Dianne Feinstein) [hereinafter "Hearing of July 9, 2002"]. On his website, Chairman Kyl has posted information concerning identity theft. See Appendix B.

<sup>116</sup> Hearing of July 9, 2002, at 82 (statement of Dianne Feinstein).

<sup>117</sup> Attorney General John Ashcroft, Remarks at the Department of Justice (Aug. 26, 2004), at <http://www.usdoj.gov/ag/speeches/2004/82604ag.htm>.

<sup>118</sup> Attorney General John Ashcroft, Remarks at the Department of Justice (Aug. 26, 2004), at <http://www.usdoj.gov/ag/speeches/2004/82604ag.htm>.

Since 1998, the Subcommittee has held seven hearings on identity theft and fraud.<sup>119</sup> During a Subcommittee hearing in 2002, Dennis Lormel, Chief of the FBI's Terrorist Financial Review Group, testified that identity theft was a "key catalyst" for terrorist groups.<sup>120</sup> He said that identity theft posed an "alarming" threat and that "terrorists have long utilized identity theft as well as Social Security Number fraud to enable them to obtain . . . cover employment and access to secure locations."<sup>121</sup>

### *GAO Report Finds Vulnerabilities*

Confirming Mr. Lormel's testimony, the General Accounting Office (GAO)<sup>122</sup> concluded an investigation in September 2003 and found significant security vulnerabilities in eight states. The GAO tested the ease with which driver's licenses (the primary form of identification used by U.S. citizens in order to board airplanes and open bank accounts) could be obtained by terrorists and other criminals.<sup>123</sup> Separate investigations revealed that terrorists could easily use fraudulent documents to obtain Social Security numbers or enter federal buildings without challenge.<sup>124</sup>

The GAO investigation reviewed the procedures of motor vehicle offices in eight states, including Chairman Kyl's home state of Arizona, between July 2002 and May 2003.

---

<sup>119</sup> Hearing of July 9, 2002; *Identity Theft: Restoring Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (Mar. 20, 2002) (S. Hrg. 107-900, Serial No. J-107-68); *Privacy, Identity Theft, and the Protection of Your Personal Information in the 21<sup>st</sup> Century: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (Feb. 14, 2002) (S. Hrg. 107-852, Serial No. J-107-60); *Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107<sup>th</sup> Cong., 1<sup>st</sup> Sess. (Nov. 14, 2001) (S. Hrg. 107-657, Serial No. J-107-46A); *Identity Theft: How to Protect and Restore Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 106<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (July 12, 2000) (S. Hrg. 106-902, Serial No. J-106-97); *ID Theft: When Bad Things Happen to Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 106<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (Mar. 7, 2000) (S. Hrg. 106-885, Serial No. J-106-70); *The Identity Theft and Assumption Deterrence Act: S. 512: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 105<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (May 20, 1998) (S. Hrg. 105-845, Serial No. J-105-104).

<sup>120</sup> Hearing of July 9, 2002, at 89 (written statement of Dennis Lormel).

<sup>121</sup> Hearing of July 9, 2002, at 89-90 (written statement of Dennis Lormel).

<sup>122</sup> Now the Government Accountability Office.

<sup>123</sup> GAO Report, *Soc. Sec. Numbers: Improved SSN Verification & Exchange of States' Driver Records Would Enhance Identity Verification*, GAO-03-920, at 3 (Sept. 2003).

<sup>124</sup> *The Alias Among Us: Homeland Security and Terrorism Threat from Document Fraud, Identity Theft and Social Security Number Misuse: Hearing Before the Senate Comm. on Finance*, 108<sup>th</sup> Cong., 1<sup>st</sup> Sess. (Sept. 9, 2003) (S. Hrg. 108-388), at 3-4 (transcript) (written statement of John Pistole) [hereinafter "Hearing of Sept. 9, 2003"].

Undercover agents attempted to apply for driver's licenses using fictitious names, counterfeit documents, and counterfeit out-of-state driver's licenses. The agents did provide valid Social Security numbers. The GAO found that, in every case, motor vehicle employees failed to identify any of the documents as fraudulent. While some employees noted irregularities in the false documents, all were eventually returned to the GAO agents and driver's licenses were granted.

The GAO also used fraudulent documents to obtain valid Social Security numbers by mail and by posing as parents of newborn children, using fraudulent birth certificates. Fraudulent documents were also used to infiltrate federal buildings in Atlanta and to enter the United States from Jamaica, Barbados, Mexico, and Canada. None of the tested officials recognized the fraudulent nature of the documents presented to them.

### *Key Methods for Terrorist Infiltration*

It is clear from the GAO's report that terrorists and other dangerous criminals can pass as U.S. citizens or steal American identities with alarming ease. Robert Cramer, the Managing Director of the GAO, who oversaw the investigations, testified, "The weaknesses we found during these investigations clearly show that border inspectors, motor vehicle departments, and firearms dealers need to have the means to verify identity and to determine whether out-of-state driver's licenses presented to them are authentic."<sup>125</sup>

John Pistole, Acting Assistant Director of the FBI's Counterterrorism Division, said that terrorists have long committed identity theft and misused Social Security numbers to infiltrate the United States.<sup>126</sup> Social Security number fraud has enabled them "to obtain such things as cover employment and access to secure locations."<sup>127</sup> Once Social Security numbers and driver's licenses are obtained, bank and credit-card accounts, through which terrorism financing is facilitated, are easily accessed.<sup>128</sup>

Chairman Kyl said that the GAO's investigation "shows a dangerous lapse in the ability of state and federal employees to detect and deter document fraud, which is often the first step terrorists must take to assimilate themselves in the United States and form sleeper cells."<sup>129</sup>

---

<sup>125</sup> Hearing of Sept. 9, 2003, at 3-4 (written statement of Robert Cramer).

<sup>126</sup> Hearing of Sept. 9, 2003, at 3 (written statement of John Pistole).

<sup>127</sup> Hearing of Sept. 9, 2003, at 3 (written statement of John Pistole).

<sup>128</sup> Hearing of Sept. 9, 2003, at 3 (written statement of John Pistole).

<sup>129</sup> Sergio Bustos, *Investigators Expose Lax Security at Driver's License Offices*, GANNETT NEWS SERV., Sept. 9, 2003, available at 2003 WL 5603090.

### *Identity Theft Penalty Enhancement Act*

In response to the growing threat of identity theft, Senators Feinstein and Kyl introduced the Identity Theft Penalty Enhancement Act (S. 153)<sup>130</sup> at the request of the Attorney General and the Bush administration.<sup>131</sup> Senator Feinstein stressed the importance of the bill: “Unfortunately, because of the proliferation of identity theft and its use in other crimes, some extraordinarily serious, the enhancement penalties have become, I think, necessary and important.”<sup>132</sup> The Senate and House passed the bill by unanimous consent and the President has signed it into law.<sup>133</sup>

The Identity Theft Penalty Enhancement Act provides law-enforcement officers with the tools necessary both to prevent identity theft when possible and to vigorously prosecute the crime when deterrence fails. The Act implements four major changes:

- It establishes mandatory penalty enhancements for identity theft crimes in connection with serious federal offenses, including terrorism;
- It prohibits judges from allowing the penalty enhancement to run concurrently with the underlying sentence;
- It adds Social Security fraud and theft embezzlement by a bank officer to the list of crimes eligible for enhanced penalties; and
- It criminalizes possession of stolen or fraudulent identification with intent to commit an unlawful act.

The act also strengthens the ability of law enforcement to prosecute anyone who possesses stolen documents. (Prior to enactment of the bill, federal law prohibited the transfer and use of stolen documents, but not mere possession.)

### *Mandatory Penalty Enhancements*

Mandatory penalty enhancements will increase the deterrent effect of identity-theft laws for thieves who steal an identity in order to commit another crime. As Senator Feinstein pointed out at a Subcommittee hearing, identity theft is often a precursor to other crimes.<sup>134</sup> For

---

<sup>130</sup> S. 153, 108<sup>th</sup> Cong. (2003); *see also* H.R. 1731, 108<sup>th</sup> Cong. (2003).

<sup>131</sup> Hearing of July 9, 2002, at 81 (statement of Dianne Feinstein).

<sup>132</sup> Hearing of July 9, 2002, at 81 (statement of Dianne Feinstein).

<sup>133</sup> Pub. L. No. 108-275 (July 15, 2004); 150 CONG. REC. S7527 (daily ed. June 24, 2004).

<sup>134</sup> Hearing of July 9, 2002, at 81 (statement of Dianne Feinstein).

example, on October 15, 2003, Mohamed Amry, a former employee of Bally's Health Club, admitted transmitting the names, credit-card information, and Social Security numbers of at least 30 people to Abdelgnani Meskini. Meskini pled guilty to conspiracy in connection with a plot to blow up the Los Angeles International Airport in 1999.<sup>135</sup> Despite Amry's knowledge of Meskini's terrorist connections, Amry was only sentenced to 15 months imprisonment.<sup>136</sup> Under the Identity Theft Penalty Enhancement Act, Amry would receive a mandatory five year prison term, in addition to the 15 months, for knowingly transferring stolen identity information to an individual planning a terrorist attack.<sup>137</sup>

In addition to the five year mandatory penalty enhancement for commission of an identity-theft crime in connection with an act of terrorism, the Act also provides a two year mandatory penalty enhancement for identity-theft crimes in connection with serious federal predicate offenses.<sup>138</sup> These include immigration violations, false citizenship offenses, firearms offenses, and other serious crimes.

### *Removal of Judicial Discretion*

Before the Identity Theft Penalty Enhancement Act became law, judges had the discretion to allow enhanced penalties, such as those proposed in the Identity Theft Penalty Enhancement Act, to run concurrently with the underlying sentence. This allowed a convict to serve multiple penalties at the same time, and decreased the deterrence value of enhanced penalties. The Identity Theft Penalty Enhancement Act expressly prohibits judges from ordering the enhanced sentence to run concurrently with the underlying sentence.<sup>139</sup> This change will help guarantee that individuals convicted of identity theft crimes in connection with other offenses — especially terrorism — receive and serve long prison terms.

### *Bank Officers and Social Security Fraud*

Social Security fraud and theft embezzlement by a bank officer are often difficult crimes to prosecute. In most cases, the perpetrator commits many small crimes, each involving less than \$1000, the threshold for a felony. District courts are currently split on whether related crimes may be aggregated to reach the felony minimum. As a result, in districts that do not allow aggregation, the crimes are often either not prosecuted at all or pled out with the guilty party receiving only probation. The Identity Theft Penalty Enhancement Act clarifies the law to

---

<sup>135</sup> *U.S. v. Amry*, 2003 WL 124678 (S.D.N.Y. Jan. 16, 2003).

<sup>136</sup> Associated Press, *Man Charged with Identity Theft in Millennium Terror Plot* (Jan. 31, 2002) (available at LEXIS, Nexis library, AP file).

<sup>137</sup> Pub. L. No. 108-275 § 2(a)(2) (July 15, 2004).

<sup>138</sup> Pub. L. No. 108-275 § 2(a)(1) (July 15, 2004).

<sup>139</sup> Pub. L. No. 108-275 § 2(b)(2) (July 15, 2004).

allow aggregation of stolen funds in all related cases for the purpose of reaching the felony minimum.<sup>140</sup>

### *New Tools for Prevention*

Prior law only prohibited the knowing use or transfer, without legal authority, of another person's means of identification.<sup>141</sup> This meant that prior law only addressed those situations in which a defendant could be shown to have obtained someone else's identification and actually put that identification to use, or to have transferred it to another person or location where it could be put to use. Therefore, even when it could be shown that an individual intended to use (but did not use) the fraudulent or stolen identification in the commission of another crime, the authorities were prevented from prosecuting.

The Identity Theft Penalty Enhancement Act addresses this problem by criminalizing the possession of fraudulent or stolen identification when the possessor intends to use the identification in the commission of another crime.<sup>142</sup>

### *Making Full Use of the Identity Theft Penalty Enhancement Act*

Within a month of the bill's enactment into law, the Justice Department began to vigorously use the Identity Theft Penalty Enhancement Act. On August 26, 2004, the Justice Department announced the arrests of more than 150 individuals and the return of 117 criminal complaints, indictments, and informations in a collaborative nationwide sweep directed at cyber economic crime and other cyber crimes.<sup>143</sup> Known as "Operation Web Snare," the operation targeted identity theft, fraud, counterfeit software, computer intrusions, and other intellectual property crimes.<sup>144</sup> The Attorney General directed the Department to "make full use of the Act's provisions in any appropriate investigation or prosecution involving identity theft, including fraud, organized crime, drug trafficking, and terrorism-related matters."<sup>145</sup>

### *The Future of Identity Theft and Phishing*

---

<sup>140</sup> Pub. L. No. 108-275 § 4 (July 15, 2004).

<sup>141</sup> 18 U.S.C. § 1028(a)(1-8) (2003) (*superseded by* Pub. L. No. 108-275 (July 15, 2004)).

<sup>142</sup> Pub. L. No. 108-275 § 2(a)(1) (July 15, 2004).

<sup>143</sup> Attorney General John Ashcroft, Remarks at the Department of Justice (Aug. 26, 2004), at <http://www.usdoj.gov/ag/speeches/2004/82604ag.htm>.

<sup>144</sup> Attorney General John Ashcroft, Remarks at the Department of Justice (Aug. 26, 2004), at <http://www.usdoj.gov/ag/speeches/2004/82604ag.htm>.

<sup>145</sup> Attorney General John Ashcroft, Remarks at the Department of Justice (Aug. 26, 2004), at <http://www.usdoj.gov/ag/speeches/2004/82604ag.htm>.

One of the latest methods of ID theft, “phishing,” involves unsolicited e-mails sent to Internet users.<sup>146</sup> A recent edition of the *Washington Post* featured four articles on this new form of identity theft.<sup>147</sup> The *Post* stated, “Phishing scams usually start with an e-mail that looks like it comes from a bank, Internet service provider or e-commerce company. It often tells recipients that they need to update their account information by clicking on a link provided in the e-mail. If they do not, the mail warns, their accounts could be terminated or they could be subject to some other negative consequence.”<sup>148</sup> Often marked “URGENT,” these messages attempt to convince Internet users to disclose personal information, user names, passwords, credit-card numbers, etc.

One article, providing a history of “phishing,” indicated that as early as September 2003 e-mail fraudsters were registering dozens of lookalike domain names, such as yahoo-billing.com and ebay-fulfillment.com.<sup>149</sup> In the first six months of 2004, the number of unique phishing attacks jumped by more than 800 percent — from 176 in January 2004 to 1,422 in June 2004.<sup>150</sup>

While it might be assumed that the elderly and the technophobic are the most frequent victims of such scams, it is actually 18- to 25-year-olds who are the most frequent victims.<sup>151</sup> This is because people in that age group spend more time online and are more likely to bank online.<sup>152</sup> Larry Ponemon, an adjunct professor of privacy and ethics at Carnegie Mellon

---

<sup>146</sup> On his website, Chairman Kyl has posted information concerning “phishing.” See Appendix C.

<sup>147</sup> Brian Krebs, *Phishing Feeds Internet Black Markets*, WASH. POST, Nov. 18, 2004, available at <http://www.washingtonpost.com/ac2/wp-dyn/A59347-2004Nov18?language=printer>; Brian Krebs, *Phishing Schemes Scar Victims*, WASH. POST, Nov. 18, 2004, available at <http://www.washingtonpost.com/ac2/wp-dyn/A59349-2004Nov18?language=printer>; Brian Krebs, *How to Fend off Phishing*, WASH. POST, Nov. 18, 2004, available at <http://www.washingtonpost.com/ac2/wp-dyn/A59383-2004Nov18?language=printer>; Brian Krebs, *A Brief History of Phishing*, WASH. POST, Nov. 18, 2004, available at <http://www.washingtonpost.com/ac2/wp-dyn/A59350-2000Nov18?language=printer>.

<sup>148</sup> Brian Krebs, *Phishing Schemes Scar Victims*, WASH. POST, Nov. 18, 2004, available at <http://www.washingtonpost.com/ac2/wp-dyn/A59349-2004Nov18?language=printer>.

<sup>149</sup> Brian Krebs, *A Brief History of Phishing*, WASH. POST, Nov. 18, 2004, available at <http://www.washingtonpost.com/ac2/wp-dyn/A59350-2000Nov18?language=printer> (citing the Anti-Phishing Working Group).

<sup>150</sup> Brian Krebs, *A Brief History of Phishing*, WASH. POST, Nov. 18, 2004, available at <http://www.washingtonpost.com/ac2/wp-dyn/A59350-2000Nov18?language=printer>.

<sup>151</sup> Brian Krebs, *A Brief History of Phishing*, WASH. POST, Nov. 18, 2004, available at <http://www.washingtonpost.com/ac2/wp-dyn/A59350-2000Nov18?language=printer>. According to a study of more than 1,330 Internet users conducting in September by the Tucson, Arizona-based Ponemon Institute, 18- to 25-year-olds are nearly three times more likely to get hooked than any other age group. *Id.*

<sup>152</sup> Brian Krebs, *A Brief History of Phishing*, WASH. POST, Nov. 18, 2004, available at <http://www.washingtonpost.com/ac2/wp-dyn/A59350-2000Nov18?language=printer>.

University, which conducted the survey on “phishing” victims, said younger people “seem to be more complacent about those risks than other age groups.”<sup>153</sup>

The FTC reported last year that the average identity theft victim could expect to lose roughly \$500 per incident.<sup>154</sup> According to experts, a person who “falls for a phishing scam is exposed to far more fraudulent activity than someone who loses a credit card, in part because phishing victims give their personal data directly to people who are most likely to defraud them.”<sup>155</sup>

The Subcommittee will continue to follow this “rapidly growing form of fraud that blends old-fashioned confidence scams with innovations in technological trickery”<sup>156</sup> and examine ways to crack down on the criminal network committed to perpetuating a crime that can haunt victims for years.

## **Virtual Threat, Real Terror: Cyberterrorism**

### *Virtual Threat, Real Terror*

On February 24, 2004, the Subcommittee held a hearing to assess the cyberterrorist threat to the United States and our vulnerability to cyberterrorist attacks.<sup>157</sup> Since 1997, the

---

<sup>153</sup> Brian Krebs, *A Brief History of Phishing*, WASH. POST, Nov. 18, 2004, available at <http://www.washingtonpost.com/ac2/wp-dyn/A59350-2000Nov18?language=printer>.

<sup>154</sup> Brian Krebs, *A Brief History of Phishing*, WASH. POST, Nov. 18, 2004, available at <http://www.washingtonpost.com/ac2/wp-dyn/A59350-2000Nov18?language=printer>.

<sup>155</sup> Brian Krebs, *A Brief History of Phishing*, WASH. POST, Nov. 18, 2004, available at <http://www.washingtonpost.com/ac2/wp-dyn/A59350-2000Nov18?language=printer>.

<sup>156</sup> Brian Krebs, *Phishing Feeds Internet Black Markets*, WASH. POST, Nov. 18, 2004, available at <http://www.washingtonpost.com/ac2/wp-dyn/A59347-2004Nov18?language=printer>.

<sup>157</sup> *Virtual Threat, Real Terror: Cyberterrorism in the 21<sup>st</sup> Century: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (Feb. 24, 2004) (S. Hrg. 108-516, Serial No. J-108-58) [hereinafter “Hearing of Feb. 24, 2004”].

Subcommittee has held seven hearings on cyber attacks and critical infrastructure protection.<sup>158</sup>

Cyber attacks have increased both in frequency and effectiveness. The number of computer-security intrusions increased from 84,000 in 2002 to 137,000 in 2003.<sup>159</sup> Computer viruses are spreading at much faster rates and causing more damage than ever before. While it took 26 hours for a virus in 2001 to infect 300,000 machines worldwide, a virus in February 2003 infected the same number of machines in only 14 minutes.<sup>160</sup> As Homeland Security Secretary Ridge stated in December 2003, “anywhere there is a computer . . . whether in a corporate building, a home office, or a dorm room . . . if that computer isn’t secure, it represents a weak link. Because it only takes one vulnerable system to start a chain reaction that can lead to devastating results.”<sup>161</sup>

In his opening statement, Chairman Kyl stressed that “[t]errorists are targeting our cyber infrastructure, and we must educate the public about the threat of cyberterrorism.”<sup>162</sup> Data from Al Qaeda computers found in Afghanistan show that the group scouted systems that control

---

<sup>158</sup> See *Improving Our Ability to Fight Cybercrime: Oversight of the National Infrastructure Protection Center: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107<sup>th</sup> Cong., 1<sup>st</sup> Sess. (July 25, 2001) (S. Hrg. 107-366, Serial No. J-107-22); *Cyber Attack: Improving Prevention and Prosecution: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 106<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (Apr. 21, 2000) (S. Hrg. 106-838, Serial No. J-106-79); *Cyber Attacks: Removing Roadblocks to Investigation and Information Sharing: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 106<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (Mar. 28, 2000) (S. Hrg. 106-839, Serial No. J-106-72); *Cyber Attacks: The National Protection Plan and Its Privacy Implications: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 106<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (Feb. 1, 2000) (S. Hrg. 106-889, Serial No. J-106-62). See also *Critical Infrastructure Protection: The Threat Is Real: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 106<sup>th</sup> Cong., 1<sup>st</sup> Sess. (Oct. 6, 1999) (S. Hrg. 106-858, Serial No. J-106-53); *Critical Infrastructure Protection: Toward a New Policy Directive: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 105<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (Mar. 17, 1998) (S. Hrg. 105-763, Serial No. J-105-88); *The Nation at Risk: The Report of the President’s Commission on Critical Infrastructure Protection: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 105<sup>th</sup> Cong., 1<sup>st</sup> Sess. (Nov. 5, 1997) (S. Hrg. 105-447, Serial No. J-105-68).

<sup>159</sup> CERT Coordination Center, *CERT/CC Statistics 1988-2003*, at [http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html) (last visited Jan. 21, 2005).

<sup>160</sup> Fiona Harvey, *Online Crime Set to Rise: Cyberspace: The Fight Against Hackers Is a Big Burden*, FIN. TIMES (London), Dec. 3, 2003, at 3.

<sup>161</sup> Secretary Tom Ridge, Remarks at the National Cyber Security Summit (Dec. 3, 2003), at <http://www.dhs.gov/dhspublic/display?content=3059>.

<sup>162</sup> Hearing of Feb. 24, 2004, at 37 (written statement of Jon Kyl).

critical U.S. infrastructure systems.<sup>163</sup> An attack on these systems could have devastating results, especially if done in conjunction with a physical attack. A study by the National Infrastructure Protection Center concluded that the effects of September 11 would have been “far greater” if launched in conjunction with a cyber attack disabling New York City’s water or electrical systems.<sup>164</sup> Knocking out those systems would have inhibited emergency services from dealing with the crisis, and turned many of the bystanders into victims.

At previous Subcommittee hearings,<sup>165</sup> witnesses had expressed concerns about terrorists conducting cyber attacks against the United States. Terrorists already use cyber tools to raise funds and organize physical attacks; they could use those same tools for conducting cyber warfare. In 2000, FBI Director Louis Freeh testified that cyberterrorism was “a very real, though still largely potential threat.”<sup>166</sup> The February 2004 Subcommittee hearing focused on the current status of that threat, what is being done to reduce it, and whether any additional resources or changes in the law are needed. “Although the United States has not suffered a major cyberterrorist attack,” Chairman Kyl stated, “we must continue to improve the security of our critical infrastructure systems.”<sup>167</sup> The Subcommittee heard from five witnesses: Amit Yoran, Director of the National Cyber Security Division (NCSD) of the Department of Homeland Security; Keith Lourdeau, Deputy Assistant Director of the FBI’s Counterterrorism Division; John Malcolm, Deputy Assistant Attorney General of the Justice Department; Howard Schmidt, Chief Information Security Officer for eBay; and Dan Verton, a senior writer on cyber security for Computerworld and author of *Black Ice: The Invisible Threat of Cyberterrorism*.

### *Tracking Down Cyber Intruders and the Importance of the Patriot Act*

---

<sup>163</sup> David McLemore, *On the Cyberterror Front Lines; San Antonio Carving a Niche by Helping Protect Vital Systems*, DALLAS MORNING NEWS, Sept. 21, 2003, at 31A.

<sup>164</sup> National Infrastructure Protection Center (NIPC), *Swarming Attacks: Infrastructure Attacks for Destruction and Disruption*, at 7 (July 2002). NIPC’s functions have since been assumed by the Department of Homeland Security’s Information Analysis and Infrastructure Protection Directorate (IAIP), which is under the direction of the DHS witness, Director Amit Yoran. NIPC was formerly part of the Department of Justice.

<sup>165</sup> See *Improving Our Ability to Fight Cybercrime: Oversight of the National Infrastructure Protection Center: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107<sup>th</sup> Cong., 1<sup>st</sup> Sess. (July 25, 2001) (S. Hrg. 107-366, Serial No. J-107-22); *Cyber Attack: Improving Prevention and Prosecution: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 106<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (Apr. 21, 2000) (S. Hrg. 106-838, Serial No. J-106-79).

<sup>166</sup> *Cyber Attacks: Removing Roadblocks to Investigation and Information Sharing: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 106<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (Mar. 28, 2000) (S. Hrg. 106-839, Serial No. J-106-72), at 28 (written statement of Louis Freeh [hereinafter “Hearing of Mar. 28, 2000”]).

<sup>167</sup> Hearing of Feb. 24, 2004, at 3 (statement of Jon Kyl).

Progress has been made since September 11 in our ability to detect and prosecute cyberterrorists and other cyber criminals. The Justice Department has created the Computer Crime and Intellectual Property System (CCIPS), a team of 37 attorneys who work exclusively on cyber and intellectual property crime.<sup>168</sup> In addition, 13 Computer Hacking and Intellectual Property (CHIP) Units were set up to prosecute cyber crime cases and work with local industry to deter cyber crimes before they occur.<sup>169</sup> The FBI has established the Interagency Coordination Cell to facilitate information-sharing among federal, state, and local agencies, and is expanding the coordination cell to work with foreign governments as well.<sup>170</sup> The FBI has also developed the Cyber International Investigative Program, to facilitate FBI cyber investigations in foreign countries.<sup>171</sup> This focus on improving international investigations paid off in June 2003, when a joint operation of the FBI and Romanian police apprehended two suspects who had hacked into the National Science Foundation's South Pole Research Station.<sup>172</sup>

At the Subcommittee hearing, Mr. Malcolm testified that recent changes in the law, particularly certain provisions of the USA Patriot Act,<sup>173</sup> will play a vital role in preventing and prosecuting cyberterrorism and cyber crime.<sup>174</sup> One provision, for example, allows computer service-providers to voluntarily disclose subscriber communications in emergency situations without fear of civil liability.<sup>175</sup> In one case, a death threat was made on a high school Internet message board, but the owner/operator of the message board initially refused to release information to the authorities out of fear of monetary liability.<sup>176</sup> Once informed of the Patriot Act provision waiving such liability, he cooperated; his information helped identify and arrest

---

<sup>168</sup> Hearing of Feb. 24, 2004, at 57 (written statement of John Malcolm).

<sup>169</sup> Hearing of Feb. 24, 2004, at 58 (written statement of John Malcolm).

<sup>170</sup> Hearing of Feb. 24, 2004, at 47 (written statement of Keith Lourdeau).

<sup>171</sup> Hearing of Feb. 24, 2004, at 48 (written statement of Keith Lourdeau).

<sup>172</sup> Hearing of Feb. 24, 2004, at 50-51 (written statement of Keith Lourdeau). In May 2003, an e-mail was sent to the National Science Foundation (NSF) saying that the sender had hacked into the server of the South Pole Research Station, and would "tell the world" how vulnerable the server was unless the NSF paid a certain level of money. *Id.* at 50. After confirming that the system was hacked into, the FBI determined that the message was sent from a cyber café in Romania. *Id.* Working with Romanian police, the FBI tracked down the hackers and arrested them in June 2003, only one month after the start of the investigation. *Id.* at 57.

<sup>173</sup> See Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act), Pub. L. No. 107-56 (Oct. 24, 2001).

<sup>174</sup> Hearing of Feb. 24, 2004, at 64 (written statement of John Malcolm).

<sup>175</sup> Hearing of Feb. 24, 2004, at 64 (written statement of John Malcolm).

<sup>176</sup> Hearing of Feb. 24, 2004, at 64-65 (written statement of John Malcolm).

the guilty party.<sup>177</sup> Mr. Malcolm also testified that another provision, permitting courts to issue nationwide search warrants for electronic communications, has greatly improved prosecutions by preserving time-sensitive evidence in cases where the evidence could have been lost if access to it had not been expedited.<sup>178</sup> Mr. Malcolm told the Subcommittee that these, and other, provisions of the Patriot Act were “essential to any . . . prosecution of cyberterrorism.”<sup>179</sup>

### *Lacking a Cyberterrorism Threat Assessment*

While progress has been made in investigating and prosecuting cyber attacks, the Subcommittee hearing showed the need for better cooperation among the agencies in developing a clear assessment of the cyberterrorist threat. Director Yoran testified that, to protect critical infrastructure, NCSA takes a “threat-independent” approach that concentrates on eliminating vulnerabilities in cyber systems.<sup>180</sup> However, Richard Pethia, the Director of the CERT Coordination Center (a reporting center for computer-security problems, housed at Pittsburgh’s Carnegie Mellon University) had testified at a March 2000 hearing that the government really needed to develop an accurate threat assessment for cyber attacks.<sup>181</sup> Mr. Pethia said that private sector entities could not afford to eliminate every vulnerability in their operations, and needed a threat assessment to allocate their resources efficiently.<sup>182</sup>

When asked by Chairman Kyl whether the Department of Homeland Security had conducted a cyberterrorism threat assessment, Mr. Yoran replied that the Department is developing a critical infrastructure threat and protection strategy, but not a strategy focused on cyberterrorism.<sup>183</sup> In fact, Mr. Yoran did not appear to know of any cyber threat assessment, even though the FBI’s Mr. Lourdeau testified that the Bureau had created a classified assessment of cyber threats.<sup>184</sup> Mr. Yoran only knew of the National Intelligence Estimate (NIE) being prepared on cyber threats, which had not been completed at the time of the Subcommittee hearing.<sup>185</sup> Regarding the FBI’s threat assessment, Mr. Lourdeau of the FBI characterized the cyberterrorism threat as “rapidly expanding,” yet he offered no real specifics on what types of

---

<sup>177</sup> Hearing of Feb. 24, 2004, at 65 (written statement of John Malcolm).

<sup>178</sup> Hearing of Feb. 24, 2004, at 65 (written statement of John Malcolm).

<sup>179</sup> Hearing of Feb. 24, 2004, at 65 (written statement of John Malcolm).

<sup>180</sup> Hearing of Feb. 24, 2004, at 9 (statement of Amit Yoran).

<sup>181</sup> Hearing of Mar. 28, 2000, at 37 (statement of Richard Pethia).

<sup>182</sup> Hearing of Mar. 28, 2000, at 37 (statement of Richard Pethia).

<sup>183</sup> Hearing of Feb. 24, 2004, at 13 (statement of Amit Yoran).

<sup>184</sup> Hearing of Feb. 24, 2004, at 14 (statement of Keith Lourdeau).

<sup>185</sup> Hearing of Feb. 24, 2004, at 14 (statement of Amit Yoran).

systems or vulnerabilities the terrorists were targeting.<sup>186</sup> In any case, neither the NIE nor the FBI's threat assessment would give the private sector the information it needs to allocate cyber security resources more efficiently, since both assessments are classified.

The most detailed information on the cyberterrorism threat was provided to the Subcommittee by Computerworld's Mr. Verton. Mr. Verton, whose book chronicled Al Qaeda's use of computer technology, testified that it has the "intent, resources, and opportunity" to carry out cyber attacks.<sup>187</sup> A high-ranking Al Qaeda official told Mr. Verton that cyber attacks could be used in the near future to destroy U.S. economic markets.<sup>188</sup> Also, the growing number of technologically sophisticated Al Qaeda sympathizers gives the terrorist network more potential personnel who could conduct cyber attacks.<sup>189</sup> Al Qaeda has held formal electronics training in Pakistan. It trains only those people who have previous electronics or computer-engineering experience.<sup>190</sup> Finally, Mr. Verton told the Subcommittee that Al Qaeda definitely has a ripe target in the United States, as there are ample vulnerabilities in U.S. critical infrastructure systems.<sup>191</sup> While some progress has been made in cyber security since September 11, 2001, Mr. Verton said that "we are nowhere near where we should be."<sup>192</sup>

### *Interagency Responsibility*

Another issue raised at the Subcommittee hearing was the apparent confusion among government agencies as to their respective roles in preventing cyberterrorism. According to Deputy Assistant Attorney General Malcolm, these roles were clarified by President Bush in Homeland Security Presidential Directive 7, issued on December 17, 2003.<sup>193</sup> The directive grants specific "core missions" to the Justice Department, the FBI, and the Department of Homeland Security.<sup>194</sup>

---

<sup>186</sup> Hearing of Feb. 24, 2004, at 46 (written statement of Keith Lourdeau).

<sup>187</sup> Hearing of Feb. 24, 2004, at 22 (statement of Dan Verton).

<sup>188</sup> Hearing of Feb. 24, 2004, at 21-22 (statement of Dan Verton).

<sup>189</sup> Hearing of Feb. 24, 2004, at 22 (statement of Dan Verton).

<sup>190</sup> Hearing of Feb. 24, 2004, at 21 (statement of Dan Verton).

<sup>191</sup> Hearing of Feb. 24, 2004, at 22 (statement of Dan Verton).

<sup>192</sup> Hearing of Feb. 24, 2004, at 22 (statement of Dan Verton).

<sup>193</sup> Exec. Dir. H.S.P.D. 7 (December, 17, 2003).

<sup>194</sup> Written Response of John Malcolm, at 3 (June 25, 2004).

The Justice Department is principally responsible for investigating, deterring, and prosecuting crimes against computer systems and data. As part of this function, the Justice Department gathers, disseminates, and exploits intelligence related to cyber threats.<sup>195</sup> The Department is also responsible for coordinating with foreign authorities to prosecute and prevent cyber crimes that cross international borders.<sup>196</sup>

The FBI, under the direction of the Justice Department, is responsible for investigating specific cyber crimes. The FBI's Cyber Division not only investigates and assists in the prosecution of such acts, but also works with the Computer Security Institute to prepare the annual Computer Crime and Security Survey, an initiative designed to encourage the sharing of cyber security information between government agencies and the private sector.<sup>197</sup>

The Department of Homeland Security is principally responsible for identification, prevention, and remediation of vulnerabilities related to cyber security. The Department of Homeland Security's National Cyber Security Division issues warnings and alerts, conducts vulnerability and threat assessments, and works closely with other components of the Department of Homeland Security in the research and development of new technologies to enhance cyber security.<sup>198</sup>

While lines may occasionally blur, each agency is primarily responsible for those aspects of cyber security that relate to its core mission. To facilitate better communication between the agencies, the FBI, the Justice Department, and the Department of Homeland Security all participate in regular interagency contact and cooperation activities organized by the Department of Homeland Security's Cyber Interagency Incident Management Group.<sup>199</sup>

#### *Public/Private Cooperation Has a Long Way to Go*

With 85 to 90 percent of U.S. critical infrastructure controlled by private entities,<sup>200</sup> cyber security depends on the ability of the government to work with the private sector. The Subcommittee hearing showed that, while improvements have been made in this area in recent years, problems still remain. To encourage private companies to report cyber intrusions, the

---

<sup>195</sup> Written Response of John Malcolm, at 2 (June 25, 2004).

<sup>196</sup> Written Response of John Malcolm, at 2 (June 25, 2004).

<sup>197</sup> Written Response of John Malcolm, at 2 (June 25, 2004).

<sup>198</sup> Written Response of John Malcolm, at 2-3 (June 25, 2004).

<sup>199</sup> Written Response of John Malcolm, at 3 (June 25, 2004).

<sup>200</sup> Hearing of Feb. 24, 2004, at 17 (statement of John Malcolm).

Homeland Security Act of 2002<sup>201</sup> exempted such reporting from Freedom of Information Act (FOIA)<sup>202</sup> requests. Mr. Schmidt told the Subcommittee that the FOIA exception did increase private sector cooperation by protecting the information reported from being released to the public.<sup>203</sup> He said, however, that companies are still concerned about sharing security information with state governments, because under many state sunshine laws, such information could be released to the general public.<sup>204</sup>

### *Making Combating Cyberterrorism a Priority*

While progress has been made in combating cyber attacks, much remains to be done. At the Subcommittee hearing, Senator Feinstein stated that “cyber security should be one of the lead priorities of the Department of Homeland Security,”<sup>205</sup> and she expressed concern that cyberterrorism has not received the priority that it requires. Senator Feinstein noted that, before the formation of the Department of Homeland Security, Richard Clarke and Howard Schmidt served as special advisors to the White House on cyberspace security. However, when the Department was created, Amit Yoran was appointed director of the National Cyber Security Division and cyberspace security was relegated to a mid-level position. As Senator Feinstein pointed out, Mr. Yoran “does not report directly to Secretary Ridge, but to an assistant secretary.”<sup>206</sup>

Senator Feinstein asked Mr. Yoran to comment on his lack of seniority in the Department: “How will you be able to direct assistant secretaries in other directorates to bolster up cyber security? Do you have the organizational clout, for example, to get the Border and Transportation Directorate to bolster its cyber security policies?”<sup>207</sup> Mr. Yoran responded by maintaining that cyber security has “a very high profile with the administration and within the Department . . . .”<sup>208</sup>

---

<sup>201</sup> Pub. L. No. 107-296 (Nov. 25, 2002).

<sup>202</sup> Pub. L. No. 104-231 (Oct. 2, 1996).

<sup>203</sup> Hearing of Feb. 24, 2004, at 26 (statement of Howard Schmidt).

<sup>204</sup> Hearing of Feb. 24, 2004, at 26-27 (statement of Howard Schmidt).

<sup>205</sup> Hearing of Feb. 24, 2004, at 10 (statement of Dianne Feinstein).

<sup>206</sup> Hearing of Feb. 24, 2004, at 10 (statement of Dianne Feinstein).

<sup>207</sup> Hearing of Feb. 24, 2004, at 10 (statement of Dianne Feinstein).

<sup>208</sup> Hearing of Feb. 24, 2004, at 10 (statement of Amit Yoran).

Seven months after the Subcommittee hearing (and exactly one year after taking the job), Mr. Yoran resigned unexpectedly as the nation's top cyber-security official.<sup>209</sup> Mr. Yoran is the third cyber security chief to resign in less than two years.<sup>210</sup> In an interview, he praised the President's plan and indicated that Secretary Ridge understood the significance of cyber security,<sup>211</sup> but he declined to say why he left his post after giving just one day's notice. He did, however, confide to industry officials that "he had been disappointed that he was not given as much authority as he was promised to attack the problems."<sup>212</sup> It was reported that his lack of authority disturbed the technology industry and some lawmakers.<sup>213</sup> They pressed unsuccessfully "to elevate Yoran's role to that of an assistant secretary, which could mean broader authority and more resources for cyber security issues."<sup>214</sup>

Mr. Yoran was frustrated "over what he considers a lack of attention paid to computer security issues within the agency."<sup>215</sup> Paul Kurtz, Executive Director of the Cyber Security Industry Alliance, who also worked on security issues in the White House, stated that "it's kind of symptomatic of the frustration all around."<sup>216</sup> He warned that "cyber-security has fallen down

---

<sup>209</sup> Ted Bridis, *U.S. Cybersecurity Chief Abruptly Resigns*, ASSOC. PRESS, Oct. 1, 2004, available at [http://hosted.ap.org/dynamic/stories/C/CYBERSECURITY\\_CHIEF?SITE=LAAL&SECTION=HOME&TEMPLATE=DEFAULT](http://hosted.ap.org/dynamic/stories/C/CYBERSECURITY_CHIEF?SITE=LAAL&SECTION=HOME&TEMPLATE=DEFAULT).

<sup>210</sup> Robert O'Harrow Jr. and Ellen McCarthy, *Top U.S. Cyber-Security Official Resigns*, WASH. POST, Oct. 2, 2004, at A18.

<sup>211</sup> Robert O'Harrow Jr. and Ellen McCarthy, *Top U.S. Cyber-Security Official Resigns*, WASH. POST, Oct. 2, 2004, at A18.

<sup>212</sup> Robert O'Harrow Jr. and Ellen McCarthy, *Top U.S. Cyber-Security Official Resigns*, WASH. POST, Oct. 2, 2004, at A18.

<sup>213</sup> Ted Bridis, *U.S. Cybersecurity Chief Abruptly Resigns*, ASSOC. PRESS, Oct. 1, 2004, available at [http://hosted.ap.org/dynamic/stories/C/CYBERSECURITY\\_CHIEF?SITE=LAAL&SECTION=HOME&TEMPLATE=DEFAULT](http://hosted.ap.org/dynamic/stories/C/CYBERSECURITY_CHIEF?SITE=LAAL&SECTION=HOME&TEMPLATE=DEFAULT).

<sup>214</sup> Ted Bridis, *U.S. Cybersecurity Chief Abruptly Resigns*, ASSOC. PRESS, Oct. 1, 2004, available at [http://hosted.ap.org/dynamic/stories/C/CYBERSECURITY\\_CHIEF?SITE=LAAL&SECTION=HOME&TEMPLATE=DEFAULT](http://hosted.ap.org/dynamic/stories/C/CYBERSECURITY_CHIEF?SITE=LAAL&SECTION=HOME&TEMPLATE=DEFAULT).

<sup>215</sup> Ted Bridis, *U.S. Cybersecurity Chief Abruptly Resigns*, ASSOC. PRESS, Oct. 1, 2004, available at [http://hosted.ap.org/dynamic/stories/C/CYBERSECURITY\\_CHIEF?SITE=LAAL&SECTION=HOME&TEMPLATE=DEFAULT](http://hosted.ap.org/dynamic/stories/C/CYBERSECURITY_CHIEF?SITE=LAAL&SECTION=HOME&TEMPLATE=DEFAULT).

<sup>216</sup> Robert O'Harrow Jr. and Ellen McCarthy, *Top U.S. Cyber-Security Official Resigns*, WASH. POST, Oct. 2, 2004, at A18.

on that totem pole.”<sup>217</sup> Kevin Poulsen, a cyber security specialist, stated, “In an age of physical terrorism and real-world threat, they’re not giving cyber security much attention.”<sup>218</sup>

On October 13, 2004, Homeland Security Secretary Tom Ridge said the role of overseeing cyber security should have a higher profile at the agency, especially as technology executives and experts express concern that cyber security is getting inadequate attention.<sup>219</sup> Secretary Ridge indicated that the agency was creating a new assistant secretary position.<sup>220</sup> When Mr. Yoran heard that the agency might create an assistant secretary of cybersecurity, he called it a “fantastic move.”<sup>221</sup> The Agency later indicated that the job will instead be a deputy assistant secretary position.<sup>222</sup> As the agency seeks to redefine the role of overseeing cybersecurity, the Subcommittee will exercise oversight to help ensure that the government is working to protect the nation from cyber crime.

In the 109th Congress, a follow-up hearing will likely be needed to discuss any such legislation, and to make sure that the relevant federal agencies are developing a cyber strategy that addresses both the threats to, and the vulnerabilities of, U.S. critical infrastructure.

## **Database Security**

### *Preventing Unauthorized Access*

The Subcommittee also looked at ways to prevent terrorists and other criminals from hacking into databases to obtain Social Security numbers, driver’s licenses, and financial

---

<sup>217</sup> Robert O’Harrow Jr. and Ellen McCarthy, *Top U.S. Cyber-Security Official Resigns*, WASH. POST, Oct. 2, 2004, at A18.

<sup>218</sup> Robert O’Harrow Jr. and Ellen McCarthy, *Top U.S. Cyber-Security Official Resigns*, WASH. POST, Oct. 2, 2004, at A18.

<sup>219</sup> Jonathan Krim, *Cyber-Security to Get Higher-Profile Leader*, WASH. POST, Oct. 13, 2004, at A11.

<sup>220</sup> Jonathan Krim, *Cyber-Security to Get Higher-Profile Leader*, WASH. POST, Oct. 13, 2004, at A11.

<sup>221</sup> Jonathan Krim, *Cyber-Security to Get Higher-Profile Leader*, WASH. POST, Oct. 13, 2004, at A11.

<sup>222</sup> Jonathan Krim, *Cyber-Security to Get Higher-Profile Leader*, WASH. POST, Oct. 13, 2004, at A11.

information. In a Subcommittee hearing on November 4, 2003,<sup>223</sup> Senator Feinstein described the dire state of database security and the lack of laws to address database theft:

According to the Computer Security Institute's 2003 Computer Crime and Security Survey, they polled 376 organizations and each one admitted experiencing a security breach in the past year. Half of them said they didn't do anything, and only a third of them reported it. So of a field, everybody has been hacked into and various personal information has been violated, and yet nothing has happened.<sup>224</sup>

David McIntyre, President and CEO of TriWest Healthcare Alliance, testified about a December 2002 break-in at TriWest Healthcare's Phoenix offices. Thieves stole laptop computers and hard drives containing the names, addresses, telephone numbers, birth dates, and Social Security numbers of 562,000 military service members, dependents, and retirees.<sup>225</sup> The thieves also stole medical claims records for people on active duty in the Persian Gulf.<sup>226</sup> The motivation behind the crime is unknown, because the thieves were never found.<sup>227</sup> The potential harm to a group this large, particularly to those who wear the uniform of this country, was staggering. Due to TriWest's prompt and thorough response,<sup>228</sup> not a single individual has suffered identity theft as a result of this crime.<sup>229</sup>

Mark MacCarthy, Senior Vice President of Public Policy for Visa U.S.A., testified about the steps that Visa has taken to avoid database security breaches and notify its customers of any security breach that does occur.<sup>230</sup> First, Visa has a policy to "black out" all but the last four digits of a credit-card number on receipts printed from new terminals, and within a short while,

---

<sup>223</sup> *Database Security: Finding Out When Your Information Has Been Compromised: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 1<sup>st</sup> Sess. (Nov. 4, 2003) (S. Hrg. 108-520, Serial No. J-108-52) [hereinafter "Hearing of Nov. 4, 2003"].

<sup>224</sup> Hearing of Nov. 4, 2003, at 3 (statement of Dianne Feinstein).

<sup>225</sup> Hearing of Nov. 4, 2003, at 44 (written statement of David McIntyre).

<sup>226</sup> Hearing of Nov. 4, 2003, at 4 (statement of David McIntyre).

<sup>227</sup> Hearing of Nov. 4, 2003, at 44 (written statement of David McIntyre).

<sup>228</sup> Upon discovering the theft, TriWest worked "around the clock" to contact the affected individuals and assist them in placing fraud flags on their credit files. Hearing of Nov. 4, 2003, at 45 (written statement of David McIntyre). Within a few weeks, TriWest had contacted each of the affected individuals, created a web site and call center to answer questions about identity-theft issues, and coordinated with the three credit bureaus to provide information on how to prevent identity theft and how to place fraud alerts in individual credit files. Hearing of Nov. 4, 2003, at 45-46 (written statement of David McIntyre).

<sup>229</sup> Hearing of Nov. 4, 2003, at 5 (statement of David McIntyre).

<sup>230</sup> Hearing of Nov. 4, 2003, at 38 (written statement of Mark MacCarthy).

the last four digits will be blacked out at all terminals.<sup>231</sup> Second, Visa is implementing a comprehensive cardholder information security plan that requires entities to comply with the Visa “digital dozen,” 12 basic requirements for safeguarding account information.<sup>232</sup> Third, the Visa system includes sophisticated neural networks that flag unusual spending patterns.<sup>233</sup> The network blocks authorization when such a pattern is detected.<sup>234</sup> Visa also maintains a worldwide database of account numbers that are lost or stolen and advocates “customer notification whenever unauthorized access to customer information results in a significant recognizable threat that requires customer action.”<sup>235</sup> Visa also advocates that “notification requirements be sufficiently flexible to allow notice to be provided by the account-holding institution, even if the account-holding institution was not the operator of the system where the break occurred.”<sup>236</sup> Mr. MacCarthy testified that S. 1350, the Notification of Risk to Personal Data Act,<sup>237</sup> introduced by Senator Feinstein, afforded such flexibility while “establishing consistent procedures for notifying individuals about security breaches.”<sup>238</sup>

Evan Hendricks, Editor of *Privacy Times*, testified that “this bill is a very good starting point and can accomplish a lot of good in setting a national standard.”<sup>239</sup> Mr. Hendricks also testified to the increasing number of database security breaches:

Identity theft is the fastest growing crime in the United States. There are so many studies out this summer by the FTC, the GAO, the Gartner Group, Privacy in American Business, that say it is far worse than we even expected and that the biggest threat to information security is by authorized insiders using their authorized insiderness to use that information for unauthorized purposes.<sup>240</sup>

---

<sup>231</sup> Hearing of Nov. 4, 2003, at 6 (statement of Mark MacCarthy).

<sup>232</sup> Hearing of Nov. 4, 2003, at 6 (statement of Mark MacCarthy).

<sup>233</sup> Hearing of Nov. 4, 2003, at 6 (statement of Mark MacCarthy).

<sup>234</sup> Hearing of Nov. 4, 2003, at 6 (statement of Mark MacCarthy).

<sup>235</sup> Hearing of Nov. 4, 2003, at 6 (statement of Mark MacCarthy).

<sup>236</sup> Hearing of Nov. 4, 2003, at 6-7 (statement of Mark MacCarthy).

<sup>237</sup> S. 1350, 108<sup>th</sup> Cong. (2003).

<sup>238</sup> Hearing of Nov. 4, 2003, at 7 (statement of Mark MacCarthy).

<sup>239</sup> Hearing of Nov. 4, 2003, at 8 (statement of Evan Hendricks).

<sup>240</sup> Hearing of Nov. 4, 2003, at 8 (statement of Evan Hendricks).

He admitted that the openness and leadership shown by TriWest and Visa are the exception to the rule, not the norm.<sup>241</sup> He cited the recent Victoria's Secret case, which was prosecuted by New York Attorney General Elliott Spitzer. In that case, a computer glitch on the company's website allowed access to people's purchases. When notified, Victoria's Secret said (in the words of Evan Hendricks) that "no credit card numbers were involved, so what is the big deal?"<sup>242</sup>

Mr. Hendricks testified to another problem: outsourcing of personal data processing to other countries.<sup>243</sup> On October 22, 2003, the *San Francisco Chronicle* ran a story about an employee in Pakistan who was doing medical transcription.<sup>244</sup> Apparently, she was not paid, so she threatened to post medical details about the patients on the Internet to force her employer to pay her.<sup>245</sup>

Big credit bureaus such as Equifax, Experian, and Trans Union are outsourcing to Jamaica, the Philippines, and India.<sup>246</sup> Evan Hendricks testified, "These [practices] raise serious questions about how [data will] be protected as it goes across our borders and [whether] Americans feel secure in that. So that is another reason why this bill is so important."<sup>247</sup>

#### *The Notification of Risk to Personal Data Act*

Recognizing the gravity of the threat, Senator Feinstein introduced S. 1350, which would require businesses to maintain computerized databases enabling customers to be informed of hacking incidents that could compromise their sensitive personal data. The bill's notification requirements would be triggered if a hacker obtained access to a customer's Social Security number, driver's license number, or bank-account, debit-card, or credit-card number. Notice would be provided to individuals in writing, by e-mail, or by substitute notice. Substitute notice

---

<sup>241</sup> Hearing of Nov. 4, 2003, at 8 (statement of Evan Hendricks).

<sup>242</sup> Hearing of Nov. 4, 2003, at 8 (statement of Evan Hendricks).

<sup>243</sup> Hearing of Nov. 4, 2003, at 8 (statement of Evan Hendricks).

<sup>244</sup> David Lazarus, *At Tough Lesson on Medical Privacy: Pakistani Transcriber Threatens UCSF Over Back Pay*, SAN FRAN. CHRON., Sept. 9, 2003, at A1.

<sup>245</sup> David Lazarus, *At Tough Lesson on Medical Privacy: Pakistani Transcriber Threatens UCSF Over Back Pay*, SAN FRAN. CHRON., Sept. 9, 2003, at A1.

<sup>246</sup> Hearing of Nov. 4, 2003, at 9 (statement of Evan Hendricks).

<sup>247</sup> Hearing of Nov. 4, 2003, at 9 (statement of Evan Hendricks).

could be used to avoid undue burdens on agencies or companies.<sup>248</sup> Action on the bill was not completed on the bill before the end of the 108<sup>th</sup> Congress.

### *Cyber-Crooks Gaining the Upper Hand*

Such notification requirements are a step in the right direction. Sadly, one year after the hearing, cyber analysts believe the number of database breaches is increasing. A CNN report published on September 22, 2004 indicates that analysts “believe cyber-crooks may be gaining the upper hand on Internet security.”<sup>249</sup> In fact, just days before the CNN report, a computer technician involved in the largest identity theft in U.S. history, surpassing \$50 million, pled guilty to conspiracy in a scheme that stole personal information from tens of thousands of individuals.<sup>250</sup> Earlier this year, the MyDoom.M virus shut down the Internet search engines Google, Yahoo, Lycos, and AltaVista for several hours.<sup>251</sup> These search engines often contain records of personal information.

Today, experts contend that “even the latest anti-virus software and expensive firewalls cannot fully protect . . . computer[s] from the latest hacker attacks.”<sup>252</sup> Mikko Hypponen of the virus research firm F-Secure Corporation warned, “The situation on the Internet right now is so bad that if you go and buy a brand new computer and turn it on and plug it into the Internet, it will be infected by a worm within five to ten minutes. You will not even have enough time to go online and download all the patches to your computer before it is infected.”<sup>253</sup> According to Microsoft, such intruders create a cost up to \$20.5 billion annually in lost business and repair work.<sup>254</sup>

---

<sup>248</sup> Substitute notice includes notice by e-mail, the posting of notice on the company or agency website, or the notification of major media. Substitute notice is allowed if (i) the company demonstrates that the cost of providing direct notice would exceed \$250,000; (ii) the number of subject persons to be notified exceeds 500,000; or (iii) the company does not have sufficient contact information to notify people whose information is at risk. S. 1350, 108<sup>th</sup> Cong. (2003).

<sup>249</sup> Neil Curry, *Protecting the office from cyber-attack*, CNN.com (Sept. 22, 2004), at <http://www.cnn.com/2004/BUSINESS/09/13/go.cyber.security/index.html>.

<sup>250</sup> *Guilty Plea in \$50 Million Identity Theft*, CNN.com (Sept. 14, 2004), at <http://www.cnn.com/2004/LAW/09/14/identity.theft.ap/index.html>.

<sup>251</sup> Neil Curry, *Protecting the office from cyber-attack*, CNN.com (Sept. 22, 2004), at <http://www.cnn.com/2004/BUSINESS/09/13/go.cyber.security/index.html>.

<sup>252</sup> Neil Curry, *Protecting the office from cyber-attack*, CNN.com (Sept. 22, 2004), at <http://www.cnn.com/2004/BUSINESS/09/13/go.cyber.security/index.html>.

<sup>253</sup> Neil Curry, *Protecting the office from cyber-attack*, CNN.com (Sept. 22, 2004), at <http://www.cnn.com/2004/BUSINESS/09/13/go.cyber.security/index.html>.

<sup>254</sup> Neil Curry, *Protecting the office from cyber-attack*, CNN.com (Sept. 22, 2004), at <http://www.cnn.com/2004/BUSINESS/09/13/go.cyber.security/index.html>.

Mikko Hypponen explains, “The formula for virus protection has changed little for users over the years.”<sup>255</sup> He advocates four rules for protecting computers and personal information: (1) Put anti-virus software on every computer, (2) install a firewall on every computer, (3) keep the patches up-to-date on every computer, and (4) turn off every computer when not in use.<sup>256</sup> The last rule is especially important as identity theft is facilitated by the proliferation of high-speed Internet connections — and computers left permanently connected.

## SEAPORT SECURITY

### Seaport Security

#### *The Importance of America’s Seaports and the Dangers of Attack*

The Subcommittee held a hearing on January 27, 2004 to examine how to protect U.S. seaports from terrorist attack.<sup>257</sup> Senator Feinstein noted their critical vulnerability when she described them as the “soft underbelly of our Nation’s security.”<sup>258</sup> She also stated that there was a “very real possibility that a weapon of mass destruction could be brought in a container, either detonated in a port in a busy metropolitan area or shipped in by rail or truck into Arizona or the heartland of our Nation.”<sup>259</sup>

U.S. seaports present a particularly attractive target for terrorists because the effects of such an attack could be catastrophic. An attack that shut down a major American port for even a few days could devastate the regional economy that it serves.<sup>260</sup> By one estimate, a nuclear

---

<sup>255</sup> Neil Curry, *Protecting the office from cyber-attack*, CNN.com (Sept. 22, 2004), at <http://www.cnn.com/2004/BUSINESS/09/13/go.cyber.security/index.html>.

<sup>256</sup> Neil Curry, *Protecting the office from cyber-attack*, CNN.com (Sept. 22, 2004), at <http://www.cnn.com/2004/BUSINESS/09/13/go.cyber.security/index.html>.

<sup>257</sup> *Covering the Waterfront: A Review of Seaport Security Since September 11, 2001: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (Jan. 27, 2004) (transcript) [hereinafter “Hearing of Jan. 27, 2004”].

<sup>258</sup> Hearing of Jan. 27, 2004, at 6 (transcript) (statement of Dianne Feinstein).

<sup>259</sup> Hearing of Jan. 27, 2004, at 6 (transcript) (statement of Dianne Feinstein).

<sup>260</sup> Council on Foreign Relations, *Terrorism Q & A: Ports*, at [http://www.terrorismanswers.com/security/ports\\_print.html](http://www.terrorismanswers.com/security/ports_print.html) (last visited Jan. 23, 2004). This view is supported by M.R. Dinsmore, Chief Executive of the Port of Seattle and a member of the CEO Roundtable of the National Defense Transportation Association, who wrote in a September 17, 2004 *Washington Post* article, “We can verify the contents of only about 4 to 6 percent of those containers. And it would require only one rogue container to bring commerce to its knees . . . Global trade could practically be shut down. And we don’t have the systems in place to get our seaports up and running again.” He added, “We’re spending a fraction of what we spend at airports, on a far more complex problem. We do not have a

weapon detonated in a major seaport or Washington, D.C., would kill 50,000 to one million people, would result in direct property damage of \$50 billion to \$500 billion, would cause trade disruption of \$100 billion to \$200 billion, and would create indirect costs of \$300 billion to \$1.2 trillion.<sup>261</sup>

The hearing, a follow up to one held by the Subcommittee in February 2002,<sup>262</sup> stressed the importance of seaport security. In the immediate aftermath of the attacks of September 11, the Secretary of Transportation shut down virtually the entire airline industry for four days; each plane was checked to ensure the safety of air travel and to prevent additional hijackings.<sup>263</sup> If the United States ever experienced a similar situation with shipping — if we had to shut down our ports and check all ships for terrorists — commercial shipping would halt for at least four months.<sup>264</sup> As Captain William Schubert of the Department of Transportation testified, “[i]f anything can bring our economy down, that can.”<sup>265</sup>

The January 2004 Subcommittee hearing sought to determine what progress had been made in seaport security since September 11, and what needs to be done. In his opening statement, Chairman Kyl stated that U.S. seaports offer relatively easy access points for terrorists and their weapons, including weapons of mass destruction.<sup>266</sup> Immediately following the September 11 attacks, seaport security became the Coast Guard’s main focus, but that commitment has wavered in the last two years. Before the attacks on New York and Washington, the Coast Guard devoted not more than two percent of its operations to port security, according to the Council on Foreign Relations.<sup>267</sup> In the months immediately following September 11, the Coast Guard spent 50 to 60 percent of its time and effort defending U.S. ports. Since then, however, that figure has fallen to between 20 to 30 percent because of other

---

comprehensive plan . . . What we need is for the federal government . . . to produce a set of standards, practices and protocols giving clear policy guidance and to make intelligent investments to secure our ports.” M.R. Dinsmore, *Make Our Ports Safer*, WASH. POST, Sept. 17, 2004, at A27.

<sup>261</sup> Abt Associates, *The Economic Impact of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability*, Apr. 30, 2003, at 7 (executive summary).

<sup>262</sup> *Securing Our Ports Against Terror: Technology, Resources & Homeland Defense: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (Feb. 26, 2002) (S. Hrg. 107-855, Serial No. J-107-61) [hereinafter “Hearing of Feb. 26, 2002”].

<sup>263</sup> Hearing of Feb. 26, 2002, at 23 (statement of William Schubert).

<sup>264</sup> Hearing of Feb. 26, 2002, at 23 (statement of William Schubert).

<sup>265</sup> Hearing of Feb. 26, 2002, at 23 (statement of William Schubert).

<sup>266</sup> Hearing of Jan. 27, 2004, at 1-2 (transcript) (statement of Jon Kyl).

<sup>267</sup> Council on Foreign Relations, *Terrorism Q & A: Ports*, at [http://www.terrorismanswers.com/security/ports\\_print.html](http://www.terrorismanswers.com/security/ports_print.html) (last visited Jan. 23, 2004).

commitments and mounting costs.<sup>268</sup> Noel Cunningham, the Los Angeles Port's Chief of Police, said the Los Angeles harbor remained “wide open” to terrorist attack.<sup>269</sup>

The Subcommittee heard from three government officials: Rear Admiral Larry Hereth, Director of Port Security for the U.S. Coast Guard; Gary Bald, Acting Assistant Director of the Counterterrorism Division of the FBI; and Robert Jacksta, Executive Director of Border Security and Facilitation for Customs and Border Protection (CBP). Their testimony described the approach their agencies have adopted to seaport security, as U.S. authorities try to identify and respond to threats heading toward but still far from the United States and seek to improve security inside the ports themselves.

*Extending the Security Net: Identifying and Intercepting Threats Before They Happen*

Terrorists could not only inflict severe damage by detonating a nuclear weapon in a U.S. seaport, they could inflict severe damage by just getting the weapon near a port and detonating it. The only way to protect against that scenario is to detect the threat at sea, well before it reaches a port. Admiral Hereth testified that the Department of Homeland Security (DHS) has adopted a strategy to widen security awareness geographically, with a multi-agency, layered approach to seaport security that focuses on “identifying and intercepting threats well before they reach U.S. shores.”<sup>270</sup> Several new programs by CBP are designed to accomplish these goals:

- National Targeting Center (NTC): The NTC receives and processes, 24 hours a day, electronic cargo and travel information from ships in advance of their arrival in the United States.<sup>271</sup>
- Automated Targeting System (ATS): ATS organizes the information processed by the NTC and then ranks cargo containers in order of risk, so that CBP can focus on physically inspecting only the containers that pose a significant security threat.<sup>272</sup>
- Container Security Initiative (CSI): To extend the zone of security even farther, CSI was implemented to screen and examine shipments before they depart foreign

---

<sup>268</sup> Council on Foreign Relations, *Terrorism Q & A: Ports*, at [http://www.terrorismanswers.com/security/ports\\_print.html](http://www.terrorismanswers.com/security/ports_print.html) (last visited Jan. 23, 2004).

<sup>269</sup> *About 12 Million Containers Enter U.S. Ports Annually; Only 4% Get Security*, WALL ST. J., Apr. 21, 2003, at B1.

<sup>270</sup> Hearing of Jan. 27, 2004, at 1 (written statement of Larry Hereth).

<sup>271</sup> Hearing of Jan. 27, 2004, at 2 (written statement of Robert Jacksta).

<sup>272</sup> Hearing of Jan. 27, 2004, at 3 (written statement of Robert Jacksta).

ports for the United States.<sup>273</sup> Based on information analyzed by the ATS, CBP determines whether to conduct an inspection overseas.<sup>274</sup> So far, 19 of the 20 foreign ports that conduct the most trade with the United States have committed to joining CSI; these 20 ports account for two-thirds of the containers shipped to U.S. ports.<sup>275</sup> Mr. Jacksta testified that the foreign governments participating in CSI have been very cooperative — they have been willing to take the containers CBP has selected and even help conduct the examination of the suspected cargo.<sup>276</sup>

### *Improving Security at the Ports: Targeted Screening, Security Plans, and Pilot Programs*

While there is a new emphasis on widening scrutiny of international shipping, security in the ports themselves remains a key concern. Mr. Bald of the FBI testified at the Subcommittee hearing that U.S. seaports are “inherently vulnerable” because of their proximity to land and air, as well as to chemical and natural resource storage facilities.<sup>277</sup>

Improving security at the ports is a work in progress. The increased security regulations mandated by the Maritime Transportation Security Act of 2002,<sup>278</sup> such as the requirement for transportation security ID cards, are just starting to be implemented.<sup>279</sup> CBP has developed a more thorough process, with the NTC and the ATS, of identifying threats and targeting high-risk cargo for screening. While CBP still only physically inspects 5.4 percent of the containers coming into the country, Mr. Jacksta informed the Subcommittee that CBP plans to enhance non-intrusive inspection technology, with the eventual goal of screening 100 percent of cargo for radiation.<sup>280</sup> Admiral Hereth also stated that the Coast Guard is still reviewing vessel and facility security plans, and pledged at the hearing that the security assessments for all 55 of the nation’s most strategically important ports would be completed by December 2004.<sup>281</sup> As of January 19, 2005, the Coast Guard has completed port security assessments at 54 of the 55 U.S. ports. The Coast Guard is in the process of conducting a port security assessment on the one remaining port

---

<sup>273</sup> Hearing of Jan. 27, 2004, at 4 (written statement of Robert Jacksta).

<sup>274</sup> Hearing of Jan. 27, 2004, at 38 (transcript) (statement of Robert Jacksta).

<sup>275</sup> Hearing of Jan. 27, 2004, at 4 (written statement of Robert Jacksta).

<sup>276</sup> Hearing of Jan. 27, 2004, at 38 (transcript) (statement of Robert Jacksta).

<sup>277</sup> Hearing of Jan. 27, 2004, at 2 (written statement of Gary Bald).

<sup>278</sup> Pub. L. No. 107-295 (Nov. 25, 2002).

<sup>279</sup> Hearing of Jan. 27, 2004, at 41-42 (transcript) (statement of Larry Hereth).

<sup>280</sup> Hearing of Jan. 27, 2004, at 8 (written statement of Robert Jacksta).

<sup>281</sup> Hearing of Jan. 27, 2004, at 33-34 (transcript) (statement of Larry Hereth).

(San Francisco/Oakland/Richmond), which will be completed by the end of February 2005, and the report finalized in March 2005.<sup>282</sup>

Although DHS is the lead agency in charge of seaport security, the FBI has a major role in providing threat analysis and working with DHS on the National Joint Terrorism Task Force (NJTTF) and local JTTFs.<sup>283</sup> Mr. Bald testified that the FBI has participated in several pilot programs that could greatly improve port security. In Miami, for example, the FBI developed the Manning Agency Screening Initiative, to provide limited database checks on agencies that provide staff members to global cruise lines.<sup>284</sup>

#### *Working with the Private Sector: Improving Security Without Hindering Trade*

One of the major challenges of seaport security is safeguarding our ports without stopping the free flow of goods into the country. The United States could attempt to physically inspect every container to ensure that no terrorists or weapons were being smuggled into the country, but such a solution would completely halt commercial shipping. Admiral Hereth testified at the Subcommittee hearing that DHS is sensitive to these concerns, and that the security measures to date have not hampered significantly the flow of commerce into the seaports.<sup>285</sup> The Coast Guard has created Area Maritime Security Committees to give the private sector input into developing security plans at individual seaports.<sup>286</sup> These committees are comprised of personnel from the local maritime industry, in addition to federal, state, and local officials, and are a key means of developing improved vessel and facility security within U.S. seaports.<sup>287</sup>

#### *Follow-Up Hearing and Future Legislation*

As testimony at the Subcommittee hearing made clear, seaport security is improving but much remains to be done. Chairman Kyl and Senator Feinstein introduced a bill (S. 746) to tighten standards for container security, and to increase penalties for those violating seaport-

---

<sup>282</sup> Briefing paper provided by U.S. Coast Guard, "Status of the Domestic Port Security Assessment Program," Jan. 19, 2005 (on file with the Senate Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary).

<sup>283</sup> Hearing of Jan. 27, 2004, at 2-3 (written statement of Gary Bald).

<sup>284</sup> Hearing of Jan. 27, 2004, at 3-4 (written statement of Gary Bald).

<sup>285</sup> Hearing of Jan. 27, 2004, at 12 (transcript) (statement of Larry Hereth).

<sup>286</sup> Hearing of Jan. 27, 2004, at 4 (written statement of Larry Hereth).

<sup>287</sup> Hearing of Jan. 27, 2004, at 4 (written statement of Larry Hereth).

security measures.<sup>288</sup> The bill, the Reducing Crime and Terrorism at America's Seaports Act, would:

- Clarify that existing law concerning fraudulent access to transport facilities includes seaports and waterfronts within its scope;
- Increase from five to ten years the maximum prison term for fraudulently gaining access to a U.S. port;
- Toughen sanctions, including criminal charges, for failure to cooperate with the U.S. Coast Guard;
- Amend current law to close loopholes and make it a crime, with stiff penalties, to willfully use a dangerous weapon (including chemical, biological, radiological, or nuclear materials) or explosives with the intent to cause death, serious bodily harm, or catastrophic economic injury;
- Provide criminal sanctions for intentionally damaging any of the Coast Guard's 50,000-plus navigational aids, and make it a crime to knowingly place in waters any device or substance likely to damage a vessel or its cargo, or to willfully and maliciously discharge a hazardous substance into U.S. waters with the intent to cause death, serious bodily harm, or catastrophic economic injury;
- Make it a crime to transport aboard any vessel explosives, biological agents, chemical weapons, or radioactive or nuclear materials knowing that they are intended for a terrorist act; and
- Modernize current law to increase sanctions to deter criminal or civil violations related to a range of offenses, including bribery, "stowaways," and theft of interstate or foreign shipments and goods from transportation facilities or instruments, including trailers, cargo containers, and warehouses.

The Subcommittee will continue to fight for passage of this bill.<sup>289</sup>

## **BORDER SECURITY**

### **Role of Technology in Border Security**

---

<sup>288</sup> S. 746, 108<sup>th</sup> Cong. (2003).

<sup>289</sup> See also companion bills S. 1587, 108<sup>th</sup> Cong. (2003) and S. 2653, 108<sup>th</sup> Cong. (2004).

## Border Technology

In the aftermath of September 11, the Department of Homeland Security (DHS) was created and 22 different agencies were brought together to better coordinate efforts to protect the United States and its citizens against terror threats. Among the Department's core responsibilities is preventing terrorists from entering the country. The September 11 hijackers entered the United States through a legitimate immigration process that failed to catch inaccuracies in their student and tourist visa applications. The result was that officials at the Immigration and Naturalization Service (INS) did not know the terrorists remained in the country after those visas expired.

On March 12, 2003, the Subcommittee held a joint hearing with the Subcommittee on Immigration, Border Security, and Citizenship, entitled "Border Technology: Keeping Terrorists Out of the United States."<sup>290</sup> The hearing complemented the Subcommittee's October 2002 hearing on how technology could be used to prevent terrorist entry into the United States.<sup>291</sup> The three primary purposes of the joint hearing were:

- To review the progress of the administration, in particular DHS, in implementing the technology systems that Congress had specifically mandated in the Enhanced Border Security and Visa Entry Reform Act of 2001,<sup>292</sup>
- To examine the existing Customs Service infrastructure and technology policies and identify the additional infrastructure and technology needed at U.S. land ports of entry; and
- To examine technology and other needs along the borders between ports of entry.

In short, the hearing focused on what technology programs and infrastructures would better prevent terrorists from entering the United States.

### *The Enhanced Border Security and Visa Reform Act*

---

<sup>290</sup> *Border Technology: Keeping Terrorists Out of the United States: Joint Hearing Before the Subcomm. on Immigration, Border Security, and Citizenship and the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 1<sup>st</sup> Sess., (Mar. 12, 2003) (S. Hrg. 108-148, Serial No. J-108-5) [hereinafter "Hearing of Mar. 12, 2003 "].

<sup>291</sup> *The Role of Technology in Preventing the Entry of Terrorists into the United States: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 107<sup>th</sup> Cong., 1<sup>st</sup> Sess. (Oct. 12, 2001) (S. Hrg. 107-611, Serial No. J-107-43) [hereinafter "Hearing of Oct. 12, 2001 "].

<sup>292</sup> Pub. L. No. 107-173 (May 14, 2002).

The Enhanced Border Security and Visa Reform Act<sup>293</sup> was enacted to prevent terrorists from exploiting our nation's visa processing and inspection system. Terrorists had exploited loopholes and gaps in the system in three ways: (1) they could enter the United States with valid, or at least facially valid, visas issued by the Department of State; (2) terrorists, smugglers, and illegal immigrants could use fraudulent documents to enter the country; and (3) individuals could be smuggled into the country.<sup>294</sup>

To address these weaknesses and prevent terrorists from entering the country, the Act implements a series of technology-related tools and infrastructures. The Act requires implementation of an automated Entry-Exit system (which would track entry and exit information on all individuals who hold travel documents); the creation of biometric travel documents; the implementation of biometric data readers and scanners at all points of entry; the implementation of the Chimera Interoperable Data System to integrate all INS databases of intelligence information relevant to making decisions on visa admissibility and removal of aliens; and the implementation of the Mexican Laser Visa and Reader Program, which would require such visas to contain a biometric identifier.

### *Border Security Challenges*

The witnesses at the March 12, 2003 hearing were Asa Hutchinson, Under Secretary for Border and Transportation Safety at the DHS; Nancy Kingsbury, Managing Director of Applied Research and Methods at the General Accounting Office;<sup>295</sup> and Stephen Flynn, Jeanne J. Kirkpatrick Senior Fellow in National Security Studies at the Council on Foreign Relations.

Under Secretary Hutchinson described the visa-issuance and border-security challenges that DHS faced in the aftermath of September 11, as well as the Department's efforts to improve the visa-issuance program and comply with the congressionally mandated deadlines for implementation of homeland security technology. At the time of the hearing, the Department expected to meet the December 31, 2003 deadline for implementation of the Exit-Entry system, and had already begun registering aliens through the National Security Entry-Exit Registration System (NSEERS).<sup>296</sup> In fact, some 88,989 people had been registered and eight terror suspects

---

<sup>293</sup> Pub. L. No. 107-173 (May 14, 2002).

<sup>294</sup> Hearing of Mar. 12, 2003, at 2 (statement of Jon Kyl).

<sup>295</sup> Now the Government Accountability Office.

<sup>296</sup> Hearing of Mar. 12, 2003, at 14, 21 (statement of Asa Hutchinson). On January 5, 2004, US-VISIT entry procedures became operational at 115 airports and 14 seaports. *Homeland Security to Begin Biometric Pilot Program*, at [http://www.dhs.gov/dhspublic/interapp/content\\_multi\\_image/content\\_multi\\_image\\_0006.xml](http://www.dhs.gov/dhspublic/interapp/content_multi_image/content_multi_image_0006.xml) (last visited Oct. 18, 2004). Also in January 2004, a pilot program testing biometric exit procedures was started at one airport and one seaport. *Id.* In November 2004, the Department of Homeland Security announced that a pilot program testing the entry procedures was implemented at three land ports of entry, including Douglas, Arizona. DHS Press Release, *US-VISIT Implementation Dates at Land Border Crossings Announced*, Nov. 9, 2004. The Department was required by the end of 2004 to expand US-VISIT to the 50 busiest land ports of entry. For more

had been arrested through NSEERS.<sup>297</sup> Other programs, such as the Biometric Verification System and the Secure Electronic Network for Travelers Rapid Inspection (SENTRI), a system used at land ports of entry to identify and validate international travelers who regularly cross the border, successfully identified suspected terrorists attempting to enter the United States.<sup>298</sup> Those programs were to be expanded, and additional Border Patrol agents were to be deployed to U.S. borders with FY 2003 DHS funding.<sup>299</sup>

The GAO's Ms. Kingsbury testified that the use of biometric identifiers is a highly effective way to verify the identity of individuals who seek to enter the United States, and thus prevent suspected terrorists from entering.<sup>300</sup> Several biometric programs are already being used to control the border, including the Automated Fingerprint Identification System (IDENT), which identifies aliens who repeatedly attempt to enter the United States.<sup>301</sup> While Ms. Kingsbury agreed that using biometrics is an efficient way to identify and document individuals who attempt to enter the country, she emphasized that the costs and benefits of the system still needed to be addressed.<sup>302</sup> She stated, "[w]e believe it is very important that a thorough and documented concept of operations be created and examined before these decisions are made and before this starts down the path of spending huge amounts of money."<sup>303</sup> She also cautioned, "[e]ffective border security at ports of entry requires technology and people to work together to implement a decision system that is grounded in well-developed and implemented policies and procedures."<sup>304</sup>

To prevent dangerous terror-related goods from entering the United States, the Department of Homeland Security implemented 112 non-intrusive cargo-inspection systems at air, sea, and land ports of entry, and planned to deploy additional systems.<sup>305</sup> Trade data was

---

detailed information on US-VISIT, see *US-VISIT Statistics*, at Department of Homeland Security Home: [http://www.dhs.gov/dhspublic/interapp/editorial/editorial\\_0437.xml](http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0437.xml) (last visited Oct. 18, 2004).

<sup>297</sup> Hearing of Mar. 12, 2003, at 57 (written statement of Asa Hutchinson).

<sup>298</sup> Hearing of Mar. 12, 2003, at 58 (written statement of Asa Hutchinson).

<sup>299</sup> Hearing of Mar. 12, 2003, at 58 (written statement of Asa Hutchinson).

<sup>300</sup> Hearing of Mar. 12, 2003, at 63 (written statement of Nancy Kingsbury).

<sup>301</sup> Hearing of Mar. 12, 2003, at 66 (written statement of Nancy Kingsbury).

<sup>302</sup> Hearing of Mar. 12, 2003, at 31-32 (statement of Nancy Kingsbury).

<sup>303</sup> Hearing of Mar. 12, 2003, at 32-33 (statement of Nancy Kingsbury).

<sup>304</sup> Hearing of Mar. 12, 2003, at 32 (statement of Nancy Kingsbury).

<sup>305</sup> Hearing of Mar. 12, 2003, at 59 (written statement of Asa Hutchinson).

also collected under the Automated Commercial Environment (ACE) to identify high risk cargo and target it for inspection without interrupting the flow of trade across U.S. borders.<sup>306</sup>

Mr. Flynn of the Council on Foreign Relations testified that the United States remained open to, and unprepared to prevent or respond to, terrorists attacks, and that additional resources are essential to protect the United States against terrorism. Those resources include funding for staffing, training, infrastructure, and technology, among other things. As discussed in this report, due to budget constraints, the best way to effectively fund homeland security is by analyzing the risks of terrorist-related activity to points of entry and allocating funds on the basis of need.<sup>307</sup> Intelligence must be gathered so that priority can be given to high risk ports — whether they be land, sea, or air — to maximize our ability to prevent terrorists from entering the country.<sup>308</sup>

As Senator Feinstein noted at the hearing, had certain databases and other immigration and visa security measures been in place, INS could have been alerted to the terrorists overstaying their visas and might therefore have been able to prevent the tragedy of September 11: “The benefit of hindsight provides a clearer picture of how existing technologies might have been used to at least alert the appropriate officials that some, if not all, of the hijackers’ visas should have been denied.”<sup>309</sup>

### *Looking Ahead*

Significant progress toward terrorism prevention has been made since March 2003: The entry portion of the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) was implemented on January 5, 2004 at 115 airports and 14 seaports.<sup>310</sup> The program collects fingerprints and photographs so that an individual’s entry into, and eventually his or her exit from, the United States can be confirmed. In August of 2004, DHS began a pilot program to test the exit portion of US-VISIT at 10 airports, including Phoenix Sky Harbor and San Francisco International Airport, and the San Pedro and Long Beach Seaports. DHS and the Department of State signed a Memorandum of Understanding in September 2003 giving DHS the responsibility for establishing and administering visa-issuance rules, as mandated in Section 428 of the Homeland Security Act, while allowing the State Department to retain the technical responsibility for issuing visas.

---

<sup>306</sup> Hearing of Mar. 12, 2003, at 60 (written statement of Asa Hutchinson).

<sup>307</sup> Hearing of Mar. 12, 2003, at 46 (written statement of Stephen Flynn).

<sup>308</sup> Hearing of Mar. 12, 2003, at 35-36 (written statement of Stephen Flynn).

<sup>309</sup> Hearing of Mar. 12, 2003, at 6 (statement of Dianne Feinstein).

<sup>310</sup> U.S. Dep’t of Homeland Security, *DHS Launches US-VISIT Program Nationwide to Enhance Security, Facilitate Travel*, Press Release, Jan. 5, 2004.

The Subcommittee's hearing publicized steps taken by the government to ensure public safety. It also stressed the importance of continued funding for terrorism-prevention programs and infrastructure. While significant steps have been taken to protect the United States from terrorist activity in the aftermath of September 11, much remains to be done to prevent a future terrorist attack.<sup>311</sup> It is obvious that the implementation of immigrant-tracking databases, such as the US-VISIT and NSEERS, are vital to protecting our borders<sup>312</sup> — but those programs alone will not ensure the safety of Americans in their homeland.

## **Securing the United States through Biometrics**

### *The Biometric Passport Deadline*

Section 303 of the Enhanced Border Security and Visa Reform Act of 2002,<sup>313</sup> coauthored by Chairman Kyl and Senator Feinstein, required that, by October 26, 2004, all countries participating in the Visa Waiver Program (VWP) issue machine-readable, tamper-resistant passports containing biometric identifiers to their citizens who want to enter the United States. Unfortunately, none of the 27 VWP countries has been able to comply with the deadline, even though standardized machine readers and other technology required for the use of biometric passports were available for widespread use before October 26, 2004. If all citizens of VWP countries were required to obtain a non-immigrant visa, travel to the United States may significantly decrease. Because of the potential economic loss and diplomatic unrest that could result, the administration requested that the deadline be extended to November 30, 2006.

The Border Security Act also required that the International Aviation Civil Organization (ICAO) set the standards for the biometric identifier to be included in the passports.<sup>314</sup> ICAO

---

<sup>311</sup> In July 2004, the FBI issued a bulletin to the Mexican media and border law enforcement to be on the lookout for suspected Al Qaeda leader Adnan G. El Shukrijumah. *Arizona: A "Terrorist Corridor?"* Chairman Kyl's WKLY. COLUMN (Aug. 30, 2004), at <http://kyl.senate.gov/record.cfm?id=225605>. The general reaction to this, said Chairman Kyl, was "an aggravated lack of surprise." *Id.* He asked, "How could our notoriously porous border *not* be a conduit for terrorists?" *Id.* The U.S. Border Patrol released data on how many "Other Than Mexican" (OTM) foreign nationals were apprehended in a nine-month period on the southern border. It found that over 100 illegal aliens were OTM, including persons from countries such as Afghanistan, Iran, Pakistan, and Saudi Arabia. *Id.*

<sup>312</sup> Congress has also provided significant increases in personnel and resources, including raising the Border Patrol force from 4,000 in 1996 to around 11,000 today, adding Customs inspectors, and providing "force multipliers" like lighting projects, night-vision goggles, and truck-sized X-ray machines. *Arizona: a "Terrorist Corridor?"* Chairman Kyl's WKLY. COLUMN (Aug. 30, 2004), at <http://kyl.senate.gov/record.cfm?id=225605>. Furthermore, after a visit to the Arizona border with Chairman Kyl and Senator McCain, Department of Homeland Security Undersecretary for Border and Transportation Security, Asa Hutchinson, announced additional resources and policy changes to address the problem. *Id.*

<sup>313</sup> Pub. L. No. 107-173 (May 14, 2002).

<sup>314</sup> Pub. L. No. 107-173 (May 14, 2002).

selected facial recognition as the biometric standard, but also acknowledged that countries could have even more secure passports by using facial recognition in conjunction with a secondary biometric identifier such as digital fingerprints or iris scans.<sup>315</sup>

On June 15, 2004, the Judiciary Committee held a hearing entitled “Biometric Passports.”<sup>316</sup> This hearing, aimed at ensuring that the U.S. government is taking every possible step to protect the country against terrorism, explored the implementation of biometric passports, the status of compliance with biometric requirements by VWP countries, the United States’ compliance with the October 2004 deadline, and the wisdom of a deadline extension.<sup>317</sup> Another topic examined at the hearing was ICAO’s selection of facial recognition as the biometric standard instead of digital fingerprints. The witnesses at the hearing were Asa Hutchinson, Under Secretary for the Border and Transportation Security Directorate at the Department of Homeland Security, and Maura Harty, Assistant Secretary for Consular Affairs at the Department of State.

### *The Visa Waiver Program*

The Visa Waiver Program, begun as a pilot program in 1986 and made permanent with the passage of the Visa Waiver Permanent Program Act of 2000,<sup>318</sup> allows citizens of certain qualified countries<sup>319</sup> to travel to the United States for a maximum of 90 days for tourism or business purposes without first obtaining a visa.<sup>320</sup> To enter the United States, the individual must present a valid passport issued by his country of origin. VWP countries reciprocate by allowing U.S. citizens to enter their countries with only a valid U.S. passport.

From 1998 through 2003, more than 93 million people entered the United States using the VWP.<sup>321</sup> Although 157 individuals with terrorist connections have been denied entry since

---

<sup>315</sup> Technical Advisory Group on Machine Readable Travel Documents, *Updated Technical Report on Biometrics Deployment in Machine Readable Travel Documents*, 15<sup>th</sup> Meeting, May 17-21, 2004, at [http://www.icao.int/icao/en/atb/fal/mrtd/tagmrt15/Docs/TagMrt15\\_WP005\\_en.pdf](http://www.icao.int/icao/en/atb/fal/mrtd/tagmrt15/Docs/TagMrt15_WP005_en.pdf).

<sup>316</sup> Hearing of June 15, 2004.

<sup>317</sup> Hearing of June 15, 2004, at 1 (transcript) (statement of Orrin Hatch).

<sup>318</sup> Pub. L. No. 106-396 (Oct. 30, 2000).

<sup>319</sup> As of March 2004, there were 27 foreign countries participating in the Visa Waiver Program. U.S. Dep’t of State, *VWP Travelers Must Use MRP*, Oct. 26, 2004, at [http://travel.state.gov/visa/temp/without/without\\_1990.html#2](http://travel.state.gov/visa/temp/without/without_1990.html#2).

<sup>320</sup> Dep’t of Homeland Sec., Off. of Inspector Gen., *An Evaluation of the Security Implications of the Visa Waiver Program*, Report Number OIG-04-26, April 2004, at 4 [hereinafter “DHS OIG Report, April 2004”].

<sup>321</sup> DHS OIG Report, April 2004, at 9.

1991,<sup>322</sup> it is possible that terrorists have entered the country through VWP because nationals from VWP countries are subject to less scrutiny by consular and immigration officials than are nationals from non-VWP countries. In fact, according to the DHS Office of the Inspector General, individuals with terrorist connections who were allowed into the United States through the VWP include: (1) Zacarias Moussaoui, the alleged 20th September 11 hijacker; (2) Richard Reid, the “shoe bomber” who attempted to detonate explosives hidden in his shoe during a flight from France to the United States; and (3) Ahmed Ajaj, an organizer of the 1993 World Trade Center bombing who presented a fraudulent Swedish passport in order to enter the United States through VWP.<sup>323</sup>

Before entering the United States, visitors from VWP countries complete an I-94W, Non-immigrant Visa Waiver Arrival/Departure Form, which requests such information as name, date, country of current citizenship, country of residence, passport number, and U.S. destination address.<sup>324</sup> When the visitor enters the United States, the form is checked by a DHS port-of-entry inspector and the passport picture is inspected to determine if he or she is the person who is pictured on the passport. In the absence of indications of fraud, the individual is then admitted into the United States.<sup>325</sup>

### *Why Biometrics?*

The United States government must do everything possible to prevent terrorists from attacking the country again. Since the VWP is an avenue through which terrorists could enter the country, a biometric identifier embedded in foreign passports and other travel documents is essential to lessen the possibility of another attack. Digital fingerprints, a digital photograph, or other biometric information is stored on a microchip embedded in the passport. Upon arriving at a U.S. port of entry, an individual’s passport is scanned by a machine reader to verify that this is, in fact, the individual who was issued the passport. This check greatly reduces the possibility that a terrorist, or other criminal, could enter the United States using either a stolen or a forged passport. The biometric identification information of an individual attempting to use a stolen or altered passport would not match the biometric identification information in the passport, thus alerting port-of-entry inspectors to the fact that the individual was trying to fraudulently enter the country.

### *Biometric Deadline Challenges*

During the hearing, Under Secretary Hutchinson reiterated the administration’s request for a two year extension of the October 26, 2004 deadline for requiring VWP countries to issue

---

<sup>322</sup> DHS OIG Report, April 2004, at 11.

<sup>323</sup> DHS OIG Report, April 2004, at 10-11.

<sup>324</sup> DHS OIG Report, April 2004, at 8.

<sup>325</sup> DHS OIG Report, April 2004, at 8.

machine-readable, tamper-resistant, biometric passports, and testified as to the importance of the use of biometric identifiers in the immigration process.<sup>326</sup> He stated that “the use of biometrics, including digital fingerprints and photographs, is consistent . . . with the values and character of our nation and our commitment to enhance security while facilitating trade and travel, respecting individual rights and privacy, and maintaining positive relations with our allies.”<sup>327</sup> Under Secretary Hutchinson stated that, while most of the 27 designated VWP countries have taken steps toward implementation of procedures to begin issuing biometric passports, none of the countries would be ready to issue such passports by the October deadline, nor would DHS be able to process such passports by the October deadline because a machine reader capable of processing passports from 27 different countries was not yet available.<sup>328</sup> The Under Secretary stated that all of the VWP countries would be able to meet a November 30, 2006 deadline.<sup>329</sup>

Maura Harty, Assistant Secretary for Consular Affairs at the Department of State, described the complexity of complying with the October 2004 deadline. Because ICAO did not establish, until May of 2004, the technical standards for the interoperability of the microchips to be embedded in the passports or the standards for the machine readers to be installed at ports of entry,<sup>330</sup> manufacturers lacked enough time to begin producing the required type of machine readers. Assistant Secretary Harty did, however, testify about the progress that the United States is making toward compliance with the deadline. She said the Department of State planed to begin issuing biometric tourist passports at the Los Angeles passport agency in February 2005, and expects to produce such passports at all passport facilities by December 2005.<sup>331</sup>

Assistant Secretary Harty also testified that State Department Consular Offices would not have the personnel necessary to efficiently issue the estimated five million visas that would be applied for by foreign nationals who would normally travel to the United States through the VWP but who would, after October 26, 2004, be required to obtain non-immigrants visas for such travel. Delays in the visa-issuance process would discourage travel to the United States, harm the U.S. economy, and hurt relations with some of our closest friends and allies.<sup>332</sup>

### *A Plan to Ensure Compliance*

---

<sup>326</sup> Hearing of June 15, 2004, at 13-17 (transcript) (statement of Asa Hutchinson).

<sup>327</sup> Hearing of June 15, 2004, at 13-14 (transcript) (statement of Asa Hutchinson).

<sup>328</sup> Hearing of June 15, 2004, at 15 (transcript) (statement of Asa Hutchinson).

<sup>329</sup> Hearing of June 15, 2004, at 15 (transcript) (statement of Asa Hutchinson).

<sup>330</sup> Hearing of June 15, 2004, at 21 (transcript) (statement of Maura Harty).

<sup>331</sup> Hearing of June 15, 2004, at 3 (written statement of Maura Harty).

<sup>332</sup> Hearing of June 15, 2004, at 3 (written statement of Maura Harty).

Assistant Secretary Harty stated that, while confident that the VWP countries would meet a November 30, 2006 deadline, the State Department would continue to pursue compliance on a diplomatic front.<sup>333</sup> She testified that the biometric passport deadline would be discussed by senior State Department officials at every opportunity with European Union, G-8, and Asia-Pacific Economic Commission members.<sup>334</sup> The State Department also instituted benchmarks for progress toward compliance with the program. Those benchmarks include the establishment of a timeline for compliance and a pilot program to test the configuration, durability, and operability of the microchips and other technology that will be used for the passports.<sup>335</sup>

Understanding that the October 2004 deadline would not be met, Chairman Kyl expressed concern about whether the VWP countries would be able to comply with a new deadline and what steps the Departments of State and Homeland Security would take to ensure that they do. He made it clear that such steps should be reported to Congress, stating “[T]he key point I would like to make to both of you is that there are questions about whether or not we have tried hard enough to get our friends in other countries to meet the compliance date. . . . You have in place a series of checks, milestones to meet. I think it is critical that you supply that information to us on an ongoing basis so that we know how [progress toward compliance] is going.”<sup>336</sup>

#### *Other Concerns About Biometrics and the Visa Waiver Program*

Chairman Kyl and Senator Jeff Sessions questioned ICAO’s selection of facial recognition as the biometric passport standard in lieu of digital fingerprints, stating that digital fingerprint matching is more accurate than facial recognition matching, and that the use of fingerprints as the standard would allow those who enter the United States to be checked against databases already in place in the United States.<sup>337</sup> Assistant Secretary Harty said one of the reasons ICAO chose facial recognition was that the ICAO member countries already collect photographs as part of the passport process.<sup>338</sup> Under Secretary Hutchinson testified that it would be beneficial if digital fingerprints were also made a mandatory biometric identifier in the VWP.<sup>339</sup>

---

<sup>333</sup> Hearing of June 15, 2004, at 4 (written statement of Maura Harty).

<sup>334</sup> Hearing of June 15, 2004, at 4 (written statement of Maura Harty).

<sup>335</sup> Hearing of June 15, 2004, at 4 (written statement of Maura Harty).

<sup>336</sup> Hearing of June 15, 2004, at 42 (transcript) (statement of Jon Kyl).

<sup>337</sup> Hearing of June 15, 2004, at 34 (transcript) (statement of Jeff Sessions) and 40 (transcript) (statement of Jon Kyl).

<sup>338</sup> Hearing of June 15, 2004, at 35 (transcript) (statement of Maura Harty).

<sup>339</sup> Hearing of June 15, 2004, at 37 (transcript) (statement of Asa Hutchinson).

The placement of a biometric identifier in passports will also ensure that it is more difficult to enter the United States with a fraudulent passport through the VWP. Senator Feinstein questioned Under Secretary Hutchinson about the findings of an April 2004 report by the DHS Office of the Inspector General regarding use of fraudulent passports in the VWP, and also the statement of Secretary Ridge explaining that such passports are sometimes given back to the individuals who had tried to use them.<sup>340</sup> She stated that a person using a stolen passport “ought to be taken into custody”<sup>341</sup> and that “there ought to be a very strong penalty to use a fraudulent passport, a fraudulent international driver’s license, a fraudulent Geneva Convention travel document, or any other document as part of the visa waiver program.”<sup>342</sup>

### *Hearing Aftermath*

While significant concerns about extending the biometric passport deadline were discussed at the hearing, the fact that the deadline would not be met was clear. Thus on July 22, 2004, the Senate passed H.R. 4417 (by unanimous consent), which granted a one year extension of the deadline set in Section 303 of the Enhanced Border Security and Visa Reform Act of 2002. H.R. 4417 was signed into law on August 9, 2004.<sup>343</sup> Therefore, by October 26, 2005, all VWP participating countries must issue machine-readable, tamper-resistant, biometric passports to their citizens who wish to enter the United States. The United States will also issue such passports by that date.

It is essential that the 27 VWP-designated countries, along with the United States, meet the October 26, 2005 deadline. The U.S. government must address every vulnerability in the security of our nation, and the use of biometric identifiers in passports issued by VWP countries will narrow one such vulnerability.

Since Chairman Kyl and Senator Feinstein coauthored the original legislative requirement that a biometric identifier be contained in passports issued by VWP countries, and since they remain concerned that terrorists will try to enter the country through VWP, the Subcommittee will continue to monitor progress toward full compliance with Section 303 of the Border Security Act, through critical, ongoing progress updates from the Department of State and the Department of Homeland Security.

## **Drug Trafficking and Terrorism — A Dangerous Mix**

### *Link Between International Drug Traffickers and Terrorists*

---

<sup>340</sup> Hearing of June 15, 2004, at 45-46, 48-49 (transcript) (statement of Dianne Feinstein).

<sup>341</sup> Hearing of June 15, 2004, at 47 (transcript) (statement of Dianne Feinstein).

<sup>342</sup> Hearing of June 15, 2004, at 52 (transcript) (statement of Dianne Feinstein).

<sup>343</sup> Pub. L. No. 107-173 (Aug. 9, 2002).

On several occasions, full Committee Chairman Hatch and Subcommittee Chairman Kyl have collaborated to hold full Committee hearings on issues within the jurisdiction of the Subcommittee. One example was the full Committee hearing on May 20, 2003 to examine narcoterrorism and evaluate the effectiveness of current federal policies, practices, and laws.<sup>344</sup> The Committee's hearing, chaired by Senator Kyl, followed a 2002 Subcommittee hearing that had examined illegal drug-trafficking and its link to terrorism in two parts of the world, Afghanistan and Colombia.<sup>345</sup> The Subcommittee and Committee hearings revealed that a significant and growing connection exists between international drug-traffickers and terrorists.

The Department of State has attested to the connections between Osama bin Laden and drug-trafficking. The following was posted on its website:

Osama bin Laden and his organization finance many of their terrorist activities through the drug trade. In fact, on October 25, 2001, *The Herald* (Glasgow) reported, "Osama bin Laden financed the development of a highly-addictive liquid heroin which he named 'The tears of Allah' as part of his multi-pronged terrorist campaign to destabilize Western society . . . . One source said yesterday: 'It should be called the Devil's Brew rather than Allah's tears. It is a one-way ticket to addiction and death.'" The United Nations has also weighed in on the Taliban and [A] Qaeda connection to the drug trade. According to a U.N. Committee of Experts report on Resolution 1333 (May 2001), "Funds raised from the production and trading of opium and heroin are used by the Taliban to buy arms and other war material, and to finance the training of terrorists and support the operations of extremists in neighboring countries and beyond."<sup>346</sup>

Several terrorist groups have been found to benefit, directly or indirectly, from drug-trafficking activities. The form of such relationships varies among groups and areas in the world. Some terrorist groups are directly involved in the trafficking of illegal drugs; some are indirectly involved in raising funds by providing security for, or taxing, traffickers who transport drugs through areas controlled by the terrorist groups; and some terrorist groups support the actual cultivation of illegal drugs, such as coca or opium. Examples abound:

- In Houston, Texas, in November 2002, four members of the United Self-Defense Groups of Colombia were caught trying to exchange \$25 million in cash and

---

<sup>344</sup> *Narco-Terrorism: International Drug Trafficking and Terrorism — A Dangerous Mix, Hearing Before the Senate Comm. on the Judiciary, 108<sup>th</sup> Cong., 1<sup>st</sup> Sess. (May 20, 2003) (S. Hrg. 108-173, Serial No. J-108-12) [hereinafter "Hearing of May 20, 2003"]].*

<sup>345</sup> *Narco-Terror: The Worldwide Connection Between Drugs and Terror: Hearing Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary, 107<sup>th</sup> Cong., 2<sup>nd</sup> Sess. (Mar. 13, 2002) (S. Hrg. 107-885, Serial No. J-107-66) [hereinafter "Hearing of Mar. 13, 2002"]].*

<sup>346</sup> U.S. State Department, *The Global War on Terrorism: The First Hundred Days*, at <http://www.state.gov/s/ct/rls/rpt/6947.htm> (last visited Jan. 15, 2004).

cocaine for weapons, including shoulder-fired anti-aircraft missiles, 53 million rounds of ammunition, 9,000 rifles, rocket-propelled grenade launchers, along with almost 300,000 grenades to be used by the group's operatives.<sup>347</sup>

- In San Diego, California, in November 2002, two Pakistani nationals and a U.S. citizen were charged with attempting to exchange 6,000 kilograms of heroin and five metric tons of hashish for cash and four anti-aircraft missiles to supply to the Taliban and Al Qaeda associates.<sup>348</sup>
- In April 2003, the FBI and DEA disrupted a major Afghanistan-Pakistan heroin-smuggling operation by arresting 16 individuals. This operation was shipping heroin to the United States, laundering profits from the sale of heroin through Afghan- and Pakistani-owned businesses in the United States, and then sending money back to Afghanistan and India to finance terrorists.<sup>349</sup>
- In the Persian Gulf, during a two-week period in late December 2003 and early January 2004, U.S. naval forces intercepted three ships carrying over three tons of marijuana. At least three of the crewmen seized were identified as having ties to Al Qaeda.<sup>350</sup>

### *Global Phenomenon*

Money is the primary link between terrorism and illegal narcotics.<sup>351</sup> Before 1991, states aligned with the Soviet Union financed most international terrorism. Within three years of the Soviet Union's collapse, the number of Marxist-aligned terrorist groups fell by half. State sponsorship of terrorism has also come under increased scrutiny and greater international condemnation.<sup>352</sup> Several terrorist groups have turned to drug-trafficking as a substitute source of financing.<sup>353</sup>

---

<sup>347</sup> Hearing of May 20, 2003, at 2-3 (statement of Orrin Hatch).

<sup>348</sup> Hearing of May 20, 2003, at 3 (statement of Orrin Hatch).

<sup>349</sup> Hearing of May 20, 2003, at 3 (statement of Orrin Hatch).

<sup>350</sup> Victoria Burnett and Mark Huband, *UK Trains Afghans in anti-Drugs Drive: Kabul and Its Allies Have Struggled to Formulate a Coherent Policy for Tackling Heroin Traffickers, Says Victoria Burnett*, FIN. TIMES (London), Jan. 10, 2004, at 8.

<sup>351</sup> Hearing of May 20, 2003, at 76 (written statement of Larry Johnson).

<sup>352</sup> Hearing of May 20, 2003, at 94 (written statement of Deborah McCarthy).

<sup>353</sup> Hearing of May 20, 2003 at 94 (written statement of Deborah McCarthy).

Narcoterrorism is a world-wide problem.<sup>354</sup> In South America, the State Department has officially designated the National Liberation Army (ELN), the Revolutionary Armed Forces of Colombia (FARC), and the United Self-Defense Groups of Colombia (AUC) as terrorist organizations.<sup>355</sup> Hezbollah and the Islamic Resistance Movement (known as Hamas) operate in the tri-border area of Paraguay, Argentina, and Brazil. The Kurdish Workers Party (PKK) operates among violent separatist Kurds in Turkey.<sup>356</sup> The United Wa State Army is the largest heroin- and methamphetamine-producing organization in Southeast Asia.<sup>357</sup> The Abu Sayyaf Group engages in kidnaping, drug-smuggling, extortion, and other profitable criminal activity in support of its goal of establishing a separate Islamic state in the Philippines.<sup>358</sup> This far-flung group of terrorist organizations connected to narcotics and other illicit activities suggests the global scope of the narcoterror problem. And, as an official of the DEA testified, “the nexus between drugs and terrorism is perilously evident.”<sup>359</sup>

Terrorists also use several types of money-laundering schemes to conduct financial transactions without drawing government scrutiny. At the May 20, 2003 hearing, Deborah McCarthy, of the State Department’s Bureau of International Narcotics and Law Enforcement Affairs, outlined several ways to combat money-laundering. First, governments should ensure a firm legal foundation that criminalizes both money-laundering and terrorist financing, and that provides investigators and prosecutors with the necessary tools to use against sophisticated organizations. Second, they should assist legitimate financial institutions in preventing abuse of their services by criminal elements and terrorist organizations. Third, they should provide investigators with training in the conduct of financial investigations. Finally, they should provide prosecutors and judges with instruction in the complexities of money-laundering, terrorist financing, asset-blocking, and forfeiture.<sup>360</sup> These building blocks would establish a foundation for combating money-laundering with tough, consistent law-enforcement operations.

### *Narcoterror Problem Also an Opportunity*

Terrorists have turned to drug-trafficking for funding, and in so doing, have become more susceptible to law-enforcement actions that target drug-trafficking, money-laundering, and

---

<sup>354</sup> In the United States, a number of agencies are involved in fighting narcoterrorism: the Bureau of Immigration and Customs Enforcement, the FBI, the Drug Enforcement Agency, the State Department Bureau of International Narcotics and Law Enforcement Affairs, and the CIA.

<sup>355</sup> Hearing of May 20, 2003, at 110 (written statement of Raphael Perl).

<sup>356</sup> Hearing of May 20, 2003, at 2 (statement of Orrin Hatch).

<sup>357</sup> Hearing of May 20, 2003, at 9 (statement of Steven Casteel).

<sup>358</sup> Uli Schmetzer, *Fighting Terror with Goodwill in Philippines: U.S. Provides Aid to Win Over Locals*, CHI. TRIB., Feb. 2, 2003, at 4.

<sup>359</sup> Hearing of May 20, 2003, at 10 (statement of Steven Casteel).

<sup>360</sup> Hearing of May 20, 2003, at 99-100 (written statement of Deborah McCarthy).

smuggling.<sup>361</sup> The federal government should enhance the intelligence capabilities and training that support these law-enforcement activities. The Subcommittee will continue to periodically reexamine the progress against narcoterrorist activity, and the suitability of federal laws to the evolving narcoterrorist threat.

## “AFTER-ATTACK” SECURITY

### First Responders

#### *Responding to Terrorist Attacks*

In addition to investigating seaport security and border security, the Subcommittee held a hearing to examine the nation’s ability to respond once a terrorist strike has occurred.<sup>362</sup> The hearing focused on a report prepared by the Independent Task Force on Emergency Responders (sponsored by the Council on Foreign Relations) entitled “Drastically Underfunded, Dangerously Unprepared.”<sup>363</sup> Senator Feinstein described this report as “the first systematic attempt to estimate national homeland security needs.”<sup>364</sup>

The chairman of the task force, former Senator Warren Rudman, and Richard Clarke, Senior Advisor to the Council on Foreign Relations, presented the task force’s report and its chilling conclusion: “the United States must assume that terrorists will strike again,” and “the United States remains dangerously ill-prepared to handle a catastrophic attack on American soil.”<sup>365</sup> Their report recommended that sufficient resources be allocated to address identified threats and vulnerabilities, noting that “[t]he federal government should consider such factors as population, population density, vulnerability assessment, and presence of critical infrastructure within each state.”<sup>366</sup>

---

<sup>361</sup> Hearing of May 20, 2003, at 30 (statement of Raphael Perl).

<sup>362</sup> *Terrorism: First Responders: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 1<sup>st</sup> Sess. (Sept. 3, 2003) (S. Hrg. 108-344, Serial No. J-108-35) [hereinafter “Hearing of Sept. 3, 2003”]; see also *Domestic Preparedness in the Next Millennium: Joint Hearing of the Subcomm. on Youth Violence and the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm. on the Judiciary*, 106<sup>th</sup> Cong., 1<sup>st</sup> Sess. (Apr. 20, 1999) (S. Hrg. 106-424, Serial No. J-106-18) [hereinafter “Hearing of Apr. 20, 1999”].

<sup>363</sup> Council on Foreign Relations, Independent Task Force on Emergency Responders, *Drastically Underfunded, Dangerously Unprepared*, prepared June 2003 [hereinafter “Emergency Responders Report, June 2003”], available at <http://www.cfr.org/pubs.php?year=2003&type=reports>.

<sup>364</sup> Hearing of Sept. 3, 2003, at 4 (statement of Dianne Feinstein).

<sup>365</sup> Emergency Responders Report, June 2003, at 1.

<sup>366</sup> Emergency Responders Report, June 2003, at 4.

At the hearing, Dr. Paul Posner of the General Accounting Office (GAO)<sup>367</sup> made a similar point: “Given the many needs and high stakes involved, it is all the more important that the structure and design of federal grants be geared to fund the highest priority projects with the greatest potential impact for improving homeland security.”<sup>368</sup>

Chairman Kyl concurred with the need for the government to allocate sufficient money carefully, based on an accurate threat analysis:

[I]n its report, the Council says, “In some respects, there is no natural limit to what the United States could spend on emergency preparedness. The United States could spend the entire gross domestic product (GDP) and still be unprepared, *or wisely spend a limited amount and end up sufficiently prepared.*” If it does the former — if it just throws money at the problem — then, as the Council observed, “the United States will have created an illusion of preparedness based on boutique funding initiatives without being systematically prepared. The American people will feel safer because they observe a lot of activity, not be safer because the United States has addressed its vulnerabilities.”<sup>369</sup>

A targeted, needs-based system should be developed for high-risk states and counties; border counties and states, which are high-risk by definition, should receive a more equitable proportion of first responder funding.<sup>370</sup>

### *Faster and Smarter Funding*

Representative Christopher Cox, Chairman of the House Select Committee on Homeland Security, testified before the Subcommittee about how the federal government could improve funding allocations. His proposal is based on the following principles:

- *Threat analysis:* Federal grants should be distributed to state and local governments based on an authoritative assessment of the greatest risk.<sup>371</sup>
- *Rapid distribution of funding:* Funding should reach its intended first responders as quickly as possible.<sup>372</sup>

---

<sup>367</sup> Now the Government Accountability Office.

<sup>368</sup> Hearing of Sept. 3, 2003, at 49 (written statement of Paul Posner).

<sup>369</sup> Hearing of Sept. 3, 2003, at 2 (written statement of Jon Kyl) (quoting Emergency Responders Report, June 2003, at 8) (emphasis added).

<sup>370</sup> Hearing of Sept. 3, 2003, at 3 (written statement of Jon Kyl).

<sup>371</sup> Hearing of Sept. 3, 2003, at 7 (statement of Christopher Cox).

<sup>372</sup> Hearing of Sept. 3, 2003, at 6-7 (statement of Christopher Cox).

- *Regional cooperation:* Funding priorities should reward communities that successfully develop interoperability plans and work across jurisdictional lines.<sup>373</sup>

The Cox bill (H.R. 3266) was introduced after the hearing, at the end of the first session of the 108<sup>th</sup> Congress.<sup>374</sup> The House Homeland Security (Select) Committee favorably reported the bill on March 17, 2004 by unanimous consent, but the full House did not act on it before the end of the Congress. In the meantime, to determine the amount of money spent on first responders and anti-terrorism programs, Chairman Kyl and Senator Feinstein, and other Members, wrote a letter to the General Accounting Office<sup>375</sup> requesting an update of its report entitled *Combating Terrorism: Funding Data Reported to Congress Should Be Improved*.<sup>376</sup> The report was a valuable resource for Congress but became outdated when Congress passed the Homeland Security Act of 2001 and established the Department of Homeland Security. The updated report would address “not only the effect of structural and statutory changes . . . but would review the conclusions and recommendations of the original report.”<sup>377</sup> Once this report is completed, the Subcommittee will review it as the Subcommittee considers ways to ensure faster and smarter funding for first responders.

## **Rapid Bioterrorism Detection and Response: Project Zebra**

### *The Current State of Affairs*

Deputy Secretary of Defense Paul Wolfowitz has put into sharp focus the threat of bioterrorism:

As horrible as it was to have thousands of innocent Americans killed on our own territory on that tragic day (Sept. 11, 2001), that is nothing compared to what terrorists could do with the biological weapons that we know they have been actively seeking. In many ways, biological weapons may be ideally suited for the methods and purposes of terrorists. A mass attack with anthrax or some other biological agent could bring about civilian casualties and catastrophic damage to our economy on a scale far beyond even that which we experienced on September

---

<sup>373</sup> Hearing of Sept. 3, 2003, at 7 (statement of Christopher Cox).

<sup>374</sup> H.R. 3266, 108<sup>th</sup> Cong. (2003).

<sup>375</sup> Now the Government Accountability Office.

<sup>376</sup> Letter to the GAO from Senators Kyl, Feinstein, Graham, and Shelby and Congressmen Sensenbrenner and Conyers, August 11, 2004. The GAO accepted the request per its letter of response to Senators Kyl and Feinstein dated September 10, 2004.

<sup>377</sup> Letter to the GAO from Senators Kyl, Feinstein, Graham, and Shelby and Congressmen Sensenbrenner and Conyers, August 11, 2004.

11<sup>th</sup>, as devastating as that was.<sup>378</sup>

With the advent of bioterrorism, doctors must reorient their thinking. “When you hear hoof beats, you think of horses; you don’t think of zebras.” This old saying summarizes the training doctors receive in medical school: look for the most common illness that matches your patient’s symptoms and treat the patient according to that illness. Medical students are taught to avoid chasing “zebras.” Unfortunately, with the advent of bioterrorism, the zebra has become a far more dangerous phenomenon.

Even when infectious disease agents are successfully identified, the answer often arrives late in the course of the illness — after the patient has either recovered or succumbed.<sup>379</sup> This is why, today, doctors institute antibiotic treatment in a broad manner without a definitive diagnosis. This results in two problems: First, in many cases, had the diagnosis been more definitive, a specific drug could have treated the patient more effectively.<sup>380</sup> This is especially true where the origin of the illness is viral and thus antibiotics are entirely ineffective. Second, the broad use of antibiotics can eventually lead to the evolution of antibiotic-resistant strains of illnesses,<sup>381</sup> negating one of the few treatments we have.

In contrast, the use of DNA analysis allows physicians to make accurate diagnoses the first time they see a patient, enabling doctors to use particularized treatments instead of taking the antibiotic “shotgun” approach. Patients then receive optimal treatment and the growth of antibiotic-resistant bacteria can be kept to a minimum.

#### *What is Project Zebra?*

On May 11, 2004, the Subcommittee held a hearing on bioterrorism and “Project Zebra.”<sup>382</sup> Four experts testified: Dr. Jeffery Trent, a pioneer in the field of functional genomics, is the president and scientific director of the Translational Genomics Research Institute (TGen) in Phoenix, Arizona; Dr. Paul Keim, a leading expert in the field of pathogen genomics, is a scientist with TGen and a faculty member at Northern Arizona University in Flagstaff; Dr. Harvey Meislin, one of the most influential emergency room physicians in the nation, heads up the Emergency Room Department at the University of Arizona Health Science Center in Tucson; and Dr. David Relman, one of the country’s leaders in the field of gene expression profiling and

---

<sup>378</sup> Deputy Secretary of Defense Paul Wolfowitz, *Joint Press Conference with the Department of Health and Human Services and the Department of Homeland Security*, at 5 (April 28, 2004), available at <http://www.defenselink.mil/transcripts/2004/tr20040428-depsecdef1383.html>.

<sup>379</sup> *Rapid Bio-terrorism Detection and Response: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 2<sup>nd</sup> Sess., (May 11, 2004) (S. Hrg. 108-559, Serial No. J-108-74), at 51 (written statement of David Relman) [hereinafter “Hearing of May, 11, 2004”].

<sup>380</sup> Hearing of May 11, 2004, at 52 (written statement of David Relman).

<sup>381</sup> Hearing of May 11, 2004, at 52 (written statement of David Relman).

<sup>382</sup> Hearing of May 11, 2004.

infectious diseases, serves on the faculty at Stanford Medical School and is a practicing physician with the U.S. Department of Veterans Affairs.

As these experts explained to the Subcommittee, using highly precise DNA fingerprinting technology, scientists are able to determine the entire genetic composition of various pathogens.<sup>383</sup> Once a fingerprint has been established for a pathogen, a patient's DNA can be compared to a pathogen's fingerprint to determine whether the patient has been exposed to that agent.<sup>384</sup>

Project Zebra is a collaborative scientific research effort led by pioneers in genetics, toxicology, medicine, and engineering to expand this early research. Its goal is to create a method of disease detection that could quickly, accurately, and, in many cases, pre-symptomatically identify not only if patients are ill, but identify precisely from what illness they suffer. Project Zebra furthermore aims to create a comprehensive training program for emergency room physicians and staff to efficiently manage patients after diagnosis.<sup>385</sup> The project has five key elements:

1. Creation of a DNA database containing the genetic expressions — “fingerprints” — of every known illness and pathogen.
2. Design of diagnostic tools that can extract, copy, and digitize a patient's DNA sequence in a short period of time. The tools must be small, mobile, and relatively inexpensive.
3. Design and implementation of a network that can instantly upload a patient's DNA, compare it to a national database, and return a diagnosis.
4. Institution of a national standardized training program to teach emergency room staff how to manage bio-attack victims effectively.
5. Development of vaccines and suitable drug stockpiles to be easily obtained

---

<sup>383</sup> Hearing of May 11, 2004, at 4 (statement of Paul Keim). Scientists have already accomplished this for anthrax. Edward Winstead, *Three Years After the Anthrax Letters, Are We Safer?*, GENOME NEWS NETWORK, Sept. 17, 2004, available at <http://www.genomenewsnetwork.org/articles/2004/09/17/anthrax.php>. Researchers, including Dr. Keim, “were able to identify very rare genetic differences among the strains, and this will enable us to come up with really effective diagnostic tools.” *Id.*

<sup>384</sup> Hearing of May 11, 2004, at 9 (statement of David Relman). Research demonstrates that when an individual is exposed to environmental stimuli such as a biological, chemical, toxic, radiological, or natural agent, his or her DNA sequence changes in a fashion unique to that agent. *Id.* Different stimuli promote different responses. The challenge is to learn how to read these patterns of change in order to identify which stimulus provoked it. *Id.*

<sup>385</sup> Hearing of May 11, 2004, at 7 (statement of Harvey Meislin).

through the local emergency room system.<sup>386</sup>

### *Creation of a National Database*

Establishment of Project Zebra would require a database containing the genetic expression of every known pathogen as it relates to the human genetic sequence. Once the database is complete, a physician would perform one test, a simple DNA extraction.<sup>387</sup> The DNA sample would then be compared with the pathogen database in search of a match. Using this one test, a physician could test for both the common and the rare — the “horse” and the “zebra.” The patient would receive better care and the system would save money. No longer would a doctor have to guess which test to perform based on a patient’s symptoms, and no longer would the rare incidence of bioterrorism or plague go unnoticed at the outset because the physician failed to properly test for it. Creating a national database of the genetic footprints of all known biological, chemical, toxic, and possibly radiological agents is a colossal undertaking, and should be done on an international scale utilizing both public and private agencies.<sup>388</sup>

### *Data Transmitting Network and Training Program*

The Project Zebra system would require a network that can quickly and accurately

---

<sup>386</sup> While rapidly detecting and accurately diagnosing bioterrorism will help prevent the spread of infection because exposed individuals will be quarantined more quickly, the exposed will need further help. Currently, of the 17 chemical, 30 biological, and 10 toxic agents listed as the most dangerous by the CDC, 21 have known manufactured vaccines or treatments, four have known vaccines no longer in production, five have vaccines that are unlicensed in the United States, six have vaccines or treatments currently undergoing laboratory research, and 21 have no vaccine or treatment options at all. *Small-Scale Terrorist Attacks Using Chemical and Biological Agents: An Assessment Framework and Preliminary Comparisons*, CONG. RESEARCH SERV., May 20, 2004, at 57-79. That means of 57 agents, 36 lack licensed and currently produced vaccines or treatments. The Bush administration has made the development and manufacture of new vaccines and treatments a high priority through the BioShield Act, and that focus must be maintained. *Project BioShield*, CONG. RESEARCH SERV., May 10, 2004.

<sup>387</sup> The technology to extract and digitize an individual’s DNA exists today, as does the technology to extract and digitize the genetic fingerprint of a given pathogen. What is needed now is small scale ER and mobile instruments that can accomplish this task quickly, accurately, and at minimal expense. Programs also need to be established to research smaller, less expensive alternatives.

<sup>388</sup> The U.S. government currently has in place the infrastructure to manage such a massive undertaking. Beginning in 1986, the Human Genome Project has been coordinated by the National Institute of Health (NIH) and the Department of Energy. For more information see <http://www.ornl.gov/hgmis>. The NIH has granted federal funds to public and private research laboratories performing genetic research. NIH scientists have then reviewed grant proposals from the individual laboratories and apportioned further funds, while also standardizing the methods the laboratories used to report their findings. *Id.* The research needed to create the national DNA database is strikingly similar to that used in the initial Human Genome Project. The NIH already has on record those laboratories whose research was the most useful and economically efficient; it should be able to use that information in deciding to whom to disseminate federal funds. *Id.* Therefore, given the success of the Human Genome Project, NIH coordination of the Project Zebra database would be highly recommended.

transmit the large amounts of data contained in a given DNA sequence.<sup>389</sup> The CDC's Public Health Information Network (PHIN) has a platform for this type of network already in use — the National Electronic Disease Surveillance System (NEDSS) which uses data standards and common architecture to communicate data on infectious diseases.<sup>390</sup> The system is currently used in 19 states to transmit data on infectious diseases from member states to the CDC.<sup>391</sup> Given the CDC's current role as the watchdog of national health, it would be appropriate for Project Zebra's database to be housed within one of the CDC's systems.

It is also essential that practices be standardized to guarantee that each patient is tested and diagnosed correctly. Therefore, the proper operation of Project Zebra would require a nationwide training program for emergency room staff similar to the American Heart Association's Advanced Cardiac Life Support (ACLS), which is updated on a regular basis.<sup>392</sup> A similarly dynamic program must be provided for the medical management of victims exposed to hazardous materials, including victims of bioterrorism. The Advanced Hazmat Life Support Program, a two-day continuing education program cosponsored by the University of Arizona and the American Academy of Clinical Toxicology, is a good example.<sup>393</sup>

### *Laboratory Security*

Another issue discussed at the Subcommittee hearing that caught the attention of Senator Feinstein was laboratory security. Chairman Kyl noted in his opening statement that Dr. Keim's laboratory had a database of 450 unique types of anthrax, which is the world's largest collection of anthrax strains.<sup>394</sup> Senator Feinstein asked if security had been tightened at research facilities.<sup>395</sup> Dr. Keim stated that his lab had "very good security before September 11" and that after September 11, the lab "voluntarily increased [its] security tremendously."<sup>396</sup>

---

<sup>389</sup> The database should be housed in a secure location and controlled by computers powerful enough to compare a patient's DNA with the entire database and render a diagnosis quickly. This would also allow the outbreak of any illness, or the onset of any bioterror attack, to be monitored automatically from one government office rather than at numerous local emergency rooms. Hearing of May 11, 2004, at 44, 46 (written statement of Harvey Meislin).

<sup>390</sup> For more information see <http://www.cdc.gov/programs/research12.htm>.

<sup>391</sup> For more information see <http://www.cdc.gov/programs/research12.htm>.

<sup>392</sup> Hearing of May 11, 2004, at 7 (statement of Harvey Meislin).

<sup>393</sup> The Advanced Hazmat Life Support Program is an international event cosponsored by the University of Arizona Emergency Medical Research Center and the American Academy of Clinical Toxicology, and features experts on everything from community response, to ER decontamination, to specific agents and their effects and hazards. Dr. Meislin spoke very highly of the program in his testimony. Hearing of May 11, 2004, at 7.

<sup>394</sup> Hearing of May 11, 2004, at 2 (statement of Jon Kyl).

<sup>395</sup> Hearing of May 11, 2004, at 13 (statement of Dianne Feinstein).

<sup>396</sup> Hearing of May 11, 2004, at 13 (statement of Paul Keim).

The issue has long concerned the Subcommittee. In January 2003, Chairman Kyl and Senator Feinstein wrote to the Department of Health and Human Services (HHS) to question its plans to delay new security requirements for laboratories working with deadly pathogens. As a result of the Subcommittee hearing and Dr. Keim's testimony, Senator Feinstein wrote another letter to the HHS on June 22, 2004 asking that the Department work with the Inspector General to ensure that reviews of laboratories are conducted promptly and that she be informed of the progress.

On November 16, 2004, HHS responded to Senator Feinstein's letter. HHS explained, "All 316 of these registered entities [labs] have been inspected by HHS/CDC's Select Agent Program . . . These inspections revealed minor deficiencies at some institutions that have either been corrected, or are in the process of being corrected."<sup>397</sup> On December 23, 2004, Senator Feinstein wrote a follow-up letter to the Inspector General of HHS, asking the Inspector General to assess the security of laboratories and other entities.<sup>398</sup> The Subcommittee will continue to monitor this matter.

### *A Vast Undertaking*

Dr. Meislin said at the hearing, "The science and technology necessary to accomplish these goals is within our grasp. This is not an academic exercise. We can develop these tools and achieve a level of practicality that will be valued everyday by the individuals treated in the healthcare system."<sup>399</sup>

A recent *Washington Post* article claimed that despite progress, the United States remains "woefully" unprepared for a bioterrorist attack.<sup>400</sup> At the same time, the article acknowledged the enormity of the undertaking and the progress made thus far. Citing a study by the University of Pittsburgh Medical Center's Biosecurity Center, the *Post* article stated, "The Bush administration has sharply stepped up biodefense efforts. Spending has increased 18-fold since the Sept. 11, 2001 attacks, from \$414 million in fiscal 2001 to a proposed \$7.6 billion this year."<sup>401</sup> Anthony S. Fauci, head of biodefense research at NIH, stated that the government "is

---

<sup>397</sup> Letter from Tommy G. Thompson, Secretary, U.S. Dep't of Health and Human Services, to Dianne Feinstein, U.S. Senator (Nov. 16, 2004) (on file with the Senate Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary).

<sup>398</sup> Letter from Dianne Feinstein, U.S. Senator, to Daniel Levinson, Inspector General, Dep't of Health and Human Services (Dec. 23, 2004) (on file with the Senate Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary).

<sup>399</sup> Hearing of May 11, 2004, at 49 (written statement of Harvey Meislin).

<sup>400</sup> John Mintz and Joby Warrick, *U.S. Unprepared Despite Progress, Experts Say*, WASH. POST, Nov. 8, 2004, at A01.

<sup>401</sup> John Mintz and Joby Warrick, *U.S. Unprepared Despite Progress, Experts Say*, WASH. POST, Nov. 8, 2004, at A01.

on wartime footing” and that people who claim that progress is not being made do not realize how long it takes to make a vaccine.<sup>402</sup> He stressed, “This is light speed . . . . Usually vaccines can take many years or decades.”<sup>403</sup>

Administration officials argue that “most gaps in the U.S. biological defenses result from the sheer vastness of the task ahead — radically transforming entire sectors of society to mount defenses.”<sup>404</sup> In every area where critics point out weaknesses, the administration has made progress.<sup>405</sup> Stewart Simpson, Assistant HHS Secretary for Public Health Emergency Preparedness, stated, “[t]here is no comparison between where we are today and where we were before 9/11.”<sup>406</sup>

## DOMESTIC SECURITY

### Wahhabism

#### *An Extremist Ideology*

To better understand our enemy in the war on terrorism, the Subcommittee convened a series of three hearings to examine the nature of the international terrorist movement. The first hearing in this series focused on a sect of Islam that provides the ideology, recruitment, training, and support infrastructure for today’s international terrorists.<sup>407</sup> This extremist sect is Wahhabism — named for its founder Muhammad ibn Abd al-Wahhab.<sup>408</sup> All 19 of the September 11 suicide hijackers were Wahhabi followers. Fifteen of the 19 were Saudi nationals.

Throughout the Subcommittee’s hearings, Senators were careful to differentiate between

---

<sup>402</sup> John Mintz and Joby Warrick, *U.S. Unprepared Despite Progress, Experts Say*, WASH. POST, Nov. 8, 2004, at A01.

<sup>403</sup> John Mintz and Joby Warrick, *U.S. Unprepared Despite Progress, Experts Say*, WASH. POST, Nov. 8, 2004, at A01.

<sup>404</sup> John Mintz and Joby Warrick, *U.S. Unprepared Despite Progress, Experts Say*, WASH. POST, Nov. 8, 2004, at A01.

<sup>405</sup> John Mintz and Joby Warrick, *U.S. Unprepared Despite Progress, Experts Say*, WASH. POST, Nov. 8, 2004, at A01.

<sup>406</sup> John Mintz and Joby Warrick, *U.S. Unprepared Despite Progress, Experts Say*, WASH. POST, Nov. 8, 2004, at A01.

<sup>407</sup> *Terrorism: Growing Wahhabi Influence in the United States: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 1<sup>st</sup> Sess. (June 26, 2003) (S. Hrg. 108-267, Serial No. J-108-21) [hereinafter “Hearing of June 26, 2003”].

<sup>408</sup> See generally BERNARD LEWIS, *THE CRISIS OF ISLAM: HOLY WAR AND UNHOLY TERROR*, at 121-164 (2003).

Wahhabi extremism (and its ties to terrorism) and the vast majority of Muslims who peacefully practice their faith. For example, Chairman Kyl in opening the hearings said:

Analyzing Wahhabism means identifying the extreme element that, although enjoying immense political and financial resources thanks to support by a sector of the Saudi state, seeks to globally hijack Islam, one of the world's three great Abrahamic faiths. It means understanding who our worst enemies are, and how we can support the majority of the world's Muslims — ordinary, normal people who desire to live in a safe, secure, and stable environment — in their own effort to defeat terror. In the end, Islamist terror must be defeated, to a significant extent, within Islam, by Muslims themselves.<sup>409</sup>

Senator Charles Schumer (D-NY) described the purpose of the hearings:

Mr. Chairman, by holding these hearings . . . you are doing what is necessary to ensure that we do not look back after the next terrorist attack and say, “Why did we not stop it when we had the chance?” My worry is that the Saudis, and many in this administration, are not heeding these warning signs. My worry is, by not heeding these signs, we are once again letting those who hate freedom recruit disciples in our country that might potentially do us harm. My fear, Mr. Chairman, in conclusion is that if we do not wake up and take action now, those influenced by Wahhabism's extremist ideology will harm us in, as of yet, unimaginable ways.<sup>410</sup>

### *The Spread of Wahhabism and the Threat from Al Qaeda*

Prior to the hearing, the Subcommittee gathered a great deal of information about the spread of Wahhabism. According to the noted scholar of Islam, Bernard Lewis, Saudi oil revenues have “allowed the Saudis to spread this fanatical, destructive form of Islam all over the Muslim world and among the Muslims in the West. Without oil and the creation of the Saudi kingdom, Wahhabism would have remained a lunatic fringe.”<sup>411</sup> Al Qaeda, a Wahhabi-influenced movement, has succeeded in penetrating the United States. For example, Evan Thomas wrote in *Newsweek*:

To foil the heightened security after 9/11, Al Qaeda began to rely on operatives who would be harder to detect. They recruited U.S. citizens or people with legitimate Western passports who could move freely in the United States. They used women and family members as “support personnel.” And they made

---

<sup>409</sup> Hearing of June 26, 2003, at 2 (statement of Jon Kyl).

<sup>410</sup> Hearing of June 26, 2003, at 6-7 (statement of Charles Schumer).

<sup>411</sup> Michael Steinberger, *Fundamental Truths, Bernard Lewis, 85 Year-Old Scholar of Arab World and Unlikely Media Star Shares His New Found Celebrity with Michael Steinberger*, FIN. TIMES (London), Aug. 10, 2002, at P3.

an effort to find African-American Muslims who would be sympathetic to Islamic extremism. Using “mosques, prisons and universities throughout the United States,” according to the documents, [Khalid Sheikh Mohammed (KSM), the former Al Qaeda director of global operations who was captured in Pakistan last March] reached deep into the heartland, lining up agents in Baltimore, Columbus, Ohio, and Peoria, Ill. The Feds have uncovered at least one KSM-run cell that could have done grave damage to the United States.<sup>412</sup>

### *Epicenter of Terrorist Financing*

The Subcommittee’s concerns about Al Qaeda’s link to Saudi Arabia and access to Saudi financing were proven to be well-founded. At the hearing, Larry Mefford, Assistant Director of the FBI’s Counterterrorism Division, and David Aufhauser, former General Counsel of the Treasury Department, testified to the well-organized, foreign-funded terrorist infrastructure that is supported both in the United States and globally. Mr. Mefford warned that the “Al Qaeda terrorist network remains the most serious threat to U.S. interests both here and overseas.”<sup>413</sup> Mr. Aufhauser, who tracked terrorist financing networks, testified that Saudi Arabia is the “epicenter” of terrorist financing.<sup>414</sup>

Two scholars, Dr. Alex Alexiev of the Center for Security Policy, and Stephen Schwartz of the Foundation for the Defense of Democracies, testified that Wahhabism is an extreme form of Islam that distorts Muslim teachings, has been Saudi Arabia’s sole state-sanctioned religion for more than two centuries, and advocates violence against non-Muslims and against the peaceful majority of Muslims who consider Wahhabism an aberration.<sup>415</sup>

## **Saudi Arabia**

### *Connecting the Dots*

The second in the series of hearings occurred on the eve of the second anniversary of the

---

<sup>412</sup> Evan Thomas, *Al Qaeda in America: The Enemy Within*, NEWSWEEK, June 23, 2003, at 40, 42.

<sup>413</sup> Hearing of June 26, 2003, at 10 (statement of Larry Mefford).

<sup>414</sup> Hearing of June 26, 2003, at 12 (statement of David Aufhauser). This view of Saudi Arabia was confirmed later in the year by *U.S. News & World Report*, which ran a cover story announcing that a five-month investigation by *U.S. News* found that “[o]ver the past 25 years, the desert kingdom has been the single greatest force in spreading Islamic fundamentalism, while its huge, unregulated charities funneled hundreds of millions of dollars to jihad groups and [A]l Qaeda cells around the world . . . Al Qaeda, says William Wechsler, the task force director [of the CIA’s Illicit Transactions Group], was ‘a constant fundraising machine.’ And where did it raise most of those funds? The evidence was indisputable: Saudi Arabia.” David E. Kaplan *et al.*, *The Saudi Connection*, U.S. NEWS & WORLD REP., Dec. 15, 2003, at 18. The story also noted that “[t]he charities were part of an extraordinary \$70 billion Saudi campaign to spread their fundamentalist Wahhabi sect worldwide.” *Id.* at 20.

<sup>415</sup> Hearing of June 26, 2003, at 14, 17, 20 (statements of Alex Alexiev and Stephen Schwartz).

September 11 terrorist attacks.<sup>416</sup> One week before the hearing, an FBI official warned of the presence of active Al Qaeda cells in 40 states.<sup>417</sup> Chairman Kyl set forth the hearing's objective:

The Terrorism Subcommittee is gathered here today to do its part to ensure that Americans are not attacked again. Defense of our people and our way of life at home requires that law enforcement agencies, members of Congress, and the government at large take an offensive approach to trace the roots of terror and terrorist financiers overseas and here in the U.S. homeland . . . To defeat this threat, we must improve our ability to "connect the dots" between terrorists and their supporters and sympathizers.<sup>418</sup>

Additionally, in his opening statement, Chairman Kyl commented that he was troubled by "the presence of radical Islamist groups and cells here in the United States that often have the support financially, ideologically, and even diplomatically, of the Saudi regime."<sup>419</sup> He noted that Saudi Arabia has a deep historical and symbiotic relationship with the radical Islamist ideology of Wahhabism and that the Saudis continue aggressively to export this intolerant, violent form of Islam to Muslims across the globe, and to inculcate it in the major institutions of Islam worldwide.<sup>420</sup> In his opening statement, Senator Schumer expressed a similar view: "Experts agree that Saudi Arabia is the epicenter of Wahhabist belief and its extremist teachings."<sup>421</sup>

The Subcommittee heard testimony from two witnesses. First, Simon Henderson — a veteran journalist, founder of Saudi Strategies, and respected expert on the Saudi royal family

---

<sup>416</sup> *Terrorism: Two Years After 9/11, Connecting the Dots: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 1<sup>st</sup> Sess. (Sept. 10, 2003) (transcript) [hereinafter "Hearing of Sept. 10, 2003"].

<sup>417</sup> Eric Lichtblau, *Al Qaeda Still Active in U.S., Counterterrorism Official Says*, N.Y. TIMES, Sept. 5, 2003, at A11.

<sup>418</sup> Hearing of Sept. 10, 2003, at 1 (written statement of Jon Kyl). In late July, Special Agent John Pistole, Acting Assistant Director for Counterterrorism for the FBI, said that the "jury [was] still out" on whether Saudi Arabia was fulfilling its promises to combat terrorist financing. Linda Robinson *et al.*, *What's in the Report?*, U.S. NEWS & WORLD REP., Aug. 11, 2003, at 20 (quoting statement of John Pistole before the Senate Governmental Affairs Committee).

<sup>419</sup> Hearing of Sept. 10, 2003, at 4 (transcript) (statement of Jon Kyl).

<sup>420</sup> Hearing of Sept. 10, 2003, at 3 (written statement of Jon Kyl). The U.S. Commission on International Religious Freedom similarly expressed concern about "numerous credible reports that the Saudi government and members of the royal family directly and indirectly fund the global propagation of an exclusivist religious ideology, Wahhabism, which allegedly promotes hatred, intolerance, and other abuses of human rights, including violence. The concern is not about the propagation of Islam *per se*, but about allegations that the Saudi government's version of Islam promotes abuses of human rights, including violent acts, against non-Muslims and disfavored Muslims." U.S. Comm'n on Int'l Religious Freedom, *Report on Saudi Arabia*, May 2003, at 13.

<sup>421</sup> Hearing of Sept. 10, 2003, at 15 (transcript) (statement of Charles Schumer).

and related Middle Eastern subjects<sup>422</sup> — exposed a history of activity in Saudi Arabia that led to its current role as a financier of terrorism. He described a number of Saudi entities, some run by the government, that are involved in global terrorist financing.<sup>423</sup> Mr. Henderson testified that the Saudis send billions of dollars each year to spread Wahhabism throughout the world and that<sup>424</sup> some of this money is funneled through Islamic charities linked to Al Qaeda.<sup>425</sup>

Matthew Epstein — a terrorism expert, a lawyer specializing in terror financing, and Assistant Director of Research with the Investigative Project in Washington, D.C. — described the network of American Muslim organizations, many of them recipients of the Saudi largesse described by Mr. Henderson. Mr. Epstein highlighted Saudi Arabia's long history of sympathy and support for terrorist groups.<sup>426</sup> As an example, he described the Council on American-Islamic Relations (CAIR).<sup>427</sup> Mr. Epstein testified that CAIR, which has publically expressed support for Hamas, receives hundreds of thousands of dollars from Saudi individuals and organizations.<sup>428</sup> Most recently, CAIR officers have been indicted on terrorism-related charges.<sup>429</sup>

### *Saudis Playing a Double Game*

The government of Saudi Arabia must do more to help the United States win the war on terrorism. Consider the following:

---

<sup>422</sup> Mr. Henderson, a journalist with the *Financial Times* of London, covered the 1978 Iranian revolution and the 1979 hostage crisis. He has written a biography of Saddam Hussein, *Instant Empire: Saddam Hussein's Ambition for Iraq*, and a widely praised study of the Saudi royal family, *After King Fahd: Succession in Saudi Arabia*. In addition, Mr. Henderson completed a three-year term on the Council of Chatham House, the Royal Institute of International Affairs.

<sup>423</sup> Hearing of Sept. 10, 2003, at 6-12 (written statement of Simon Henderson).

<sup>424</sup> Hearing of Sept. 10, 2003, at 24 (transcript) (statement of Simon Henderson).

<sup>425</sup> Hearing of Sept. 10, 2003, at 7-8, 10 (written statement of Simon Henderson).

<sup>426</sup> Hearing of Sept. 10, 2003, at 1-2 (written statement of Matthew Epstein).

<sup>427</sup> Members of CAIR were invited to testify at the Subcommittee hearing so that the organization could refute the serious allegations concerning its funding, ideology, leadership, and foreign and domestic networks. CAIR declined the Subcommittee's invitation, but submitted a statement for the record. See Hearing of Sept. 10, 2003 (written statement of Nihad Awad). Also, Matthew Levitt, a Senior Fellow in Terrorism Studies at the Washington Institute for Near East Policy and a former FBI terror analyst, submitted written testimony entitled, *Subversion from Within, Saudi Funding of Islamic Extremist Groups: Undermining U.S. Interests and the War on Terror from Within the United States*. Mr. Levitt noted that "the foreign funding of subversive domestic organizations [in the United States] linked to designated terrorist groups poses immediate dangers to the national security of the United States." Hearing of Sept. 10, 2003, at 9 (written statement of Matthew Levitt).

<sup>428</sup> Hearing of Sept. 10, 2003, at 34 (transcript) (statement of Matthew Epstein).

<sup>429</sup> Hearing of Sept. 10, 2003, at 34 (transcript) (statement of Matthew Epstein).

- From 1973 through 2002, the Saudi Kingdom spent \$87 billion to promote Wahhabism abroad, according to the estimated of Reza F. Safa, the author of *Inside Islam*.<sup>430</sup>
- MSNBC reported that members of the Saudi royal family met with, and paid homage to, Osama bin Laden both before and after the September 11 attacks.<sup>431</sup>
- According to a task force commissioned by the Council on Foreign Relations, a leading U.S. foreign policy think tank, “[f]or years, individuals and charities based in Saudi Arabia have been the most important source of funds for [A]l-Qaeda. And for years, Saudi officials have turned a blind eye to this problem.”<sup>432</sup>

As Peter Beinart, editor of the *New Republic*, said, “There are . . . elements connected to the Saudi government that have been supporting [A]l Qaeda . . . . [T]he Saudis for a long time have been playing a very dangerous double game. It has to stop if we’re going to stop seeing these terrorist attacks.”<sup>433</sup> In a *Washington Post* op-ed, Chairman Kyl and Senator Schumer voiced a similar view:

The House of Saud has for decades played a double game with the United States, on the one hand acting as our ally, on the other supporting a movement — Wahhabism — that seeks our society’s destruction. Because of other strategic interests, our government has long indulged the Saudis, overlooking their financial and structural ties to one of the world’s most violent terror organizations. After the attacks of 9/11, President Bush made clear that he would no longer play that game. He said: “Every nation will have a choice to make: Either you are with us, or you are with the terrorists.”<sup>434</sup>

### *Ending the Double Game*

---

<sup>430</sup> RACHEL EHRENFELD, *FUNDING EVIL: HOW TERRORISM IS FUNDED AND HOW WE CAN STOP IT* 175 (2003).

<sup>431</sup> Andrea Mitchell, *How Strong Are Saudi-al-Qaida Ties?* (MSNBC television broadcast, Sept. 4, 2003) (“Two years after Osama bin Laden gave the final order to attack the World Trade Center, current and former U.S. officials tell NBC News, members of the Saudi royal family met frequently with bin Laden, both before and after 9/11”).

<sup>432</sup> Terrorist Financing Report, Oct. 2002, at 1. *See also* Lisa Beyer and Scott MacLeod, *Inside the Kingdom*, TIME, Sept. 15, 2003, at 38, 43 (“the Saudis have offered only ‘selective cooperation’ on the financial front, according to a senior U.S. official” and “[o]ne of the Administration’s top counterterrorism officials says the Saudis still appear to be protecting charities associated with the royal family and its friends”).

<sup>433</sup> *Buchanan and Press* (MSNBC television broadcast, May 13, 2003); *cf.* Jim Hoagland, *Can Anything Change the Saudi Syndrome?*, WASH. POST, Dec. 18, 2003, at A23.

<sup>434</sup> Jon Kyl and Charles Schumer, *Saudi Arabia’s Teachers of Terror*, WASH. POST, Aug. 18, 2003, at A19 (quoting President George W. Bush, Address to Joint Session of Congress, 147 CONG. REC. S9553 (daily ed. Sept. 20, 2001)).

Chairman Kyl urged the government of Saudi Arabia to take four steps to end the double game<sup>435</sup>:

- **Acknowledge the Problem:** Acknowledge that there exists a significant terrorist movement, including terrorist cells, on its soil. Also admit that Wahhabi financing of mosques and schools — and the teachings disseminated therein — have a direct relation to violent acts of terrorism around the world.
- **Cooperate:** The Saudi government must immediately and fully cooperate with U.S. requests for law enforcement assistance and intelligence sharing, including allowing U.S. investigators access to individuals suspected of terrorist involvement. It must proactively apprehend and turn over to U.S. authorities individuals known to be involved in or who have carried out terrorist plots against the United States.
- **Investigate Suspected Sources of Terrorist Financing:** The Saudi government must regulate charities under Saudi control, especially those with branches disbursing funds abroad. Crucial to this is an examination of the *hawala* system, an underground banking system which permits money transfers without actual wire transfers, making the system susceptible to abuse by terrorists. Registration, licensing, and record keeping would go far to discourage illicit *hawala* activities. And Saudi efforts must be closely coordinated with American and other international endeavors.
- **Attack Incitement to Terrorism:** The Saudi Kingdom must curtail all activities that reward “martyrdom,” and that instill hatred toward the West and toward those whom the extremists have branded as “infidels.” Specifically, this means adopting measures to stop clerics who incite terrorism. It means ceasing its prison *dawa*, or recruitment program in the United States.

### **Radical Islamist Influence of the Chaplaincy of the U.S. Military and Prisons**

#### *Terrorist Exploitation of a Free Society*

For the third hearing in the series, Chairman Kyl directed the Subcommittee to focus on the Wahhabist penetration of two key U.S. institutions: the military and the prison system.<sup>436</sup> As Senator Feinstein noted in her opening statement, “There is cause for concern . . . There are a number of questions that have emerged about how the United States military and the federal

---

<sup>435</sup> *The Need for U.S.-Saudi Cooperation to Win the War on Terrorism*, SENATE REPUBLICAN POL’Y COMM., June 2, 2003, at 14.

<sup>436</sup> *Terrorism: Radical Islamic Influence of Chaplaincy of the U.S. Military and Prisons: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 1<sup>st</sup> Sess. (Oct. 14, 2003) (S. Hrg. 108-443, Serial No. J-108-44) [hereinafter “Hearing of Oct. 14, 2003”].

prisons select chaplains and who sponsors those individuals.”<sup>437</sup> She went on to describe the dismissal of the head Muslim chaplain for New York’s state prisons, “who abused his position to promote Islamic Radicalism there.”<sup>438</sup> According a report in the *Wall Street Journal*, the chaplain stated that prison “is the perfect recruitment and training ground for radicalism and the Islamic religion” and that the September 11 hijackers should be honored as martyrs.<sup>439</sup>

Media reports preceding the hearing noted that the two accrediting organizations that recommend Muslim chaplains to the military — the Graduate School of Islamic and Social Sciences and an organization under the umbrella of the American Muslim Foundation<sup>440</sup> — have long been suspected of having links to terrorist organizations.<sup>441</sup> Another group accused of having ties to Islamic extremists — the Islamic Society of North America — refers Muslim clerics to the U.S. Bureau of Prisons.<sup>442</sup>

Shortly before the hearing, one of the key architects of the U.S. military’s chaplain program, Abdurahman Alamoudi, was arrested and charged with an illegal relationship with Libya, a longtime state sponsor of terror.<sup>443</sup> Earlier, Jose Padilla, a terrorist accused of trying to build a “dirty bomb” to use in the United States, and who had been exposed to radical Islam in the U.S. prison system, also was arrested.<sup>444</sup> And Richard Reid, the so-called “shoe bomber,” who converted to fundamentalist Islam while serving time in a British prison, also had been

---

<sup>437</sup> Hearing of Oct. 14, 2003, at 3, 4 (statement of Dianne Feinstein).

<sup>438</sup> Hearing of Oct. 14, 2003, at 3 (statement of Dianne Feinstein).

<sup>439</sup> Paul Barrett, *Criminal Fifth Column*, WALL ST. J., Feb. 5, 2003, available at <http://www.frontpagemag.com/Articles/ReadArticle.asp?ID=5984>.

<sup>440</sup> American Muslim Armed Forces and Veterans Affairs Council.

<sup>441</sup> See Laurie Goodstein, *Pentagon Says It Will Review Chaplain Policy*, N.Y. TIMES, Sept. 28, 2003, Sec. 1, at 1.

<sup>442</sup> See Michael Kilian, *Guantanamo Translator Held as a Spy*, CHI. TRIB., Sept. 24, 2003, at C1.

<sup>443</sup> Douglas Farah and John Mintz, *U.S. Charges Activist Over Links to Libya; Muslim Leader Lobbied on Sanctions*, WASH. POST, Sept. 30, 2003, at A01. Alamoudi was detained by British authorities in London as he was about to board a plane for Syria, another state sponsor of terror, with \$340,000 in his suitcase. *Id.* Prosecutors charged Alamoudi with illegally accepting money from Libya, and also alleged that he had attempted to funnel \$340,000 to terrorists in Syria. Douglas Farah, *U.S. Says Activist Funded Terrorists; Leader of Muslim Groups Denied Bail*, WASH. POST, Oct. 1, 2003, at A06. Alamoudi is currently awaiting trial in a Virginia jail. Mary Beth Sheridan & Douglas Farah, *Jailed Muslim Had Made a Name in Washington; Alamoudi Won Respect as a Moderate Advocate*, WASH. POST, Dec. 1, 2003, at A01. Alamoudi was a vocal supporter of terrorist groups such as Hamas and Hezbollah. *Id.* But in the years before his arrest, Alamoudi had met with senior U.S. government officials to create the Islamic chaplain program, and also founded a group to recommend young Muslims to serve as clerics. *Id.*

<sup>444</sup> Bob Drogin *et al.*, *The Nation: “Dirty” Bomb Probe Widens; Terrorism: A Suspect Is Interrogated in Pakistan: Officials Say Plot May Have Involved an Effort to Steal Nuclear Material from a University Lab*, L.A. TIMES, June 12, 2002, at A1.

arrested.<sup>445</sup> Noting the actions of Alamoudi, Padilla, and Reid, Chairman Kyl said, “we must understand [the Islamists’] goals, their resources, and their methods, just as well as they understand our system of freedoms and how to exploit them for their terrible purposes . . . We must ‘connect the dots.’”<sup>446</sup>

*Bureau of Prisons and Department of Defense*

On October 14, 2003, the Subcommittee heard testimony from John Pistole, Assistant Director of the Counterterrorism Division of the FBI; Charles Abell, Principal Deputy Under Secretary of Defense for Personnel and Readiness; and Harley Lappin, Director of the Bureau of Prisons.

After noting that the collective assessment of the intelligence community and the FBI was that Al Qaeda remains the greatest terrorist threat to the United States,<sup>447</sup> Mr. Pistole testified that, based on a review of training manuals and interviews with detainees, the FBI believes Al Qaeda is seeking to recruit individuals within the United States.<sup>448</sup> Mr. Pistole added that terrorist groups like Al Qaeda seek to exploit our freedom of religious expression to their advantage by using radical forms of Islam to recruit operatives.<sup>449</sup> U.S. correctional institutions are a prime venue for such radicalization and recruitment.<sup>450</sup> Prison inmates are ostracized and isolated from family and friends, which makes them susceptible to such recruitment.<sup>451</sup>

The hearing elicited information demonstrating that the terrorist threat to the chaplaincy programs is underappreciated by those in charge. For example, the Subcommittee was troubled by responses to questions concerning the funding of the accrediting groups. Senator Feinstein asked, “Do you know who funds [these] organizations? Do you know where the money comes from?”<sup>452</sup> Mr. Abell, Principal Deputy Under Secretary of Defense for Personnel and Readiness replied, “Only what I read in the papers.”<sup>453</sup> Mr. Lappin, Director of the Bureau of Prisons

---

<sup>445</sup> Daniel McGrory *et al.*, *U.K. Mosques Are Prey to Terror*, *TIMES* (London), Dec. 27, 2001, at Home News 1.

<sup>446</sup> Hearing of Oct. 14, 2003, at 2 (written statement of Jon Kyl).

<sup>447</sup> Hearing of Oct. 14, 2003, at 8 (statement of John Pistole).

<sup>448</sup> Hearing of Oct. 14, 2003, at 8 (statement of John Pistole).

<sup>449</sup> Hearing of Oct. 14, 2003, at 8 (statement of John Pistole).

<sup>450</sup> Hearing of Oct. 14, 2003, at 8 (statement of John Pistole).

<sup>451</sup> Hearing of Oct. 14, 2003, at 9 (statement of John Pistole).

<sup>452</sup> Hearing of Oct. 14, 2003, at 17 (statement of Dianne Feinstein).

<sup>453</sup> Hearing of Oct. 14, 2003, at 17 (statement of Charles Abell).

replied, “I am not familiar with who funds them.”<sup>454</sup>

At the hearing, witnesses from the Department of Defense and the Bureau of Prisons conceded that the existing criteria used to select accrediting groups were insufficient.<sup>455</sup> Mr. Abell and Mr. Lappin admitted that they rely on only two groups each to accredit and recommend Muslim chaplains.<sup>456</sup> Mr. Abell testified that the Department of Defense would no longer give these two organizations sole authority to recommend chaplains.<sup>457</sup> He also stated that if an accrediting group was funded by Saudi Arabia and promoted the religious beliefs of Wahhabism, the Department would cease to recognize that group as an acceptable accreditor.<sup>458</sup> Mr. Lappin stated that chaplain candidates would not be hired if they were referred by a group under investigation.<sup>459</sup>

Mr. Abell also testified that on the morning of the hearing, he had signed a Department of Defense memorandum requiring an organization to have IRS 501(c)(3) tax-exempt status before it can certify individuals as chaplains.<sup>460</sup> This is a minor change, unrelated to the terrorist relationship; the Subcommittee was, therefore, concerned that the witness failed to appreciate the steps necessary to fundamentally reform the military’s chaplaincy recruitment program.<sup>461</sup>

Finally, the Subcommittee also heard from Dr. Michael Waller, Annenberg Professor of International Communication at the Institute of World Politics, who testified that foreign states and movements have been financing the promotion of radical, political Islam within America’s armed forces and prisons.<sup>462</sup> He said that this radical sect of Islam preaches extreme intolerance and hatred of American society, culture, government, and the principles enshrined in the U.S. Constitution; it seeks the ultimate overthrow of our Constitution.<sup>463</sup> Dr. Waller pointed out that terrorists have exploited Americans’ religious tolerance, and the chaplain programs in particular, to infiltrate the military and prisons.<sup>464</sup>

---

<sup>454</sup> Hearing of Oct. 14, 2003, at 18 (statement of Charles Abell).

<sup>455</sup> Hearing of Oct. 14, 2003, at 24 (statements of Charles Abell and Harley Lappin).

<sup>456</sup> Hearing of Oct. 14, 2003, at 16-17 (statements of Charles Abell and Harley Lappin).

<sup>457</sup> Hearing of Oct. 14, 2003, at 16 and 17 (statement of Charles Abell).

<sup>458</sup> Hearing of Oct. 14, 2003, at 18 (statement of Charles Abell).

<sup>459</sup> Hearing of Oct. 14, 2003, at 18 (statement of Harley Lappin).

<sup>460</sup> Hearing of Oct. 14, 2003, at 11 (statement of Charles Abell).

<sup>461</sup> Hearing of Oct. 14, 2003, at 14-15 (statement of Jon Kyl).

<sup>462</sup> Hearing of Oct. 14, 2003, at 85 (written statement of Michael Waller).

<sup>463</sup> Hearing of Oct. 14, 2003, at 85 (written statement of Michael Waller).

<sup>464</sup> Hearing of Oct. 14, 2003, at 85 (written statement of Michael Waller).

To identify means for preventing terrorists from continuing to penetrate institutions such as the military and prisons, Chairman Kyl requested briefings after the hearing and asked the Office of the Inspector General at both the Department of Defense and the Justice Department to review the chaplain programs and report back to the Subcommittee with changes in procedures.

## **Bureau of Prisons' Response to the Subcommittee Hearing**

### *Deficiencies in the Chaplaincy Program*

In response to the Subcommittee's October 14, 2003 hearing and a letter from Senator Schumer,<sup>465</sup> the Justice Department's Office of the Inspector General conducted an investigation into the Federal Bureau of Prisons' (BOP) handling of Muslim inmates and religious-service providers.<sup>466</sup> The investigation concluded that the BOP's current system of managing Islamic inmates, contractors, and volunteers presented a continuing security risk, and identified 16 deficiencies, most notably:

1. The BOP and the FBI have not adequately exchanged information regarding Muslim religious service providers and Muslim endorsing organizations.<sup>467</sup>
2. The BOP does not typically examine the doctrinal beliefs of applicants for chaplain positions to determine whether those beliefs are consistent with BOP security policies.<sup>468</sup>
3. Once certain contractors and volunteers gain access to BOP facilities, ample opportunity exists for them to deliver inappropriate and extremist messages without supervision from BOP personnel.<sup>469</sup> Inmates often lead Islamic religious services, subject only to intermittent supervision from BOP staff members, increasing the likelihood that inappropriate content can be delivered to other inmates.<sup>470</sup>

The Office of the Inspector General has twice reviewed the actions taken by the Bureau

---

<sup>465</sup> Letter of March 10, 2003.

<sup>466</sup> U.S. Dep't of Just., Off. of the Inspector Gen., *A Review of Federal Bureau of Prisons' Selection of Muslim Religious Services Providers*, prepared April 2004 [hereinafter "DOJ OIG Report, April 2004"].

<sup>467</sup> DOJ OIG Report, April 2004, at 2.

<sup>468</sup> DOJ OIG Report, April 2004, at 2.

<sup>469</sup> DOJ OIG Report, April 2004, at 3.

<sup>470</sup> DOJ OIG Report, April 2004, at 3.

of Prisons in response to the Inspector General's report.<sup>471</sup> After its second review, the Office of the Inspector General issued a 28-page memo discussing the action taken by the Bureau of Prisons on each of the Inspector General's 16 recommendations. The Office of Inspector General concluded that the Bureau of Prisons has taken specific action to fully address all 16 recommendations.<sup>472</sup>

### *Looking Ahead*

Jose Padilla may be the only current example of a federal inmate radicalized in prison who later attempted to commit terrorist acts. According to the FBI, however, it is likely that terrorist groups such as Al Qaeda will attempt to radicalize and recruit inmates in the United States in the future.<sup>473</sup> It is important, therefore, that the BOP be vigilant maintaining strict compliance with the recommendations made by the Inspector General.

## **Department of Defense's Response to the Subcommittee Hearing**

### *Deficiencies in the Chaplaincy Program*

In response to the Subcommittee's October 14, 2003 hearing<sup>474</sup> and a letter from Senator Schumer,<sup>475</sup> the Department of Defense's Inspector General conducted an investigation into the military's chaplaincy program. The Inspector General was asked to examine the handling of Muslim religious organizations and endorsing agents. The Inspector General chose not to focus

---

<sup>471</sup> U.S. Dep't of Just., Off. of the Inspector Gen., *Office of the Inspector General (OIG) Analysis of Response by the Federal Bureau of Prisons to Recommendations in the OIG's April 2004 Report on the Selection of Muslim Religious Services Providers*, prepared July 9, 2004 (on file with the Senate Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary); U.S. Dep't of Just., Off. of the Inspector Gen., *Office of the Inspector General (OIG) Analysis of Second Response by the Federal Bureau of Prisons to Recommendations in the OIG's April 2004 Report on the Selection of Muslim Religious Services Providers*, prepared Oct. 26, 2004 (on file with the Senate Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary).

<sup>472</sup> Action on of the recommendations was completed on Dec. 10, 2004 and supplied to the Subcommittee on Terrorism, Technology, and Homeland Security (on file with the Senate Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary).

<sup>473</sup> Hearing of Oct. 14, 2003, at 69 (written statement of John Pistole).

<sup>474</sup> *Terrorism: Radical Islamic Influence of Chaplaincy of the U.S. Military and Prisons: Hearing Before the Subcomm. on Terrorism, Technology, and Homeland Security of the Senate Comm. on the Judiciary*, 108<sup>th</sup> Cong., 1<sup>st</sup> Sess. (Oct. 14, 2003) (S. Hrg. 108-443, Serial No. J-108-44) [hereinafter "Hearing of Oct. 14, 2003"].

<sup>475</sup> Letter of March 10, 2003. See U.S. Dep't of Def., Off. of the Inspector Gen., *Crystal Focus: DoD Chaplain Program*, prepared November 2004, at 1 [hereinafter "DoD OIG Report, Nov. 2004"].

on any particular faith group, but, instead, to consider the chaplaincy program in general.<sup>476</sup>

The resulting report was completed on November 15, 2004, over a year after the Subcommittee hearing. The Inspector General's investigation and subsequent report noted the following five observations:<sup>477</sup>

1. A chaplain of any faith is accepted by the Defense Department as long as the chaplain respects religious freedom and agrees to provide services in a pluralistic environment. The Defense Department does not evaluate or review religious doctrine or practices.
2. If a religious organization fails to meet the Defense Department's requirements, the Department does not revoke the organization's ability to endorse chaplains, even though the Department has the power to do so.
3. A religious organization or endorsing agent linked to terrorism remains eligible to provide candidates because the Defense Department does not have nonreligious criteria to disqualify them.
4. If a chaplain fails to maintain professional or ethical standards, the Air Force withdraws the chaplain designation. The Army and Navy have no similar procedures.
5. Defense Department policy requires that any memorandum setting forth new policy be incorporated into formal directives within 180 days. This has not been done with a policy memorandum regarding the tax-exemption requirement discussed at the Subcommittee's hearing.

These observations are discussed more fully below. At the outset, it should be noted, that in a memo dated December 17, 2004, William J. Carr, Acting Deputy Under Secretary (Military Personnel Policy), stated that the Department of Defense concurs with the observations and recommendations made by the Inspector General and will do its best to conform with the spirit of the recommendations. Staff at the Inspector General's Office has informed Subcommittee staff that the Office of the Inspector General will closely monitor the progress of the Department of Defense and will update the Subcommittee.<sup>478</sup>

### *Chaplains of Any Faith*

---

<sup>476</sup> DoD OIG Report, Nov. 2004, at 4.

<sup>477</sup> DoD OIG Report, Nov. 2004, at 12.

<sup>478</sup> Telephone call with John Crane, Assistant Inspector General, Office of Communications and Congressional Liaison, Office of the Inspector General, Department of Defense (Jan. 28, 2005).

Current Defense Department practice allows for the addition of any faith represented by a prospective chaplain who respects religious freedom and agrees to provide services in a pluralistic environment.<sup>479</sup> The Defense Department does not review or evaluate the specific doctrine or practices of each religion. Although the Inspector General discusses this practice, it recommends no changes to the current practice.<sup>480</sup> This is because chaplain program officials assert that specific procedures to review or evaluate religious doctrine or practices could lead to questions concerning constitutional rights to religious freedom.<sup>481</sup>

### *Strengthening The Defense Department's Oversight Role*

According to internal directives, religious organizations must verify that they continue to meet specific requirements.<sup>482</sup> These requirements state that religious organization officers and endorsing agents must update names, addresses, and phone numbers.<sup>483</sup> However, twenty-one of the 196 organizations did not respond to original and follow-up requests to update their information.<sup>484</sup> Although the Defense Department has the authority to revoke recognition of any organization that fails to verify such information, it has not done so.<sup>485</sup> This has weakened the Department's oversight role.<sup>486</sup>

The Inspector General recommends that the Defense Department strengthen its oversight of religious organizations by establishing internal operating procedures to verify compliance by religious organizations with Department requirements; by requiring religious organizations to comply with the verification procedures, which include updating names, addresses, and phone numbers of endorsing agents; and by revoking recognition of all religious organizations that fail

---

<sup>479</sup> DoD OIG Report, Nov. 2004, at 14.

<sup>480</sup> DoD OIG Report, Nov. 2004, at 14.

<sup>481</sup> DoD OIG Report, Nov. 2004, at 14. The Inspector General did not elaborate further on this point. However, a review of the case law by the Department of Justice Office of the Inspector General suggests that the Bureau of Prisons may legally screen all chaplain candidates by asking them questions about their beliefs. *See O'Lone v. Estate of Shabazz*, 482 U.S. 342, 349 (1987); *Hines v. South Carolina Dep't of Corrections*, 148 F.3d 353, 358 (4<sup>th</sup> Cir. 1998); *Mack v. O'Leary*, 80 F.3d 1175, 1180 (7<sup>th</sup> Cir. 1996), *rev'd in part on other grounds*, 522 U.S. 801 (1997); *Winburn v. Bologna*, 979 F. Supp. 531, 535 (W.D. Mich. 1997); *Woods v. Evatt*, 876 F. Supp. 756, 769 (D.S.C. 1995); *Kikumura v. Hurley*, 242 F.3d 950, 962 (10<sup>th</sup> Cir. 2001).

<sup>482</sup> DoD OIG Report, Nov. 2004, at 15.

<sup>483</sup> DoD OIG Report, Nov. 2004, at 15.

<sup>484</sup> DoD OIG Report, Nov. 2004, at 15.

<sup>485</sup> DoD OIG Report, Nov. 2004, at 15.

<sup>486</sup> DoD OIG Report, Nov. 2004, at 15.

to comply.<sup>487</sup>

### *Establishing Screening Procedures and Strengthening Information-Sharing*

Defense Department directives do not provide nonreligious criteria to disqualify either a religious organization or its endorsing agent.<sup>488</sup> As a result, two religious organizations with connections to terrorism and a former endorsing agent indicted on federal charges, remain eligible to provide candidates for the chaplain program.<sup>489</sup> After consulting with the Office of General Counsel, staff at the Defense Department have asserted that the Defense Department cannot perform background checks on religious organizations without the organization's consent.<sup>490</sup> The Defense Department can, however, request a law-enforcement type review in cases of probable cause regarding criminal activity.<sup>491</sup>

The Inspector General recommends that the Defense Department strengthen its screening process by establishing nonreligious criteria to justify withdrawal or removal of a religious organization from participating in the chaplain program.<sup>492</sup> Examples of nonreligious criteria include advocating the violent overthrow of the U.S. government, being listed on a watch list as a terrorist organization, conviction of a religious organization or its principal leaders in connection with terrorism, convictions of endorsing agents in connection with any criminal activity; and conviction of endorsing agents for acts constituting a breach of nonreligious criteria.<sup>493</sup>

The Inspector General also recommends that the Defense Department develop screening procedures for collecting existing information from FBI databases and public sources, and that it develop and impose program sanctions against those religious organizations, or their agents, that fail to meet the criteria in the paragraph above.<sup>494</sup> Additionally, the Inspector General recommends that any specific allegation regarding adverse conduct or behavior of a religious

---

<sup>487</sup> DoD OIG Report, Nov. 2004, at 16.

<sup>488</sup> DoD OIG Report, Nov. 2004, at 17.

<sup>489</sup> DoD OIG Report, Nov. 2004, at 17. The two endorsing agents, the Graduate School of Islamic Social Sciences and the American Muslim Armed Forces and Veterans Association, continue their advisory role despite links to terrorism. *Id.* at 29.

<sup>490</sup> DoD IOG Report, Nov. 2004, at 17-18. The Inspector General's report stated that "privacy laws prohibit disclosure of personal information without the individual's approval." *Id.* at 18. However, the report did not specify which privacy laws.

<sup>491</sup> DoD OIG Report, Nov. 2004, at 18.

<sup>492</sup> DoD OIG Report, Nov. 2004, at 1.

<sup>493</sup> DoD OIG Report, Nov. 2004, at 1.

<sup>494</sup> DoD OIG Report, Nov. 2004, at 1.

organization or endorsing agent be promptly referred to the Inspector General.<sup>495</sup>

After reviewing a previous draft of the Inspector General's report, the Defense Department did not concur with the Inspector General's recommendations.<sup>496</sup> The Acting Deputy Under Secretary of Defense for Military Personnel Policy non-concurred, stating that recommended actions "were legally problematic to the Office of General Counsel."<sup>497</sup> However, these legal objections have not been clarified. The Acting Deputy Under Secretary recommended that "the Treasury's Internal Revenue Service should remain the focal point for *institutional* merit."<sup>498</sup> To make his recommendation executable, the Acting Deputy Under Secretary suggested that "DoD OIG should report its concerns regarding frequency of review of pervious tax-exemption determinations, to the Treasury Inspector General and urge more frequent review as a means of reducing the potential for enriching coffers of those who might post harm to the Nation."<sup>499</sup> Yet, as Chairman Kyl touched on at the hearing and made clear in a meeting with the Inspector General, tax-exempt status is insufficient to screen religious organizations potentially connected to terrorism.<sup>500</sup>

### *Procedures for Removing Chaplains for Cause*

Chaplains receive their designation as a chaplain upon completion of certain accession requirements.<sup>501</sup> Once the designation is received, it can only be removed if the endorsing agent withdraws its endorsement.<sup>502</sup> Therefore, if the Defense Department wants to relieve a chaplain of his responsibilities, it must request that the endorsing agent withdraw its endorsement.<sup>503</sup> This presents two problems. First, for the endorsing agent to withdraw its endorsement, it must know about the nature of the offense. But information regarding an on-going disciplinary process is protected by the Privacy Act.<sup>504</sup> The second problem is that even if the information is provided, the endorsing agent may not agree with the military's assessment and, therefore, refuse to

---

<sup>495</sup> DoD OIG Report, Nov. 2004, at 1.

<sup>496</sup> DoD OIG Report, Nov. 2004, at 20.

<sup>497</sup> DoD OIG Report, Nov. 2004, at 20.

<sup>498</sup> DoD OIG Report, Nov. 2004, at 20 (emphasis in original).

<sup>499</sup> DoD OIG Report, Nov. 2004, at 20.

<sup>500</sup> Memorandum for Under Secretary of Defense for Personnel and Readiness from Deputy Inspector General for Inspections and Policy, Nov. 10, 2004 (included as first page in DoD OIG Report, Nov. 2004).

<sup>501</sup> DoD OIG Report, Nov. 2004, at 22.

<sup>502</sup> DoD OIG Report, Nov. 2004, at 22.

<sup>503</sup> DoD OIG Report, Nov. 2004, at 22.

<sup>504</sup> DoD OIG Report, Nov. 2004, at 22.

withdraw its endorsement.<sup>505</sup> Currently, the Air Force is the only branch that deviates from this policy. It removes chaplains for cause without approval from the endorsing agent.<sup>506</sup>

The Inspector General recommends that the Chiefs of Chaplains of the Army and Navy revise their instructions to address removal or withdrawal of the chaplain designation when that individual fails to uphold professional or ethical standards or is being removed for cause.<sup>507</sup>

The Navy concurred with this recommendation,<sup>508</sup> the Army did not agree.<sup>509</sup> The Army stated that Army policies and personnel procedures provide for adjudication of offenses within the Army's legal and administrative systems.<sup>510</sup> These extant procedures for judicial and non-judicial personnel actions are applicable to all officers including chaplains.<sup>511</sup> The Army argues, "Removal of an officer's designation as chaplain ought not to be punitive or viewed as an initial response to alleged offenses or misconduct. No requirement exists to remove a chaplain's branch designation as a primary response to an alleged offense."<sup>512</sup>

#### *Internal Procedures to Formalize Policy*

The Acting Deputy Under Secretary of Defense for Military Personnel Policy issued a policy memorandum on October 14, 2003 setting forth the tax-exemption requirements discussed at the Subcommittee's hearing.<sup>513</sup> As required by Defense Department Directive 5025.1-M,<sup>514</sup> this memorandum has not been incorporated into formal directives within the required 180 days.<sup>515</sup> As a result, the IRS has no records for 110 of the 196 religious organizations that currently are eligible to endorse Defense Department chaplains.<sup>516</sup>

---

<sup>505</sup> DoD OIG Report, Nov. 2004, at 22.

<sup>506</sup> DoD OIG Report, Nov. 2004, at 23.

<sup>507</sup> DoD OIG Report, Nov. 2004, at 23.

<sup>508</sup> DoD OIG Report, Nov. 2004, at 24, 37.

<sup>509</sup> DoD OIG Report, Nov. 2004, at 24, 36.

<sup>510</sup> DoD OIG Report, Nov. 2004, at 24, 36.

<sup>511</sup> DoD OIG Report, Nov. 2004, at 24, 36.

<sup>512</sup> DoD OIG Report, Nov. 2004, at 24, 36.

<sup>513</sup> DoD OIG Report, Nov. 2004, at 25.

<sup>514</sup> DoD OIG Report, Nov. 2004, at 25.

<sup>515</sup> DoD OIG Report, Nov. 2004, at 25.

<sup>516</sup> DoD OIG Report, Nov. 2004, at 26.

The Inspector General recommends that the new directive be published with the revised policy and instructions to implement the October 14, 2003 policy memorandum and direct the Chaplains Board to conduct outreach with the IRS to ensure successful implementation of the new directive concerning tax-exemption for religious organizations.<sup>517</sup>

*Implementation of All Inspector General Recommendations*

If the Department were to implement the Inspector General's recommendations it would be a substantial step towards increased screening of Muslim religious organizations and endorsing agents. The Department of Defense should take these necessary steps to address the danger of terrorist infiltration of its chaplaincy program.

---

<sup>517</sup> DoD OIG Report, Nov. 2004, at 27.

**APPENDIX A**

**Hearings During the 108<sup>th</sup> Congress**

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

**Border Technology: Keeping Terrorists Out of the United States - 2003**

**(Joint Hearing with the Senate Judiciary Subcommittee on Border Security, Immigration, and Citizenship)**

12 March 2003

**Witnesses:**

The Honorable Asa Hutchinson  
Under Secretary for Border and Transportation  
Department of Homeland Security

Accompanied by:

Mr. Robert Moczynski  
Director of Entry-Exit Program, Bureau of Immigration and Customs Enforcement  
and

Mr. Woody Hall  
Assistant Commissioner  
Office of Information and Technology, Bureau of Customs and Border Protection

Ms. Nancy Kingsbury  
Managing Director of Applied Research and Methods  
Government Accountability Office

Accompanied by:

Mr. Richard Stana  
Director  
Homeland Security and Justice

Mr. Stephen E. Flynn  
Jeane J. Kirkpatrick Senior Fellow in National Security Studies  
Council on Foreign Relations

**Narco-Terrorism: International Drug Trafficking and Terrorism—A Dangerous Mix**

**(Full Judiciary Committee Hearing)**  
20 May 2003

**Witnesses:**

Mr. Steven W. Casteel  
Assistant Administrator for Intelligence  
Drug Enforcement Administration

Mr. Steve McCraw  
Assistant Director  
Office for Intelligence  
Federal Bureau of Investigation

Ms. Deborah A. McCarthy  
Deputy Assistant Secretary of State  
Bureau of International Narcotics and Law Enforcement Affairs  
Department of State

Mr. John P. Clark  
Interim Director  
Office of Investigations  
Bureau of Immigration and Customs Enforcement  
Department of Homeland Security

Mr. Raphael Perl  
Specialist in International Affairs  
Congressional Research Service  
Library of Congress

Mr. Rensselaer W. Lee, III  
President  
Global Advisory Services

Mr. Larry Johnson  
Managing Director  
Berg Associates

**Terrorism: Growing Wahhabi Influence in the United States**  
26 June 2003

**Witnesses:**

Mr. David Aufhauser  
General Counsel

Department of the Treasury

Mr. Larry A. Mefford  
Assistant Director  
Counterterrorism Division  
Federal Bureau of Investigation

Dr. Alex Alexiev  
Distinguished Fellow  
Center for Security Policy

Mr. Stephen Schwartz  
Senior Fellow  
Foundation for Defense of Democracies

**Terrorism: First Responders**

3 September 2003

**Witnesses:**

The Honorable Chris Cox (R-CA)  
Chairman, House Select Committee on Homeland Security  
U.S. House of Representatives

The Honorable Jim Turner (D-TX)  
Ranking Member, House Select Committee on Homeland Security  
U.S. House of Representatives

The Honorable Warren Rudman  
Chair  
Independent Task Force on Emergency Responders

Mr. Richard Clarke  
Senior Adviser  
Independent Task Force on Emergency Responders

Dr. Paul Posner  
Managing Director of Strategic Issues  
Government Accountability Office

**Terrorism: Two Years Afer 9/11, Connecting the Dots**

10 September 2003

**Witnesses:**

Mr. Simon Henderson  
Founder  
Saudi Strategies

Mr. Matthew Epstein  
Attorney  
Terrorism Analyst and Assistant Director of Research  
The Investigative Project

**Terrorism: Radical Islamic Influence of Chaplaincy of the U.S. Military and Prisons**

14 October 2003

**Witnesses:**

Mr. John Pistole  
Assistant Director of Counterterrorism  
Federal Bureau of Investigation

The Honorable Charles Abell  
Principal Deputy Under Secretary for Personnel and Readiness  
Department of Defense

The Honorable Harley Lappin  
Director  
Federal Bureau of Prisons

Dr. Michael Waller  
Annenberg Professor of International Communication  
The Institute of World Politics

Mr. Paul Rogers  
President  
American Correctional Chaplains Association

Mr. A. J. Sabree  
Treasurer  
American Correctional Chaplains Association

**Database Security: Finding Out When Your Information Has Been Compromised**

4 November 2003

**Witnesses:**

Mr. David McIntyre  
President and CEO  
TriWest Healthcare Alliance

Mr. Mark MacCarthy  
Senior Vice President of Public Policy  
Visa U.S.A., Inc.

Mr. Evan Hendricks  
Editor  
Privacy Times

**Confronting the Waterfront — A Review of Seaport Security since September 11, 2001**  
27 January 2004

**Witnesses:**

Mr. Larry Hereth  
Rear Admiral and Director of Port Security  
United States Coast Guard

Mr. Robert M. Jacksta  
Executive Director  
United States Customs and Border Patrol

Mr. Gary M. Bald  
Inspector for the Assistant Deputy Director  
Federal Bureau of Investigation

**Virtual Threat, Real Terror: Cyberterrorism in the 21<sup>st</sup> Century**  
24 February 2004

**Witnesses:**

Mr. John Malcolm  
Deputy Assistant Director  
Department of Justice

Mr. Keith Lourdeau  
Deputy Assistant Director  
Federal Bureau of Investigation

Mr. Amit Yoran  
Director of National Cybersecurity Division

Department of Homeland Security

Mr. Dan Verton  
Author

Mr. Howard Schmidt  
Chief Information Security Officer  
E-bay

**Rapid Bio-Terrorism Detection and Response**

11 May 2004

**Witnesses:**

Dr. Paul Keim  
Director of Pathogen Genomics  
Translational Genomics Research Institute (TGen)  
Cowden Endowed Chair in Microbiology  
Northern Arizona University

Dr. Harvey Meislin  
Director  
University of Arizona Department of Emergency Medicine  
President  
American Board of Medical Specialties

Dr. David A. Relman  
Associate Professor of Medicine  
Stanford University

Dr. Jeffrey Trent  
President  
Translational Genomics Research Institute (TGEN)

**Biometric Passports**

**(Full Judiciary Committee Hearing)**

15 June 2004

**Witnesses:**

The Honorable Asa Hutchinson  
Under Secretary for Border and Transportation  
Department of Homeland Security

The Honorable Maura Harty  
Assistant Secretary for Consular Affairs  
Department of State

**Tools to Fight Terrorism: Subpoena Authority and Pretrial Detention of Terrorists**

22 June 2004

**Witnesses:**

Ms. Rachel Brand  
Principal Deputy Assistant Attorney General  
United States Department of Justice Office of Legal Policy

Mr. Michael Batle  
United States Attorney  
Western District of New York

Mr. James K. Robinson  
Former Assistant Attorney General  
United States Department of Justice Criminal Division

**A Review of the Tools to Fight Terrorism Act**

13 September 2004

**Witnesses:**

The Honorable Daniel J. Bryant  
Assistant Attorney General  
Office of Legal Policy  
Department of Justice

Mr. Barry Sabin  
Chief  
Counterterrorism Section, Criminal Division  
Department of Justice

Professor Jonathan Turley  
Shapiro Professor of Public Interest Law  
George Washington University Law School

## APPENDIX B

### Information for Victims of Identity Theft

There are few clearer violations of personal privacy than having your identity stolen and used in the commission of a crime. Criminals use Social Security numbers and other personal information to assume the identities of law-abiding citizens and steal their money.

Under the Identity Theft Penalty Enhancement Act, which is now law, a conviction for identity theft carries a maximum penalty of 15 years in prison, a fine, and forfeiture of any personal property used or intended to be used to commit the crime.

Violations of the act are investigated by federal law-enforcement agencies, including the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service, and the Social Security Administration's Office of the Inspector General. Federal identity theft cases are prosecuted by the U.S. Department of Justice.

The Federal Trade Commission is authorized to receive complaints about identity theft from consumers who have been victimized. The Commission can help victims of identity theft by providing information to assist them in resolving the financial and other problems that can result from this crime.

If you suspect that your personal information has been stolen, take action immediately. Call the Federal Trade Commission's Identity Theft Hotline toll-free at 1-877-IDTHEFT (438-4338); TDD: 202-326-2502 . The FTC also has a website to help people guard against and recover from identity theft. The site is: <http://www.consumer.gov/idtheft/>. Or you can write to the FTC:

Identity Theft Clearinghouse  
Federal Trade Commission  
600 Pennsylvania Avenue, N.W.  
Washington, D.C. 20580

#### **To minimize your risk of becoming a victim of identity theft, manage your personal information carefully.**

- ▶ Before you reveal any personally identifying information, find out how it will be used and whether it will be shared with others. Ask if you have a choice about the use of your information: Can you choose to have it kept confidential?
- ▶ Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing credit card bill could mean an identity thief has taken over your credit-card account and changed your billing address to cover his tracks.
- ▶ Guard your mail from theft. Deposit outgoing mail only in Post Office collection boxes or at your local Post Office. Promptly remove mail from your mailbox after it has been delivered.
- ▶ Minimize the identification information and the number of cards you carry to what you'll

actually need.

- ▶ Do not give out personal information on the phone, through the mail, or over the Internet unless you have initiated the contact or know who you're dealing with.
- ▶ Keep items with personal information in a safe place.
- ▶ Give your Social Security number only when absolutely necessary.
- ▶ Do not carry your Social Security card; leave it in a secure place.
- ▶ Use a cross-cut shredder to destroy old bank statements, credit-card offers, receipts, and other materials that may include account numbers, Social Security numbers, or other personal financial identifiers.
- ▶ Contact credit-reporting bureaus (Equifax, Experian, and TransUnion) to request that your name be removed from marketing lists. Equifax and TransUnion may be reached by calling 1-888-567-8688. Experian may be reached at 1-888-397-3742.
- ▶ Keep copies of all identification and credit cards. Copy both sides.
- ▶ Order a Social Security Earnings and Benefits statement once a year. You may do so by calling 1-800-772-1213 or by visiting [www.ssa.gov](http://www.ssa.gov) on-line.

## APPENDIX C

### **Avoid Becoming a Victim of “Phishing”**

One of the latest methods of ID theft, known as “phishing,” involves unsolicited e-mails sent to Internet users. The e-mails are designed to look like authentic messages from legitimate businesses, financial institutions, or government agencies. Often marked “URGENT,” the messages lead recipients to believe their accounts will be closed if they do not comply with certain instructions, like disclosing personal information, user names, passwords, and credit card numbers. The messages link recipients to websites that often look legitimate, but are not.

Phishing differs from traditional identity theft in that it is the victim who actually provides the information to the scammer. The Internet addresses of the websites to which victims are directed are purposefully misleading. For example, [billing.yahoo.com](http://billing.yahoo.com) is a legitimate yahoo site, but [yahoo-billing.com](http://yahoo-billing.com) is not and is a website used by phishers.

#### **Steps to Avoid Being “Phished”:**

1. Stop. Phishers prey on your emotions by making you think that you need to respond immediately. They want you to click on a link before you’ve had a chance to think about the content of the message. Take time to read your e-mail carefully before clicking on any links it contains.
2. Look. Carefully examine any claims that are made in your e-mail messages. If they sound too good to be true or ask for personal information, you should be highly suspicious. There is no reason for companies to be asking for your account numbers, user names, passwords, or other personal information.
3. Call. If an e-mail claims to be from a legitimate company or institution with whom you do business, call the phone number listed on your last statement to check the accuracy of the e-mail or, if you cannot find one, send an e-mail to the address given on the company’s or institution’s official website.

#### **Steps to Take if You Receive a Phishing E-mail:**

If you have accidentally submitted your personal information, you should:

1. Immediately file a complaint with the Internet Crime Complaint Center at <http://www.ic3.gov>.
2. Because of your increased risk of becoming a victim of identity theft, you should visit <http://www.consumer.gov/idtheft> and follow the directions for reporting information to credit bureaus, credit-card companies, and law enforcement.

If you have received a phishing e-mail but have not submitted personal information, DO NOT RESPOND. The Department of Justice recommends that you send a copy of the e-mail to [uce@ftc.gov](mailto:uce@ftc.gov) and [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org).

Useful Links:

The Department of Justice's March, 2004 "Special Report on 'Phishing'" can be found at <http://www.usdoj.gov/criminal/fraud/Phishing.pdf>.

Another site, [http://antiphishing.org/phishing\\_archive.htm](http://antiphishing.org/phishing_archive.htm), includes examples of actual phishing e-mails.

## APPENDIX D

### **TOOLS TO FIGHT TERRORISM ACT OF 2004**

#### **Bills Included in TFTA and Congressional Hearings**

TFTA (S. 2679) has five titles, which consist of all or part of 11 bills currently pending in the House and Senate. Every provision of TFTA previously has either been introduced as a bill in the House or Senate or has had a committee hearing. Every provision has the full support of the Justice Department. Collectively, the provisions of TFTA have been the subject of nine separate hearings before House and Senate committees and have been the subject of four separate committee reports. In addition, the entire bill was reviewed in a September 13 hearing before the Senate Subcommittee on Terrorism. At that hearing, Justice Department witnesses Barry Sabin, Chief of the Counterterrorism Section of the Criminal Division, and Dan Bryant, Assistant Attorney General for the Office of Legal Policy, both testified strongly in favor of the bill, and law professor Jonathan Turley testified that every one of TFTA's provisions would be upheld as constitutional by the U.S. Supreme Court. Collectively, as of July 19, 2004 (the day that TFTA was introduced), the bills included in TFTA have been pending before Congress for 12 years, 10 months, and 28 days.

On December 17, 2004, about half of the provisions of TFTA were signed into law by President as part of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458. The TFTA provisions that were enacted into law are: section 102 (Lone Wolf FISA/ Moussaoui fix); section 103 (Pretrial Detention); section 106 (Terrorist and Military Hoaxes); section 107 (Increased Penalties for Obstruction of Justice); section 113 (Grand Jury Information Sharing); section 114 (Material-Support Improvements); section 115 (Military-Type Training Offense and Deportation); section 116 (Expanded WMD Offenses); section 117 (Aiding Rogue States' WMD Development); Title II (possession of dangerous weapons); and section 506 (Concealment of Terrorist Financing). Much of TFTA was enacted in December 2004 as section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (S. 2845)

#### **1. Lone-Wolf FISA Authority (“Moussaoui Fix”)**

Section 102 of TFTA authorizes FISA warrants for lone-wolf terrorists – those involved in international terrorism but not affiliated with a known terrorist group. The same provision was introduced as a bill (S. 2586) by Senators Schumer and Kyl on June 5, 2002. The Senate Intelligence Committee held a hearing on S. 2586 on July 31, 2002. Witnesses included James Baker, Counsel for Intelligence Policy with the Office of Intelligence and Policy Review, Department of State; Marion “Spike” Bowman, Deputy General Counsel, National Security Law Unit, Office of the General Counsel, FBI; and Fred Manget, Deputy General Counsel, CIA.

The same provision was reintroduced in the 108th Congress by Senators Schumer and Kyl as S. 113 on January 9, 2003. S. 113 was unanimously reported by the Judiciary Committee on

March 11, 2003. The Committee issued Report No. 108-40 for S. 113 on April 29, 2003. S. 113 was approved by the Senate by 90-4 on May 8, 2003. The same provision also was included in H.R. 3179, which was introduced by House Judiciary Chairman Sensenbrenner and House Intelligence Chairman Goss on September 25, 2003. The House Subcommittee on Crime, Terrorism, and Homeland Security held a hearing on H.R. 3179 on May 18, 2004. Witnesses at the hearing included Dan Bryant, Assistant Attorney General, Office of Legal Policy, Department of Justice; Thomas Harrington, Deputy Assistant Director, FBI; and Bob Barr, former Congressman. The same provision also was introduced as H.R. 3552 by Representative King on November 20, 2003.

## **2. Presumption of No Bail for Terrorists**

Section 103 would add terrorist offenses to the list of offenses – such as drug crimes – that are subject to the statutory presumption of pretrial detention. Section 104 would make all convicted terrorists – not just those directly involved in violence – eligible for a sentence of lifetime post-release supervision. Both sections are included in H.R. 3040, which was introduced by Representative Goodlatte on September 9, 2003. The same bill was introduced as S. 1606 by Senator Kyl on September 10, 2003. S. 1606 had a hearing before the Senate Subcommittee on Terrorism, Technology, and Homeland Security on June 22, 2004. Witnesses included Rachel Brand, Principal Deputy Assistant Attorney General, Office of Legal Policy, Department of Justice; Michael Battle, U.S. Attorney, Buffalo, NY; and James K. Robinson, former Assistant Attorney General, Criminal Division, Department of Justice.

## **3. FBI Subpoena For Terrorism Offenses**

Section 105 would allow the FBI to subpoena records when investigating terrorism offenses, just as DEA agents can issue subpoenas when enforcing the Controlled Substances Act. Similar authority is provided for in H.R. 3037, which was introduced by Representative Feeney on September 9, 2003. Section 105 is identical to S. 2555, which was introduced by Senator Kyl on June 22, 2004. S. 2555 was the subject of a hearing before the Senate Subcommittee on Terrorism, Technology, and Homeland Security on June 22, 2004. Witnesses included Rachel Brand, Principal Deputy Assistant Attorney General, Office of Legal Policy, Department of Justice; Michael Battle, U.S. Attorney, Buffalo, NY; and James K. Robinson, former Assistant Attorney General, Criminal Division, Department of Justice.

## **4. Punishment for Hoaxes about Terrorism or Deaths of U.S. Soldiers**

Section 106 imposes criminal penalties for conveying false or misleading information – perpetrating hoaxes – about terrorist crimes or the death or injury of a U.S. soldier. The key elements of section 106 were introduced as H.R. 3209 in the 107th Congress by Representative Lamar Smith on November 11, 2001. H.R. 3209 was the subject of a hearing before the House Subcommittee on Crime, Terrorism, and Homeland Security on November 7, 2001. Witnesses included James Jarboe, Section Chief, Counterterrorism Division, Domestic Terrorism, FBI; and James Reynolds, Chief, Terrorism and Violent Crime Section, Criminal Division, Department of Justice. H.R. 3209 was reported by the House Judiciary Committee on November 29, 2001. The Judiciary Committee issued Report No. 107-306 for H.R. 3209 on the same day. H.R. 3209 was unanimously approved by the House of Representatives on December 12, 2001.

A similar provision was introduced as H.R. 1678 in the 108th Congress by Representative Lamar Smith on April 8, 2003. H.R. 1678 was the subject of a hearing before the House Subcommittee on Crime, Terrorism, and Homeland Security on July 10, 2003. Witnesses included Susan Brooks, the U.S. Attorney for the Southern District of Indiana; James McMahon, Superintendent, New York State Police; and Danny Hogg, a target of a war-time hoax about a family member serving in Iraq. H.R. 1678 was ordered reported by the House Judiciary Committee by voice vote on May 12, 2004. The Judiciary Committee issued Report No. 108-505 for H.R. 1678 on May 20, 2004. H.R. 1678 has 10 cosponsors.

The key provisions of sections 106 and 107 were introduced as S. 2204 by Senator Hatch on March 11, 2004. S. 2204 has four cosponsors, including Senators Schumer and Feinstein.

### **5. Confidential Requests for CIPA Protection**

Section 108 allows federal prosecutors to make confidential requests for protection of classified information in a criminal trial under the Classified Information Procedures Act, which allows the court to substitute a summary of the information or an admission of relevant facts. The same provision is included in H.R. 3179, which was introduced by House Judiciary Committee Chairman Sensenbrenner and House Intelligence Committee Chairman Goss on September 25, 2003. The House Subcommittee on Crime, Terrorism, and Homeland Security held a hearing on H.R. 3179 on May 18, 2004. Witnesses at the hearing included Dan Bryant, Assistant Attorney General, Office of Legal Policy, Department of Justice; Thomas Harrington, Deputy Assistant Director, FBI; and Bob Barr, former Congressman.

### **6. Confidential Use of FISA Information in Immigration Proceedings**

Section 109 allows the United States to use information derived from FISA to deny a suspected terrorist or spy an immigration benefit without having to reveal that the information came from a FISA investigation. The same provision is included in H.R. 3179, which was introduced by House Judiciary Chairman Sensenbrenner and House Intelligence Chairman Goss on September 25, 2003. The House Subcommittee on Crime, Terrorism, and Homeland Security held a hearing on H.R. 3179 on May 18, 2004. Witnesses at the hearing included Dan Bryant, Assistant Attorney General, Office of Legal Policy, Department of Justice; Thomas Harrington, Deputy Assistant Director, FBI; and Bob Barr, former Congressman.

### **7. Expanded Death Penalty for Terrorist Murders**

Section 110 makes a convicted terrorist eligible for the death penalty if he participates in an attack that results in death, even if he does not directly participate in killing. Section 111 makes convicted terrorists ineligible for federal benefits. The same provisions were introduced as H.R. 2934 by Representative Carter on July 25, 2003. H.R. 2934 was the subject of a hearing before the House Subcommittee on Crime, Terrorism, and Homeland Security on April 21, 2004. Witnesses included Johnny Sutton, U.S. Attorney, Western District of Texas; Dr. Joanna Shepherd, Visiting Assistant Professor, Emory Law School; and Timothy Edgar, Legislative Counsel, American Civil Liberties Union. H.R. 2934 was ordered reported by the House Judiciary Committee by voice vote on June 23, 2004. The Judiciary Committee issued Report No. 108-588 for H.R. 2934 on July 7, 2004. H.R. 2934 has 84 cosponsors.

The same provisions were introduced as S. 1604 by Senator Specter on September 10, 2003.

### **8. Information Sharing Across Federal Agencies and With State and Local Governments**

Section 112 creates a uniform standard under which the FBI may share information with other federal agencies. Section 113 authorizes the FBI to share grand-jury and national-security information with state and local authorities. The same provisions were introduced as S. 2599 by Senators Chambliss and Kyl on June 24, 2004.

### **9. Providing Material Support and Receiving Military Training from Terrorists**

Section 114 broadens the jurisdictional bases of the material-support statute and more clearly defines the terms “training” and “expert advice or assistance” in order to avoid perceived constitutional overbreadth. Section 115 makes it a crime to receive military-type training from a foreign terrorist group and makes aliens who have received such training inadmissible to and deportable from the United States. The need for a stronger material-support statute and its application to terrorist training camps were the subject of a hearing before the Senate Judiciary Committee on May 5, 2004. Witnesses included Chris Wray, Assistant Attorney General, Criminal Division, Department of Justice; Dan Bryant, Assistant Attorney General, Office of Legal Policy, Department of Justice; Gary Bald, Assistant Director, Counterterrorism Division, FBI; David Cole, law professor, Georgetown University Law Center; and Paul Rosenzweig, Senior Legal Research Fellow, Heritage Foundation.

### **10. Expanded WMD Prohibitions**

Section 116 expands the jurisdictional bases and scope of existing prohibitions on use of weapons of mass destruction, including chemical weapons within the prohibition for the first time. Section 117 expands the scope of existing prohibitions on providing assistance to nuclear proliferation. Sections 116 and 117 are substantially the same as H.R. 2939, which was introduced by Representative Forbes on July 25, 2003, and are identical to S. 2665, which was introduced by Senator Cornyn on July 15, 2004.

### **11. Prevention of Terrorist Access to Special Weapons**

Title II imposes a mandatory minimum sentence of 30 years for possession of shoulder-fired anti-aircraft rockets, atomic weapons, radiological dispersal bombs, and the variola virus, and a mandatory minimum sentence of life for use or possession and threats to use these weapons. Title II is the same as S. 2664, which was introduced by Senator Cornyn on July 15, 2004.

### **12. Attacks Against Railroads and Mass Transportation Systems**

Title III would expand and increase criminal offenses and penalties for attacks on railroad carriers and mass-transportation systems. An early version of Title III was introduced as S. 1608 by Senator Sessions on September 11, 2003. A companion bill, H.R. 4008, was introduced in the House by Representative Shays on March 18, 2004. A revised bill that is the same as Title III was introduced as H.R. 4143 by Representative Capito on April 2, 2004. The same bill was introduced as S. 2289 by Senator Sessions on April 6, 2004. S. 2289 was the subject of a hearing before the Senate Judiciary Committee on April 8, 2004. Witnesses included Harry S. Mattice, U.S. Attorney, Eastern District of Tennessee; Mark Lindsey, Chief Counsel, Federal

Rail Administration, Department of Transportation; Ernest Frazier, Chief, System Security and Safety, National Railroad Passenger Corporation (Amtrak); and Brian Jenkins, Director, National Transportation Security Center, Mineta Transportation Institute, San Jose, CA.

### **13. Seaport Security**

Title IV would create new offenses and broaden and increase penalties for existing offenses for terrorism and other crimes affecting the security of U.S. seaports. The key elements of Title IV first were introduced as S. 746 by Senator Feinstein on March 31, 2003. A companion bill was introduced as H.R. 2376 by Representative Millender-McDonald on June 5, 2003. An updated bill was introduced by Senator Biden as S. 1587 on September 5, 2003. S. 1587 has 11 cosponsors. A further updated bill that is the same as Title IV was introduced as S. 2653 by Senator Biden on July 14, 2003. The Senate Subcommittee on Terrorism, Technology, and Homeland Security held a hearing on the need for improved seaport security on January 27, 2004. Witnesses included Larry Hereth, Rear Admiral, Director of Port Security, U.S. Coast Guard; Robert Jacksta, Executive Director, U.S. Customs and Border Patrol; and Gary M. Bald, Inspector Deputy Assistant Director, FBI.

### **14. Terrorist Financing**

Title V helps undercut financing of terrorism by expanding the list of predicate offenses for money laundering and prohibiting concealing past provision of financing while knowing that it has been or will be provided to terrorists. Title V is substantially the same as S. 1837, which was introduced by Senator Grassley on November 6, 2003. The Senate Judiciary Committee held a hearing on the need to better combat terrorist financing on November 20, 2002. Witnesses included Robert J. Conrad, U.S. Attorney for the Western District of North Carolina; Jimmy Gurulé, Under Secretary for Enforcement, Department of Treasury; David Aufhauser, General Counsel, Department of Treasury; Nathan Lewin, Lewin & Lewin, LLP; Allan Gerson, Professorial Lecturer In Honors, George Washington University; Jonathan Winer, Alston & Bird, LLP (Member, Council on Foreign Relations); Salam Al-Marayati, Executive Director, Muslim Public Affairs Council.

## **Section by Section Analysis**

### **Title I: Anti-Terrorism Investigative Tools Improvement Act of 2004**

*Section 102: FISA Warrants for Lone-Wolf Terrorists (§ 4 of HR 3179; also S. 113) S. 113 passed the Senate by 90-4 in May 2003. H.R. 3179, the Sensenbrenner bill that includes this provision, had a hearing in the House Judiciary Committee.*

This section would amend FISA to allow orders for surveillance of foreign visitors to the U.S. who appear to be involved in international terrorism but are not affiliated with a known terror group. When FISA was enacted in the 1970s, terrorists generally were members of distinct, hierarchical terror groups. Today's Islamist extremists often are not formal members of any group, but rather are part of a movement – and occasionally act alone. FISA authority should be updated to reflect this new threat. This section still requires a judicial finding of probable cause that the target is preparing to engage in international terrorism.

*Section 103: Adding Terrorist Offenses to the Statutory Presumption of No Bail (§ 2 of S. 1606)* S. 1606 had a hearing in the Judiciary Subcommittee on Terrorism, Technology, and Homeland Security.

Under current law, a criminal suspect will be denied bail in federal court if the government shows that there is a serious risk that the suspect will flee, obstruct justice, or injure or threaten a witness or juror. The judge must *presume* this showing is present if the suspect is charged with a crime of violence, a drug crime carrying a potential sentence of ten years or more, any crime that carries a potential sentence of life or the death penalty, or the suspect previously has been convicted of two or more such offenses. This section would add terrorist offenses to this list – judges would be required to presume that facts requiring a denial of bail are present. This is only a presumption – the terror suspect still could attempt to show that he is not a flight risk or potential threat to jurors or witnesses.

*Section 104: Making Terrorists Eligible for Lifetime Post-Release Supervision (§ 3 of S. 1606)* Hearing held.

Under current law, a convicted terrorist is eligible for lifetime post-release supervision only if his offense creates a foreseeable risk of death or serious injury. This would not include a terrorist who mounted a massive computer attack, or who provided key financial support for terrorist acts. Yet such individuals may have a commitment to terrorist goals that is unlikely to dissipate in prison – they should at least be *eligible* for a sentence of lifetime post-release supervision. This section would make all terrorists eligible for lifetime post-release supervision.

*Section 105: Judicially Enforceable Terrorism Subpoenas (§ 2 of S. 2555)* S. 2555 had a hearing in the Judiciary Subcommittee on Terrorism, Technology, and Homeland Security.

This section would allow the FBI to subpoena documents and records “in any investigation of a Federal crime of terrorism.” It would require the FBI to go to federal court to enforce the subpoena in the event that the recipient declines to comply with it. It would also allow the recipient to act first by going to court to challenge the subpoena. This section also would allow the Justice Department to temporarily bar the recipient of a JET subpoena from disclosing to anyone other than his lawyer that he has received it. The FBI could bar such disclosure, however, only if the Attorney General certifies that “otherwise there may result a danger to the national security of the United States.” Also, the recipient of the subpoena would have the right to go to court to challenge the non-disclosure order. And finally, this section would protect the

recipient from any civil liability that might otherwise result from his good-faith compliance with a JET subpoena. FBI Director Mueller has indicated to Senators that having this subpoena authority would be “tremendously helpful” to terrorism investigations.

*Section 106: Punishment of Hoaxes Relating to Terrorist Offenses (§ 2 of S. 2204, by Hatch/Schumer/Cornyn/Feinstein/DeWine)*

This section imposes criminal penalties for knowingly conveying false or misleading information about terrorist crimes or death or injury to a U.S. soldier during war under circumstances where such information may reasonably be believed. The section proscribes hoaxes relating to all terrorist offenses listed in 18 U.S.C. 2332b(g)(5)(B), and allows the death penalty for hoaxes that result in death.

*Section 107: Increased Penalties for Obstruction of Justice in Terrorism Cases (§ 3 of S. 2204)*

This section increases from 5 years to 10 years the penalty for obstruction of justice in terror investigations. It also instructs the Sentencing Commission to increase the guidelines range for making false statements in relation to a terrorism investigation.

*Section 108: Automatic Permission for Confidential Requests for CIPA Protection (§ 5 of H.R. 3179) Hearing held.*

The Classified Information Procedures Act authorizes the government to seek protection for classified information used in a criminal proceeding. The court may order that the defendant not disclose the information, it may allow the information to be redacted or summarized, or it may allow the government to simply admit to those facts which the classified information would tend to prove (without disclosing the information itself to the defendant). Under current law, a court has discretion whether to allow a *request* for CIPA protection to be made ex parte and in camera. This section would *require* courts to allow CIPA requests to be made ex parte and in camera. Such protection for CIPA requests is necessary because the government risks disclosing sensitive national-security information simply by explaining in open court why CIPA protection is necessary. This bill does not affect the showing that the government must make in order to obtain CIPA protection.

*Section 109: Use of FISA Information in Immigration Proceedings (§ 6 of H.R. 3179) Hearing held.*

FISA requires the government to provide notice when information obtained through FISA is used in any federal proceeding. In 1996, Congress created an exception to this requirement for alien-terrorist removal proceedings. This section would extend this exception to all immigration proceedings – the government would be able to use FISA information to deny an alien a particular immigration benefit, to bar his reentry, or to detain him on immigration charges, all without revealing that the information was obtained through FISA. Such authority is necessary because in many instances, notice that information was obtained through FISA would disclose to

the alien that he or his associates have been the target of a FISA investigation – a disclosure that could compromise an ongoing investigation. In a number of instances, the government has declined to use particular information in an immigration proceeding because the government would have been required to reveal the fact of an ongoing FISA investigation.

*Section 110: Expanded Death Penalty for Terrorist Murders (§ 2 of S. 1604)*

This section would authorize the imposition of capital punishment for persons who, “in the course of committing a terrorist offense, engage in conduct that results in the death of a person.” Current law requires that a terrorist directly participate in murder in order to be eligible for the death penalty. This section would treat terrorism in the same way that federal law treats treason: the crime itself is eligible for the death penalty if it results in someone’s death, even if the crime itself does not constitute murder. In effect, the section would allow the death penalty for persons who finance or otherwise assist a fatal terrorist attack, even if they do not directly participate in killing.

*Section 111: Denial of Federal Benefits to Terrorists (§ 3 of S. 1604)*

This section allows a court to deny federal benefits for any term of years or for life to a person convicted of a terrorist offense. The scope of the benefits that can be denied is the same as a parallel provision in the Controlled Substances Act.

*Section 112: Uniform Standards for Sharing Information Across Federal Agencies (§ 2(a)-(e) of S. 2599)*

This section and Section 113 improve the FBI’s ability to share intelligence information that has been obtained under existing authorities. This section creates a uniform standard under which the FBI would disseminate intelligence information to other federal agencies. Under current law, several different statutes govern the circumstances under which the FBI may disseminate intelligence information to other federal agencies. Some of these statutes anomalously place restrictions on information sharing with other federal agencies that are greater than the restrictions applied to non-federal agencies. This section allows dissemination of intelligence information under uniform guidelines developed by the Attorney General.

*Section 113: Authorization to Share National-Security and Grand-Jury Information with State and Local Governments (§§ 2(f) and 3 of S. 2599)*

This section amends current law to make clear that national-security-related information may be shared with relevant federal, state, and local officials regardless of whether the investigation that produced the information is characterized as a “criminal” investigation or a “national security” investigation. This section also would authorize the sharing of grand-jury information with appropriate state and local authorities. This change previously was enacted by the Homeland Security Act, but that change never went into effect because the Federal Rule of Criminal

Procedure amended by the HSA was revised by the Supreme Court shortly after the enactment of the HSA, and the amendment made by HSA presupposed the earlier text of the federal rule.

*Section 114: Providing Material Support to Terrorism* (Hearing held in the Senate Judiciary Committee)

This section amends the current material-support statute by making it a crime to provide material support to any crime of international or domestic terrorism. Federal jurisdiction over material-support offenses would exist when (1) the crime occurs in or affects interstate or foreign commerce; (2) is an existing terrorism offense; (3) is a crime of domestic terrorism designed to affect the policy of the U.S. or a foreign government; (4) when a U.S. citizen, alien of the U.S., or a stateless resident whose habitual residence is in the U.S. commits international terrorism designed to influence U.S. policy or that of a foreign government; (5) an alien offender within the U.S. commits international terrorism intended to influence U.S. policy; (6) an alien offender outside of the U.S. commits an act of international terrorism designed to influence U.S. policy; (7) anyone who aids, abets, or conspires with any person over whom jurisdiction exists under this section to commit a crime identified in this section. This section also amends the definition section of the current statute by more clearly specifying what constitutes material support, including the definition of “training” and “expert advice or assistance.” Finally, this section also amends current law by defining the knowledge required to violate the statute, more specifically defining “personnel,” “training,” and “expert advice,” and specifying that nothing contained in this statute shall be construed to abridge free speech rights.

*Section 115: Receiving Military-Type Training from a Foreign Terrorist Organization* (Hearing held in the Senate Judiciary Committee)

This section makes it a crime to knowingly receive military-type training from or on behalf of a designated foreign terrorist organization. This provision applies extraterritorially to U.S. nationals, permanent residents, stateless persons whose habitual residence is the United States, or a person who is brought into or found in the United States. This section also makes aliens who have received military-type training from a terrorist group, or who are representatives or members of a terrorist group, inadmissible to the United States. Finally, this section makes deportable aliens in the United States who have received military-type training from a terrorist organization.

*Section 116: Expanded Weapons of Mass Destruction Prohibitions* (§ 2 of H.R. 2939)

This section would amend the federal weapons-of-mass-destruction statute to cover attacks on property, and would provide for federal jurisdiction in three new circumstances: (1) if the mail or any facility of interstate or foreign commerce is used in furtherance of the offense; (2) if the attacked property is used in interstate or foreign commerce, or in an activity that affects interstate or foreign commerce; or (3) if any perpetrator travels in or causes another to travel in interstate or foreign commerce in furtherance of the offense. This section also would provide for jurisdiction where the property against which the weapon of mass destruction is directed is

property within the United States that is owned, leased, or used by a foreign government. It also would amend the WMD statute to prohibit the use of chemical weapons – the current statute does not prohibit the use of such weapons. Finally, this section expands the definition of “restricted persons” who are prohibited from possessing biological agents and toxins that are select agents, such as ebola viruses and ricin, to include an agent of a terrorist country or a member or agent of a terrorist organization.

Section 117: Participation in Nuclear and Weapons of Mass Destruction Threats to the United States (§ 3 of H.R. 2939)

This section amends the Atomic Energy Act to more broadly prohibit directly and willfully participating in the development or production of any special nuclear material or atomic weapon outside of the United States. This section also makes it a crime to participate in or provide material support to a nuclear weapons program, or other weapons of mass destruction program, of a designated terrorist organization or state sponsor of terrorism. There would be extraterritorial jurisdiction for an offense under this provision.

Title II: PREVENTION OF TERRORIST ACCESS TO SPECIAL WEAPONS ACT

(S. 2664) This bill was introduced by Senator Cornyn.

This title is designed to deter the unlawful possession and use of certain weapons – Man-Portable Air Defense Systems (“MANPADS”), atomic weapons, radiological dispersal devices, and the variola virus (smallpox) – whose potential misuse are among the most serious threats to homeland security. MANPADS are portable, lightweight, surface-to-air missile systems designed to take down aircraft. Typically they are able to be carried and fired by a single individual. They are small and thus relatively easy to conceal and smuggle. A single attack could kill hundreds of persons in the air and many more on the ground. Atomic weapons or weapons designed to release radiation (“dirty bombs”) could be used by terrorists to inflict enormous loss of life and damage to property and the environment. Variola virus is the causative agent of smallpox, an extremely serious, contagious, and often fatal disease. Variola virus is classified by the CDC as one of the biological agents that poses the greatest potential threat for public health impact and has a moderate to high potential for large-scale dissemination. There are no legitimate private uses for these weapons.

Current law allows a maximum penalty of only 10 years in prison for the unlawful possession of MANPADS or an atomic weapon. No statute criminalizes mere possession of dirty bombs. Knowing, unregistered possession of the variola virus is subject only to a maximum penalty of 5 years.

*Sections 202-205* of this title make unlawful possession of MANPADS, atomic weapons, radiological devices, or variola virus a crime with a mandatory minimum sentence of 30 years to life. Use, attempts to use, or possession and threats to use these weapons are a crime with a mandatory minimum sentence of life in prison. Use of these weapons resulting in death is

subject to the death penalty. These penalties should especially deter middlemen and facilitators who are essential to the transfer of these weapons.

*Section 206* amends current law to add the criminal offenses created by this bill as federal wiretap predicates. *Section 207* amends current law to include these new offenses in the definition of “Federal crime of terrorism.” *Section 208* amends current law to include these new offenses in the definition of “specified unlawful activity” for purposes of the money laundering statute. *Section 209* amends the Arms Export Control Act by adding the offenses created by this bill to the provision specifying crimes for which a conviction or indictment is a ground for denying an arms export application.

### Title III: RAILROAD CARRIERS AND MASS TRANSPORTATION PROTECTION ACT

*Section 302: Attacks Against Railroad Carriers and Mass Transportation Systems* (S. 2289)  
This bill had a hearing in the Senate Judiciary Committee.

This section would expand and increase criminal penalties for terrorist attacks on railroads and mass transportation systems. Specifically, the section would: extend to railroads all of the protections that currently apply to mass-transportation systems, including making it a crime to aid an offense or to willfully commit an attack on a train (current law requires intent to derail or wreck a train); update current proscriptions on attacks on railroads by borrowing more specific definitions from other statutes (thus also proscribing, for example, attacks with a biological agent or toxins or destructive substances, and expanding the types of railroad equipment that are protected); extend to mass-transportation systems a proscription on undermining railroad infrastructure (this currently only applies to railroads); make it a crime to release biological agents or other hazardous materials on the property of mass transportation providers or railroads; and create an aggravated offense for terrorist attacks against vehicles carrying persons, high-level radioactive waste, spent nuclear fuel, or designated hazardous materials.

### Title IV: REDUCING CRIME AND TERRORISM AT AMERICA’S SEAPORTS ACT

(S. 2653) This bill was introduced by Senators Biden, Specter, Feinstein, Kyl, Hollings, and Allen.

This title would create new offenses and broaden and increase penalties for existing offenses for terrorist and other crimes affecting the security of U.S. seaports

*Section 402: Entry by False Pretenses to Any Seaport*

This section increases penalties for fraudulent access to transport facilities and makes clear that such facilities include seaports and waterfronts.

*Section 403: Criminal Sanctions for Failure to Heave to, Obstruction of Boarding, or Providing False Information*

This section would make it a crime for a vessel operator to fail to stop or slow a ship when ordered to do so by federal law enforcement, or for any person on board a ship to impede boarding by or provide false information to federal law enforcement.

*Section 404: Use of a Dangerous Weapon or Explosive on a Passenger Vessel*

This section would make it a crime to willfully use a dangerous weapon or explosive with the intent to seriously injure any person on board a passenger vessel.

*Section 405: Criminal Sanctions for Violence Against Maritime Navigation, Placement of Destructive Devices, and Malicious Dumping*

This section would make it a crime to intentionally damage or tamper with a maritime navigational aid if such act endangers a ship, or to knowingly place any device or substance in the water that is likely to damage a ship, or to intentionally discharge a hazardous substance into U.S. waters with the intent to cause injury.

*Section 406: Transportation of Dangerous Materials and Terrorists*

This section would make it a crime to knowingly transport bombs or WMD aboard a ship while knowing that the item is intended to be used to commit a terrorist act, or to knowingly transport a person who intends to commit, or is avoiding apprehension after committing, a terrorist act.

*Section 407: Destruction or Interference with Vessels or Maritime Facilities*

This section would make it a crime to damage or destroy a vessel or its parts, a maritime facility, or any apparatus used to store or load cargo or passengers, commit violence against a person on a vessel if such violence is likely to endanger the vessel or its passenger, commit violence that is likely to cause serious injury to a person at or near a maritime facility, or knowingly communicate false information that endangers the safety of a vessel.

*Section 408: Theft of Interstate or Foreign Shipments or Vessels*

This section expands the scope of proscriptions on theft of interstate or foreign shipments to include theft of goods from transport facilities such as trailers, cargo containers, and warehouses.

*Section 409: Increased Penalties for Noncompliance with Manifest Requirements*

This section increases penalties for noncompliance with manifest reporting and record-keeping requirements, including information regarding the content of cargo containers and the country of origin of shipments.

*Section 410: Stowaways on Vessels or Aircraft*

This section increases penalties for violations of proscriptions regarding stowaways.

*Section 411: Bribery Affecting Port Security*

This section makes it a crime to bribe a public official with the intent to either commit terrorism or facilitate a fraud affecting a secure area or seaport, or to receive a bribe in exchange for being influenced in the performance of public duties affecting secure areas or seaports while knowing that such influence will be used to commit or plan terrorism.

Title V: COMBATING MONEY LAUNDERING AND TERRORIST FINANCING ACT

(S. 1837) This bill was introduced by Senator Grassley in November 2003.

This title expands the list of predicate offenses for money laundering to include burglary and embezzlement, operation of an illegal money transmitting business, and offenses related to alien smuggling, child exploitation, and obscenity that were enacted or amended by the Protect Act. It also amends current law to prohibit concealing having provided financing while knowing that it has been or will be provided to terrorists.

###