NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE FBI IS LEADING THE WAY BY MAKING THE PRIVATE SECTOR AN INTEGRAL PART OF THE COUNTERTERRORISM HOMELAND SECURITY ENTERPRISE

by

Stephanie E. Yanta

September 2012

Thesis Co-Advisors: Paul L. Smith
Nadav Morag

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE The FBI is Leading the Way by Making the Private Sector an Integral Part of the Counterterrorism Homeland Security Enterprise		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Stephanie E. Yanta			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. government. IRB Protocol number _____N/A_____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

This thesis discusses the building of a sustainable business process wherein the private sector is integrated into the homeland security apparatus. As the threat our nation and her allies face continues to evolve, so must our responses. Integrating the private sector into the homeland security enterprise is long overdue. It is conceivable the next threat will be uncovered by a shopping mall guard or hotel housecleaning staff which is in stark contradiction to the past when the intelligence community identified a foreign-based cell or undesirable traveler to the States ready to launch an attack.

The private sector brings with it a plethora of talents and resources. Because it has not traditionally been seen as a partner the private sector has been relegated to the sidelines. This is no longer acceptable. The FBI, in partnership with the DHS, is spearheading an innovative project designed to complete the circle of 360 degrees of protection. Project Touchstone is an extremely successful example of a highly selective, small group of trusted decision makers within the private sector, primarily the security apparatus, meeting with the FBI and DHS wherein timely, actionable intelligence information is shared so soft targets can be protected and fortified.

14. SUBJECT TERMS FBI, Project Touchstone, private sector, partnership, London First, Project Griffin, homeland security enterprise, Federal Bureau of Investigation, Department of Homeland Security, critical infrastructure protection, Infragard, Domestic Security Alliance Council, Project Argus			**15. NUMBER OF PAGES** 139
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

THE FBI IS LEADING THE WAY BY MAKING THE PRIVATE SECTOR AN INTEGRAL PART OF THE COUNTERTERRORISM HOMELAND SECURITY ENTERPRISE

Stephanie E. Yanta
Supervisory Special Agent, Federal Bureau of Investigation
B.A. History, Indiana University 1997
B.A. Political Science, Indiana University, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)
from the

NAVAL POSTGRADUATE SCHOOL
September 2012

Author: Stephanie E. Yanta

Approved by: Paul L. Smith
Thesis Co-Advisor

Nadav Morag
Thesis Co-Advisor

Dan Moran, PhD
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis discusses the building of a sustainable business process wherein the private sector is integrated into the homeland security apparatus. As the threat our nation and her allies face continues to evolve, so must our responses. Integrating the private sector into the homeland security enterprise is long overdue. It is conceivable the next threat will be uncovered by a shopping mall guard or hotel housecleaning staff which is in stark contradiction to the past when the intelligence community identified a foreign-based cell or undesirable traveler to the States ready to launch an attack.

The private sector brings with it a plethora of talents and resources. Because it has not traditionally been seen as a partner the private sector has been relegated to the sidelines. This is no longer acceptable. The FBI, in partnership with the DHS, is spearheading an innovative project designed to complete the circle of 360 degrees of protection. Project Touchstone is an extremely successful example of a highly selective, small group of trusted decision makers within the private sector, primarily the security apparatus, meeting with the FBI and DHS wherein timely, actionable intelligence information is shared so soft targets can be protected and fortified.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my family, especially Jessica, for all of their support throughout my NPS journey. Jess, I know you bore the biggest burden—especially of watching the girls and Juan—during my extended absences (and even when I was home and working on school projects), and I am forever grateful for your support and understanding.

Without the help of my former boss, Brenda Heck, I would not have been afforded the opportunity to be a part of such an important and ground-breaking project. Thank you for letting me tag along! I would like to give a shout out to my current boss, Bryan Paarmann. Your understanding, compassion and support have been beyond reproach.

I would like to thank Joe Donovan, my friend and private sector partner for your passion and zeal. You have been a driving force behind this extremely important effort. I would like to thank Paul Smith and Nadav Morag for their comments, criticisms and drive to make this the best thesis possible. I would like to thank my British colleagues for their input, ideas, friendships and partnerships. Thanks to the D.C. Touchstone group. You are founding members of what hopes to be a long-standing partnership. Thank you for all you do and will do to secure our great nation.

Finally, I would like to thank my squad for allowing me the time to realize this goal. I know my absences were difficult, but I truly believe I am a better leader, manager, critical thinker and homeland security practitioner having tackled this program.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

This thesis discusses the building of a sustainable business process wherein the private sector is integrated into the homeland security apparatus as a full and trusted partner. As the threat our nation and her allies face continues to evolve, so must our responses. Integrating the private sector into the homeland security enterprise is long overdue. The private sector brings with it a plethora of talents and resources. But, because it has not traditionally been seen as a partner in securing the homeland, the private sector has been relegated to the sidelines. This is no longer acceptable. The nation demands perfection and has zero tolerance for failure.

Our enemy continues to morph and evolve. It is now a nimble, elusive, and disenfranchised enemy content to strike and immediately retreat into the shadows. No longer is it necessary for a would-be "jihadist" to travel overseas to receive training in an al-Qa'ida training camp. Instead, the disenfranchised are able to associate with the similar minded over the internet, read an on-line magazine, and easily hatch an attack plan for pennies on the dollar. In fact, it is conceivable the next threat will be uncovered by a shopping mall guard or hotel housecleaning staff, which is in stark contradiction to the past when it was the intelligence community that identified a foreign-based cell or undesirable traveler to the States ready to launch an attack.

Despite all of these changes, we continue to plug along, happy in our countering terrorism successes…until now. The Federal Bureau of Investigation (FBI), in partnership with the Department of Homeland Security (DHS), is spearheading an innovative project designed to complete the circle of 360 degrees of protection. Project Touchstone in Washington, D.C. has been active for over a year. It is an extremely successful example of a highly selective, small group of trusted decision makers within the private sector, primarily the security apparatus of the private sector, meeting with the FBI and DHS wherein timely, actionable intelligence information is shared in order to fortify otherwise soft targets. This thesis culminates by proposing the Touchstone Project uniting the FBI and key private sector stakeholders is adopted throughout the U.S.

THIS PAGE INTENTIONALLY LEFT BLANK

II. WHAT ARE WE UP AGAINST?

A. THE CURRENT THREAT ENVIRONMENT: HOW DID WE GET HERE?

This chapter will timeline Usama bin Laden's rise to prominence culminating in the birth of al-Qa'ida. It will discuss al-Qa'ida's transformation and its significant splinter organizations. It will further deliberate the evolution of the homegrown violent extremist and finally demonstrate terrorist target selection and why "soft" targets are preferred targets.

B. AN AUSPICIOUS START

The roots of al-Qa'ida took hold in the 1980s as a result of the Soviet Union's invasion of Afghanistan. Afghani Muslim Islamists used the Soviets' assault as a call for support from Muslims around the world. Consequently, young Muslim males from across the globe heeded the call and flocked to Afghanistan to engage in what they termed a holy war—*jihad*—in order to repel the super power Soviet Union from occupying Muslim lands. A chief participant was none other than Usama bin Laden.[1]

Bin Laden was born in Saudi Arabia, the son of a wealthy construction tycoon of Yemeni descent. His mother was of Syrian heritage and raised bin Laden, along with his two biological sisters, in the traditions of Islam. When bin Laden was 17 years old, he started to become more religious. While studying economics and public administration at the King Abdul-Aziz University in Jeddah, bin Laden had his first encounter with Islamic

[1] Bill Moyers, "Brief History of Al Qaeda," *Bill Moyers Journal*, July 27, 2007, PBS, http://www.pbs.org/moyers/journal/07272007/alqaeda.html (accessed July 7, 2012).

extremism. It was there that bin Laden became indoctrinated in the ways of the Muslim Brotherhood[2] and transfixed with prominent Islamic scholars Abdullah Azzam and Muhammad Qutb.[3]

Bin Laden became indoctrinated in the ways of Qutb, specifically the idea that modern societies must purify themselves of the pre-Islamic darkness or *jahiliyyah.* He fully subscribed to the revelations of the Qur'an and the teachings of the Prophet. As he continued to travel down the road to extremism, bin Laden understood the only way to accomplish the aforementioned tasks was to participate in *jihad*. Bin Laden identified with the precepts of Qutb's message and favored cleansing Muslim societies of the ignorant *jahili*, in particular, Western or non-Muslim influences.[4]

When the superior Soviet Union invaded the downtrodden people of Afghanistan, bin Laden identified with their struggle and began supporting the Afghani fighters through all available means. In part, bin Laden supplied the fighters with financial backing, trucks and other excavation equipment to assist in the construction of fighting positions as well as ideologically like-minded sympathizers. It was during this time too that bin Laden started his anti-America rhetoric, calling for "attacks on U.S. forces and the boycott of American products."[5] Ultimately bin Laden's conviction found him immersed in the mountains of Afghanistan standing side-by-side with his Muslim brothers firing American-made weapons at the evil Soviet invaders—the *infidels*.[6] *Jihad*,

---

[2] The Muslim Brotherhood was founded in Egypt in 1920 by Hassan al-Banna and is one of the oldest and biggest Islamic organizations. The Muslim Brotherhood is an Islamic movement founded upon the desire to "spread Islamic ideals and good works… [and] rid Egypt of British colonial control and cleanse it of all Western influences. ...one of its stated aims is to create a state ruled by Islamic law, or Sharia. Its most famous slogan, used worldwide, is: 'Islam is the solution.'" BBC News, "Profile: Egypt's Muslim Brotherhood," June 26, 2012, BBC News, Middle East, http://www.bbc.co.uk/news/world-middle-east-12313405 (accessed July 7, 2012).

[3] According to Bergen, "Azzam would go on to create the modern world's first truly international jihadist network, and Muhammad Qutb…was the brother of Sayyid Qutb, author of *Signposts*, the key text of the jihadist movement."Peter L. Bergen, *Holy War, Inc.: Inside the Secret World of Osama bin Laden* (New York: The Free Press; 2001), 41, 44, 47.

[4] Bergen, *Holy War, Inc*., 48.

[5] Bergen, *Holy War, Inc*., 51.

[6] From Wikipedia, "**Infidel** (literally "one without faith") is a pejorative name used in certain religions—especially Christianity or Islam—for one who has no religious beliefs, or who doubts or rejects the central tenets of the particular religion." *Wikipedia*, s.v. "infidel," n.d., http://en.wikipedia.org/wiki/Infidel (accessed July 8, 2012).

to bin Laden, was an obligation. Importantly, bin Laden encouraged Arabs to travel to Afghanistan in support of their *jihad* culminating in a global network of fighters. It was during this relative period in bin Laden's *jihadi* career that he established his base—al-Qa'ida (AQ).

Bin Laden managed to concoct a global network of *jihadi* fighters that has existed for more than 30 years. According to author Rohan Gunaratna, "Al Qaeda pursues its objectives through a network of cells, associate terrorist and guerilla groups and other affiliated organizations, and share expertise, transfer resources, discusses strategy and even conducts joint operations with some or all of them."[7] Because of its popularity, al-Qa'ida has membership across the globe. Significantly, some members of al-Qa'ida are American citizens. Gunaratna further surmised, "Within the organization itself, the notion of brotherhood ingrained in Islam helps Al Qaeda cohere."[8] Whether one is born a Muslim or converts to Islam, al-Qa'ida instills in its members a strong appreciation of "their belief system and the group's ideology, which is founded on Islamism and the pursuit of *jihad*."[9]

Al-Qa'ida's goals for *jihad*, according to a document recovered from an al-Qa'ida safe house in Afghanistan were written as:

- Establishing the rule of God on earth
- Attaining martyrdom in the cause of God
- Purification of the ranks of Islam from the elements of depravity[10]

C. AL-QA'IDA TODAY

Al-Qa'ida has evolved into a highly mobile, decentralized and extremely nimble organization. Undoubtedly, core al-Qa'ida remains a threat to the United States and our allies because of their intentions and capabilities. Core al-Qa'ida is assessed to have

---

[7] Rohan Gunaratna, *Inside Al Qaeda: Global Network of Terror* (New York: Berkley Books, 2003), 127.

[8] Ibid., 129.

[9] Ibid.,112.

[10] Al-Qaida/Al-Qaeda (The Base), June 6, 2012, Global Security, http://www.globalsecurity.org/military/world/para/al-qaida.htm (accessed August 24, 2012).

remained committed to attacking the U.S. in dramatic style. However, because of successful collaborative efforts by members of the intelligence community—especially the Central Intelligence Agency (CIA) and the Department of Defense (DoD)—significant number of high level core al-Qa'ida leaders have been eliminated. Most notably, Usama bin Laden was killed in May 2011. Because of the elimination of key al-Qa'ida figures, the al-Qa'ida threat has morphed into a disparate organization of like-minded individuals acting in the name of or on behalf of al-Qa'ida. According to the FBI's Assistant Director for the Counterterrorism Division, Mark F. Giuliano:

> We are seeing an increase in the sources of terrorism, a wider array of terrorism targets, a greater cooperation among terrorist groups, and an evolution in terrorist tactics and communication methodology. The long-term planning undertaken by senior core al Qaeda leaders which led to the 9/11 attacks is much more difficult for them to attain in today's environment. It is replaced with somewhat less sophisticated, quick-hitting strikes which can be just as lethal but which take less funding, fewer operatives, less training, and less timing to execute.[11]

D. AL-QA'IDA IN THE ARABIAN PENINSULA

Al-Qa'ida in the Arabian Peninsula (AQAP) was formed circa January 2009 in a union between two geographic-based components of al-Qa'ida in both Saudi Arabia and Yemen. The Yemeni segment of AQ maintains particular significance because it is the ancestral home of now deceased al-Qa'ida patriarch, Usama Bin Laden.[12] AQAP morphed into a single al-Qa'ida body for all the Arabian Peninsula, specifically welcoming its *jihadi* brethren from the defunct and ineffective AQ group in Saudi Arabia. According to a National Counterterrorism Center product, "AQAP's predecessor, al-

[11] Mark F. Giuliano, "Post 9/11 FBI: The Bureau's Response to Evolving Threats"(speech to Washington Institute for Near East Policy Stein Program on Counterterrorism and Intelligence Washington, D.C., April 14, 2011), Federal Bureau of Investigation, http://www.fbi.gov/news/speeches/the-post-9-11-fbi-the-bureaus-response-to-evolving-threats (accessed July 23, 2011).

[12] "Al-Aqaeda in the Arabian Peninsula: Who Are They? Channel 4 News Looks at the al-Qaeda Group in the Arabian Peninsula Linked to Explosives Found on Two Cargo Planes, and Public Enemy No 1 for the UK Intelligence Services, Anwar al-Awlaki," *Channel 4 News*, October 30, 2010, http://www.channel4.com/news/al-qaeda-in-the-arabian-peninsula-who-are-they (accessed July 23, 2011).

Qa'ida in Yemen (AQY), came into existence after the escape of 23 al-Qa'ida members from prison in the Yemeni capital, Sana'a, in February 2006."[13]

In keeping with its parental affiliation, AQAP, headquartered in Yemen, espouses the same ideological principles and goals as core AQ. They trumpet the *jihadist* ideology stating violence may be used in furtherance of achieving their demands for the expulsion of Western troops from Islamic lands, the overthrow of pro-Western regimes within the Arabian Peninsula and, elsewhere, the annihilation of Israel and the re-establishment of the Islamic Caliphate.[14] Attacks undertaken by AQAP have largely been against the West, especially the United States. The group has both inspired and been responsible for a number of attacks. Research conducted on behalf of the George Washington University Homeland Security Policy Institute concluded, "The 2000 U.S.S. Cole bombing…the droves of AQ foreign fighters of Yemeni descent, and countless other historical indicators demonstrate more than a decade of Yemeni-based extremism against the U.S."[15] Moreover, AQAP was behind the 2008 attack on the U.S. embassy in Sana'a and numerous attempts to disrupt U.S. airliners.[16] Most recently in May 2012, another AQAP plot was thwarted. Yet again, the al-Qa'ida assemblage planned to use an

---

[13] National Counterterrorism Center, "Al-Qa'ida in the Arabian Peninsula (AQAP)," National Counterterrorism Center, n.d., http://www.nctc.gov/site/groups/aqap.html (accessed July 23, 2011).

[14] Fred Burton and Scott Stewart, "Al Qaeda in the Arabian Peninsula: Desperation or a New Life?," *STRATFOR Global Intelligence Weekly*, January 28, 2009, http://www.stratfor.com/weekly/20090128_al_qaeda_arabian_peninsula_desperation_or_new_life (accessed July 23, 2011).

[15] Frank Cilluffo and Clinton Watts, "Countering the Threat Posed by AQAP: Embrace, Don't Chase Yemen's Chaos," *Homeland Security Policy Institute Security Debrief*, July 14, 2011, http://securitydebrief.com/2011/07/14/countering-the-threat-posed-by-aqap-embrace-don%E2%80%99t-chase-yemen%E2%80%99s-chaos/ (accessed July 23, 2011).

[16] Department of Homeland Security, "DHS Snapshot: Yemen Explosive Packages on Cargo Aircraft; November 1, 2010 in Department of Homeland Security: Explosives Discovered in Packages on Cargo Aircraft Bound for the Homeland," November 1, 2010, Public Intelligence, http://publicintelligence.net/ufouo-dhs-snapshot-yemen-explosive-packages-on-cargo-aircraft/ (accessed July 23, 2011).

improvised explosive device to down an airliner bound for the U.S.[17] This demonstrates AQAP's tenacity and overwhelming desire to attack transatlantic flights bound for the U.S.

Arguably, AQAP's ability to spread its ideology makes it especially concerning to counterterrorism officials. A STRATFOR Global Intelligence group assessment indicated, "In many ways, the ideological battlespace is more important than the physical battlespace in the war against jihadism, and in the jihadists' war against the rest of the world. It is far easier to kill people than it is to kill ideologies."[18] AQAP has morphed with the times and propagates its ideology through its media wing, al-Malahim. Moving beyond fiery lectures and tapes, terrorists have leapt into the world of twenty-first century technology and are utilizing all forms of social networking as their new hub for spreading their message. In addition, they are most definitely harnessing the Web to extend their global reach.[19] In particular, AQAP ideologue Anwar Aulaqi, an American born cleric of Yemeni descent, had in many ways become the Western face of AQAP.[20] The MI5 Director General described Aulaqi in a September 2010 by purporting, "His influence is all the wider because he preaches and teaches in the English language which makes his message easier to access and understand for Western audiences."[21] Anwar Aulaqi was killed in a drone strike in Yemen on September 30, 2011. The same strike also claimed another American-born Samir Khan. AQAP, and Aulaqi specifically, are said to have also been responsible for inspiring the Carlos Bledsoe and Major Nidal Hassan shooting

---

[17] Cody Curran, James Gallagher, Courtney Hughes, Paul Jarvis, Adam Kahan, Patrick Knapp, Matthew Lu, Jared Sorhaindo, "AEI Critical Threats: AQAP and AQAP Suspected Attacks in Yemen Tracker 2010, 2011 and 2012," May 21, 2012, http://www.criticalthreats.org/yemen/aqap-and-suspected-aqap-attacks-yemen-tracker-2010 (accessed August 24, 2012).

[18] Fred Burton and Scott Stewart, Al Qaeda and the Tale of Two Battlespaces, *STRATFOR Global Intelligence Weekly*, October 1, 2008, http://www.stratfor.com/weekly/20081001_al_qaeda_and_tale_two_battlespaces (accessed July 23, 2011).

[19] Evan F. Kohlmann, "A Beacon for Extremists: The Ansar al-Mujahideen Web Forum," February 3, 2010, Combatting Terrorism Center at West Point, http://www.ctc.usma.edu/posts/a-beacon-for-extremists-the-ansar-al-mujahideen-web-forum (accessed July 23, 2011).

[20] Topic: Anwar Al-Awlaki, *The Washington Times*, 2012, http://www.washingtontimes.com/topics/anwar-al-awlaki/ (accessed July 23, 2011).

[21] "Al-Aqaeda in the Arabian Peninsula," *Channel 4 News*.

sprees.[22] Both men were alleged to have been inspired by Aulaqi. Hassan reportedly sought religious guidance from Aulaqi prior to his shooting rampage.[23]

Khan was alleged to have been an author of AQAP's *Inspire* magazine. Both deaths were major blows to the terrorist group; the impacts of which are undoubtedly still being felt. According to the *Washington Post*, "President Obama called Awlaqi's death 'a major blow to al-Qaeda's most active operational affiliate' and described him as 'the leader of external operations for al-Qaeda in the Arabian Peninsula,' or AQAP. 'In that role, he took the lead in planning and directing efforts to murder innocent Americans,' Obama said." [24]

While the death of Aulaqi is seen as a major victory in the U.S.'s efforts to counter terrorism, the influence of Aulaqi cannot be discounted. Despite his death, Aulaqi's on-line presence, his recorded speeches, writings and teachings live on because of the internet. The effects of his fiery anti-Western sermons will never truly be known. His immortality can be underscored as a side effect of the globalization of the world because of social media and the internet. Notwithstanding, Aulaqi is viewed as a martyr, catapulting his status in the extremist Muslim world even higher. Without a doubt, he is still considered the single most influential recruiter and radicalizer and especially dangerous because he specifically targeted an English speaking audience.

The July 2010 publication of the on-line, English language-based AQAP magazine *Inspire* arguably changed the face of jihadists' outreach as it is said to be geared toward a U.S. audience.[25] The electronic reach of terrorists has become virtual,

---

[22] Nitasha Tiku, "The Terrorists Are Coming From Inside the Country! American Citizens Now Our Biggest Threat," *New York Magazine*, September 10, 2010, http://nymag.com/daily/intel/2010/09/american_citizens_are_now_our_biggest_threat.html (accessed July 23, 2011).

[23] "Killing of Awlaki Is Latest in Campaign against Qaeda Leaders," *New York Times*, September 30, 2011, http://www.nytimes.com/interactive/2011/09/30/world/middleeast/the-killing-of-anwar-al-awlaki.html (accessed September 8, 2012).

[24] Sudarsan Raghavan, "Awlaki Hit Misses al-Qaeda Bomb Maker, Yemen Says," *Washington Post*, October 1, 2011, http://www.washingtonpost.com/world/anwar-al-aulaqi-us-born-cleric-linked-to-al-qaeda-killed-yemen-says/2011/09/30/gIQAsoWO9K_story.html (accessed August 24, 2012).

[25] 21st Century's Phenomenon: Al-Qaeda New English On Line Magazine "*Inspire*," Global Jihad, n.d., http://globaljihad.net/view_news.asp?id=1535 (accessed July 23, 2011).

unguarded and nearly uncensored. This new trend is much different and more effective than the twentieth century flow of *jihadis*t propaganda which was circulated largely in Arabic and without the help of the internet. Conversely, "…it is increasingly second- and third-tier extremist social networking forums…offering dedicated English-language chat rooms…that appear to play pivotal roles in the indoctrination and radicalization of some of today's most notorious aspiring terrorists."[26]

In testimony, Bruce Hoffman stated, "…once a group has the people's ears and eyes it can manipulate their minds, causing them to act as they not might otherwise…It can be a vehicle for recruitment—meant to win new converts to the cause or replenish the ranks of depleted fighters."[27] AQAP radicalizes and recruits by playing upon common themes throughout their propaganda. They are experts at preying upon disenfranchised youth who are seeking acceptance and a sense of belonging. The group accomplishes this by overdramatizing the alleged killing of Muslims around the world at the hands of the Americans. They insight anger and call upon Muslims to avenge the deaths of the "innocent" Muslims killed by the U.S. and her allies.[28] AQAP exploited the words of Usama Bin Laden when he said:

> My Muslim Brothers of The World: Under the banner of the blessed awakening which is sweeping the Islamic world...Your brothers in Palestine and in the land of the two Holy Places are calling upon your help and asking you to take part in fighting against the enemy—your enemy and their enemy—the Americans and the Israelis. They are asking you to do whatever you can, with one's own means and ability, to expel the enemy, humiliated and defeated, out of the sanctities of Islam.[29]

---

[26] Kohlmann, "A Beacon for Extremists."

[27] Bruce Hoffman, *The Use of the Internet by Islamic Extremists* [testimony before the Permanent Select Committee on Intelligence United States House of Representatives], May 4, 2006, Rand Corporation, http://www.rand.org/content/dam/rand/pubs/testimonies/2006/RAND_CT262-1.pdf (accessed July 23, 2011).

[28] Thomas Joscelyn, "Analysis: Two Ex-Gitmo Detainees Featured in Al Qaeda's Inspire Magazine," *Long War Journal*, October 13, 2010, http://www.longwarjournal.org/archives/2010/10/analysis_two_exgitmo.php (accessed July 23, 2011).

[29] Osama bin Laden, "The Awakenings;" Al Sahwa [blog], August 1996) 29 December 2009, http://al-sahwa.blogspot.com/2009/12/aqap-claims-failed-midair-plot.html (accessed July 23, 2011).

Strategy changes are necessary and have better positioned AQAP to reach a multi-lingual audience, appealing to their dissidence, their longing to be accepted and desire to belong.[30] Strengthening its force is a step toward realizing AQAP's penultimate goals. For instance, AQAP is currently engaged in a bloody battle over territory in Yemen. According to the *Yemen Times*, "Pitched battles are currently taking place between Saleh's [the former President of Yemen] forces and armed Islamists who took control of Zunjubar, the capital of Abyan…."[31] This is arguably AQAP's attempt to establish an Islamic foothold in a key geographic area of the world. "…forces still fight the armed group and claim that it is Al-Qaeda who is trying to establish their Islamic state in Abyan."[32]

Holding steadfast to its principles, the level of concern for AQAP has undoubtedly risen. The FBI Assistant Director for Counterterrorism Mark F. Giuliano said, "…I believe the most serious threat to the homeland today emanates from members of al Qaeda in the Arabian Peninsula…. AQAP leaders such as Anwar Aulaqi…have published articles on the Internet detailing their intent to strike the United States."[33] Should AQAP continue along this path, they will likely be successful in radicalizing and recruiting on behalf of their cause, which will likely result in small victories. AQAP remains the top priority threat group for U.S. counterterrorism efforts. "'AQAP continues to be Al Qaeda's most active affiliate, and it continues to seek the opportunity to strike our homeland,' John Brennan, President Obama's chief counterterrorism adviser, said…in a speech justifying how U.S. officials decide to use drone strikes to target suspected terrorists."[34]

---

[30] Kohlmann, "A Beacon for Extremists."

[31] Ali Saeed, "AQAP, Military Fight Pitched Battles Abyan," *Yemen Times*, June 8, 2011, http://www.yementimes.com/defaultdet.aspx?SUB_ID=36179 (accessed July 23, 2011).

[32] Saeed, "AQAP, Military Fight."

[33] Giuliano, "Post 9/11 FBI."

[34] Azmat Khan, "Understanding Yemen's Al Qaeda Threat," May 29, 2012, PBS, http://www.pbs.org/wgbh/pages/frontline/foreign-affairs-defense/al-qaeda-in-yemen/understanding-yemens-al-qaeda-threat/ (accessed August 24, 2012).

E. AL-QA'IDA MERGER WITH AL-SHABAAB

Al-Shabaab "is an armed group that grew out of other Islamist militias that have been battling Somalia's transitional government since 2006. It currently controls much of southern Somalia—with an estimated 9,000 fighters. It wants to impose a strict version of sharia [law]."[35] According to al-Qa'ida chief Ayman al-Zawahiri, "'I will break the good news to our Islamic nation, which will ... annoy the crusaders, and it is that the Shabab movement in Somalia has joined al-Qaeda." The two groups have been known to work together in the past; however, the official April 2012 merger is significant for a number of reasons.[36]

Al-Shabaab pledged allegiance to al-Qa'ida circa 2009 in a formal statement by al-Shabaab leader Ahmed Abdi Godane, announcing their support of *jihad* under the "stewardship of bin Laden."[37] While bin Laden responded positively, he failed to fully support and endorse the kinship between al-Shabaab and al-Qa'ida. It is said bin Laden was wary of the al-Shabaab leader's "global *jihad* credentials." Because of his hesitance, bin Laden was reticent to appoint him, Godane, as the head of al-Qa'ida in East Africa (AQEA). In fact, it is reported that bin Laden placed great importance on appointing trusted confidants to positions of power within al-Qa'ida.[38]

The implications for al-Shabaab are such that they are now officially operating under the world-wide banner of al-Qa'ida. With this comes fighters and support for a force that was seemingly losing ground as it was perceived to simply be a nationalist movement. Finally, for al-Qa'ida, the impact of the union is emblematic of the problems

---

[35] "Al-Qaeda and al-Shabab: Double the Trouble? We Ask What the Formal Merger of the Two Groups Means for the Conflict in Somalia," *Al Jazeera*, February 11, 2012, http://www.aljazeera.com/programmes/insidestory/2012/02/201221017451210571 8.html (accessed August 23, 2012).

[36] Ibid.

[37] Abdi Aynte, "Understanding the Al-Shabaab /Al-Qaeda 'Merger,'" African Arguments, March 19, 2012, http://africanarguments.org/2012/03/19/understanding-the-al-shabaabal-qaeda-%E2%80%98merger%E2%80%99-by-abdi-aynte/ (accessed August 22, 2012).

[38] Aynte, "Understanding the Al-Shabaab /Al-Qaeda 'Merger.'"

they are currently facing. Plagued by continuous pressure from targeted drone strikes, al-Qa'ida senior leaders have literally been on the run. For current AQ leader Ayman al-Zawahiri:

> Somalia was the only country in the world, where half of its territory (which is the size of Texas), is under the total control of a sympathetic radical Islamist movement. Even if al-Zawahiri, like Bin Laden, was reluctant to appoint Godane, an amateur jihadist in the standards of al-Qaeda, to lead AQEA, the real estate under his command was a precious asset for global jihad.[39]

Moreover:

> Over the past few years, hundreds of global jihadists from around world, many members of al-Qaeda, flocked into Somalia from where they're operating largely unimpeded…. The country is still the best theatre of operations for al-Qaeda. Nowhere in the world does al-Qaeda have such a large and contiguous area of activity.[40]

The wedding of the two groups is indicative of the state of affairs for of core al-Qa'ida. It is on the ropes and is therefore accepting alliances with inferiors in order to stay relevant.

To this point, emphasis has been placed on the more well-known al-Qa'ida groups. This is not, however, meant to suggest there are no other threat groups to which attention should be paid. Certainly, threats from Islamic extremists are and remain significant concerns to the U.S.'s security.

There is tremendous unrest throughout the Middle East and other Islamic majority lands. As of 2010 data, 60 percent of Muslims in Muslim-majority lands are under 30 years of age.[41] Events such as the Arab Spring have energized this disenchanted youth causing significant unrest throughout the region. As a result, the lack of opportunities creates displaced anger. This frustration is projected against a common enemy—namely, the West and, in particular, the United States—in order to justify their low station in life.

---

[39] Aynte, "Understanding the Al-Shabaab /Al-Qaeda 'Merger.'"

[40] Ibid.

[41] "Future of the Global Muslim Population: Projections for 2010–2030," January 2011, The Pew Forum on Religion and Life, http://www.pewforum.org/future-of-the-global-muslim-population-main-factors-age-structure.aspx (accessed September 13, 2012).

Consequently, countries such as Syria, Egypt, Libya, Tunisia and Algeria are becoming increasingly important as the threats they pose to U.S. interests is skyrocketing.

F. HOMEGROWN VIOLENT EXTREMISTS—ENEMIES WITHIN OUR OWN RANKS

Significantly, as senior al-Qa'ida leaders fade into oblivion, core AQ is becoming more and more decentralized. For the U.S., this loose al-Qa'ida affiliation has transformed itself into homegrown violent extremism. Homegrown violent extremists (HVEs) are categorized as persons inspired by those wishing to do harm, such as al-Qa'ida. Notwithstanding, HVEs are difficult to define as there are a number of both environmental and emotional factors that weigh into someone's decision to become an extremist, and, secondly, to promote that extremism through violence. Many HVEs, however, have similar underlying characteristics.

For example, most HVEs have few, if any, true al-Qa'ida connections. Many are lone actors, and there is no age requirement or restrictions on race or citizenship. Moreover, unlike in the past when an individual attempting to engage in *jihad* had to travel overseas and attend a training camp in a place like Afghanistan or the Northwest Frontier Province in Pakistan, today's extremist need only log onto a computer and surf the Internet. In fact, al-Qa'ida has encouraged persons interested in engaging in violence in support of their radical interpretation of Islam to stay at home and conduct attacks.

HVEs have been increasingly motivated by al-Qa'ida, especially al-Qa'ida in the Arabian Peninsula (AQAP), which has exploited social media as a way of reaching large audiences with their messages. To this end, the FBI's Counterterrorism Assistant Director Mark F. Giuliano commented:

> First, we have seen individuals inside the United States become radicalized and motivated to conduct attacks against the Homeland. These individuals can be as diverse as U.S.-born citizens, naturalized U.S. citizens, foreign students, green card holders, or illegal immigrants, but the commonality is their desire to strike inside the United States…. Second, we have seen U.S. citizens become radicalized in the United States and travel or attempt to travel overseas to obtain training and return to the United States or to join and fight with groups overseas…. Lastly, we have seen U.S. citizens become radicalized and use the Internet to further their

> radicalization, contribute to the radicalization of others, or provide services to facilitate Internet radicalization. Whereas the Internet was previously used to spread propaganda, it is now used in recruiting, radicalizing, training, and inciting terrorism. Thousands of extremist websites promote violence to a worldwide audience pre-disposed to the extremist message and more of these websites and U.S. citizens are involved in Internet radicalization.[42]

The significance of HVEs should not be understated. In December 2011, the White House published its *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States*.[43] The FBI followed suit by developing its own four pronged *Threat Mitigation Strategy for Combating Homegrown Violent Extremism*. According to the FBI's Counterterrorism Division Assistant Director Mark F. Giuliano, "What makes these HVE subjects most dangerous is they demonstrated the willingness to take overt, operational steps as well as the ability to procure the materials necessary to carry out their terrorist actions. Finally, and most importantly, they demonstrated the resolve to act."[44]

Again, in addition to al-Qa'ida-related threats, there are a substantial number of non-al-Qa'ida affiliated groups that pose real challenges to homeland security. In fact, concerns arise from lone offenders, who are not as easily tracked, right and left-wing groups such as anti-abortionists and eco-warriors and other domestic terrorist organizations like Sovereign Citizens, who strive to overthrow the U.S. government. While the threat groups may vary, each is a worry for security authorities. Irrespective of their point of origin, every FBI field office is affected by some form of terrorism.

G. SOFT TARGETS ARE EASY TARGETS

A "soft target" lacks stringent security measures and is generally open and easily accessible to the public. The private sector is largely comprised of "soft targets" making them especially appealing for attack by terrorist groups such as al-Qa'ida and AQAP.

---

[42] Giuliano, "Post 9/11 FBI."

[43] The *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the United States* can be found at http://www.whitehouse.gov/sites/default/files/sip-final.pdf.

[44] Giuliano, "Post 9/11 FBI."

According to the *Washington Post*, "…The hardening of…[government and other] targets has increased the appeal of shopping malls, sports arenas, hotels, restaurants, bars, nightclubs, movie theaters, housing complexes and other 'soft' targets that remain relatively unprotected against terrorist attacks."[45] We are an open, free society devoid of harsh control measures. Because of this, places we like to frequent such as the mall and the movie theater are vulnerable to attack.

The influence of AQAP's *Inspire* magazine further exemplifies the risk posed by terrorist attacks against soft targets. This English-language propaganda continues to call for independent violent action against Western soft targets. This is especially concerning inasmuch as individuals could be mobilized or acquire the tactical capability to conduct independent attacks. For example, one edition of *Inspire* magazine provided detailed instructions on how to "Make a Bomb in the Kitchen of Your Mom."[46]

Inspire has encouraged its readers to target restaurants and cafés, military recruiting stations, nightclubs, highways and shopping malls. The edition encouraged *jihad* in place further exacerbated by the statement:

> The foreign brothers that join the mujahidin, many amongst them, conclude that it would have been better for them to return to the West and launch operations. This is because killing 10 soldiers in America for example, is much more effective than killing 100 apostates in the Yemeni military.[47]

Likewise, in a recent edition, the magazine provides detailed instructions on training with a handgun. The explicit instructions include disassembly, proper hand grips and shooting stances. This same edition provides alarmingly clear instructions on the assembly of a remote detonation device—written for the "average" skill level. Perhaps most chilling are the demonstrative diagrams that accompany these tasks.[48]

---

[45] Clark Kent Ervin, "Terrorism's Soft Targets," *Washington Post*, May 7, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/05/05/AR2006050501754.html (accessed July 27, 2012).

[46] AQ Chef, "How to Make a Bomb in the Kitchen of Your Mom," *Inspire*, summer 2010.

[47] "AQAP Urges US Sympathizers to Attack Malls, Nightclubs," *New Media Journal*, n.d., http://newmediajournal.us/indx.php/item/995?sms_ss=newsvine&at_xt=4d94a71def0a6cae%2C0 (accessed September 8, 2012).

[48] AQ Chef, "How to Make a Bomb."

It is widely known that AQ ideologues, such as American-born Adam Gadahn, have suggested conducting jihadist-type violent actions at home versus traveling overseas to engage in acts of indiscriminate violence in furtherance of their radical ideology. Specifically, "In Gadahn's June 3 [2011] video, he calls on Muslims living in America to carry out deadly one-man terrorist acts using fully automatic weapons purchased at gun shows, and to target major institutions and public figures."[49] Without timely, actionable intelligence private sector security managers are unable to enhance security and strengthen their security posture.

Time and again, terrorist groups have attacked, or planned attacks, on privately owned assets. Traditionally, these events have been taken place overseas. While there are too many to discuss, a couple involving American businesses or popular Western attractions are highlighted herein: In 2008, the Pakistani-based militant group Lashkar-e-Tayyiba assaulted several popular tourist attractions in Mumbai, including the Taj Mahal Hotel and Leopold Café, both known to be frequented by Americans and other Westerners. In fact, six Americans were killed during the hours-long siege in India's capital city. [50] The second was a strike on three American hotels in Amman, Jordan. According to an on-line source, "Suicide bombers hit 3 American hotels, Radisson, Grand Hyatt, and Days Inn, in Amman, Jordan, killing 57. Al-Qaeda claimed responsibility."[51]

As the threat continues to evolve, so do the attacks. As the acts of violence cross the sea, they become more intolerable to us as a nation. Overseas is one thing—on ones' doorstep is a game changer. Within the last few years there have been a number of foiled homeland plots against unfortified locations:

---

[49] Brian Ross, Rhonda Schwartz, Jason Ryan, and Richard Esposito, "Forty Names Appear on Terrorists' Hit List," *ABC News, The Blotter*, June 16, 2011, http://abcnews.go.com/Blotter/forty-names-terrorists-hit-list/story?id=13861410 (accessed July 27, 2012).

[50] Rama Lakshmi, "Indian Police Arrest Key Suspect in 2008 Mumbai Attack Case," *Washington Post*, June 26, 2012, http://www.washingtonpost.com/world/asia_pacific/indian-police-arrest-key-suspect-in-mumbai-attack-case/2012/06/25/gJQAXrnG1V_story.html (accessed September 30, 2011).

[51] "Terrorist Attacks in the US or Against Americans," 2011, http://www.infoplease.com/ipa/A0001454.html (accessed September 30, 2011).

> September 24, 2009 saw the arrest of Hosam Maher Husein Smadi, a 19-year old Jordanian illegal alien, who espoused his desire to conduct "*self-jihad"* to an undercover agent. The U.S. Attorney's Office press release highlighted, "Smadi made clear his intention to serve as a soldier for Usama Bin Laden and al Qaeda, and to conduct violent jihad…. The investigation determined Smadi was not associated with other terrorist organizations."[52] Smadi conducted his own pre-operational surveillance on the Fountain Place office tower in Dallas, Texas that he intended to destroy using a vehicle packed with explosives. Smadi was arrested and charged with attempting to use weapons of mass destruction.[53]

On May 1, 2010, Faisal Shahzad parked his explosives-laden Nissan Pathfinder in the heart of Times Square in New York City and fled. While the device seemingly started to ignite, it did not explode. An astute street vendor noticed smoke and alerted police. According to the *New York Times*:

> A large swath of Midtown—from 43rd Street to 48th Street, and from Sixth to Eighth Avenues—was closed for much of the evening after the Pathfinder was discovered just off Broadway on 45th Street. Several theaters and stores, as well as the South Tower of the New York Marriott Marquis Hotel, were evacuated.[54]

Shahzad, a 31-year old U.S. citizen of Pakistani descent was sentenced to life in prison without the possibility of parole having pleaded guilty to all charges. Shahzad, unlike the other examples, did travel to Pakistan where he received training in explosives from operatives of the Pakistani militant group Tehrik-e-Taliban. Janice K. Fedarcyk, the Assistant Director in Charge of the New York FBI Field Office commented:

> The case of Faisal Shahzad demonstrates the global scope of the terrorist threat. Distinctions between home-grown and foreign terrorists are blurred when a U.S. citizen travels to Pakistan to learn bomb-making from a known terrorist organization, then returns to the U.S. and receives financial backing from the overseas organization. However you define him, there's no question that Shahzad built a mobile weapon of mass

---

[52] Northern District of Texas, U.S. Attorney's Office, "FBI Arrests Jordanian Citizen for Attempting to Bomb Skyscraper in Downtown Dallas" [press release], September 24, 2009, Dallas Division, Federal Bureau of Investigation, http://www.fbi.gov/dallas/press-releases/2009/dl092409.htm (accessed August 24, 2012).

[53] Northern District of Texas, "FBI Arrests Jordanian Citizen."

[54] Al Baker and William K. Rashbaum, "Police Find Car Bomb in Times Square," *New York Times*, May 1, 2010, http://www.nytimes.com/2010/05/02/nyregion/02timessquare.html?pagewanted=all (accessed July 16, 2012).

> destruction and hoped and intended that it would kill large numbers of innocent people—and planned to do it again two weeks later.[55]

Finally, In November 2010, "a 19 year old Somali-American attempted to detonate an inert device minutes before the lighting of the Portland, Oregon holiday tree for which he was arrested and charged with attempting to use a weapon of mass destruction."[56] Mohamed Osman Mohamud had attempted to travel overseas to the Northwest Frontier Province in Pakistan to engage in violent *jihad* but was unsuccessful. Instead, Mohamud became acquainted with an undercover agent who he thought was an al-Qa'ida member through the Internet. During the course of the investigation, Mohamud "allegedly told the FBI undercover operative that he had written articles that were published in *Jihad Recollections*, an online magazine that advocated violent jihad." During the course of identifying a target, Mohamud told the undercover "that he was looking for a 'huge mass that will...be attacked in their own element with their families celebrating the holidays.'"[57]

H. SUMMARY

From its humble beginnings in the mountains of Afghanistan, al-Qa'ida has become a global menace. The threat from al-Qa'ida, its splinter and affiliated groups is real irrespective of whether or not the danger comes from a core member or someone inspired by the group's ideology. Al-Qa'ida has transformed itself into a belief system that is rousing the disenfranchised to take action against its perceived aggressors. Some

---

[55] Southern District of New York, U.S. Attorney's Office, "Faisal Shahzad Sentenced in Manhattan Federal Court to Life in Prison for Attempted Car Bombing in Times Square" [press release], October 5, 2010, New York Field Office, Federal Bureau of Investigation, http://www.fbi.gov/newyork/press-releases/2010/nyfo100510.htm (accessed August 24, 2012).

[56] Bryan Denson, "FBI Thwarts Terrorist Bombing Attempt at Portland Holiday Tree Lighting, Authorities Say," *The Oregonian*, November 26, 2010, Oregon Live, http://www.oregonlive.com/portland/index.ssf/2010/11/fbi_thwarts_terrorist_bombing.html, (accessed July 16, 2012.

[57] District of Oregon, U.S. Attorney's Office, "Oregon Resident Arrested in Plot to Bomb Christmas Tree Lighting Ceremony in Portland; Vehicle Bomb Left at Scene was Inert and Posed No Danger to Public" [press release], November 26, 2010, Portland Division, Federal Bureau of Investigation, http://www.fbi.gov/portland/press-releases/2010/pd112610.htm (accessed August 24, 2012).

of these subjugated few in the United States have become known as homegrown violent extremists. HVEs are often times lone actors with few to no real al-Qa'ida connections. HVEs are not limited in age, race or citizenship.

Advocates of engaging in violence are resoundingly attempting attacks on places that are open, easily accessible and have little to no visible security—"soft targets." As has been demonstrated both overseas and more recently in the homeland, attacks are against publicly accessible locales—most of which are owned and operated by the private sector. Indeed a properly trained company staff member may observe pre-operational activity. Whether the activity is perpetrated by an al-Qa'ida member, affiliate or inspired individual, a lone offender or even a disgruntled employee, prior to an attack, there is generally considerable planning involved.

An informed and trained private sector will undeniably see changes in behavior of co-workers who may be rapidly moving along the radicalization continuum. Too, the private sector will spot someone attempting to acquire the means (weapons, ammunition, chemicals, components, etc.) to enact an attack. Perhaps an alert cadre will notice reconnaissance of attack and egress routes as suspicious or out of the ordinary activity in and around their place of business. Simply, it may be the cleaning staff that stumbles upon propaganda materials or even attack plans in the hotel room they are in charge of tidying.

Attack planning is generally complicated and comprised of a number of evolutions. There are countless opportunities for a knowledgeable private sector employee to recognize and report terrorists' activities prior to an attack. For example, whether alone or in a cell, an attacker may have to travel to his target location. This may require out of town accommodations perhaps at a hotel or motel. Or, he may simply use a hotel room a command post or secure meeting place. He needs money which may require business in a bank or other financial institution or the use of an ATM—some of which may be located within a shopping mall or grocery store. The terrorist more often than not requires some means by which he can communicate with other cell members, terrorist leaders and financiers. Moreover, the attack will require transportation—whether it is for reconnaissance of the target location or travel to and from the target site.

Depending upon the type of attack, the perpetrator will need a place to train and rehearse his activities. The training facility could be a gymnasium, martial arts studio, shooting range or paint-ball locale. Lastly, the terrorist will need weapons. The weapons may be firearms, ammunition, large quantities of nails, or perhaps pre-cursor chemicals.

In the case of Najibullah Zazi, he and his family were seen purchasing inordinate quantities of peroxide from a local beauty supply shop. Further, he practiced mixing chemicals and conducted a pre-attack test of his bomb in the parking lot of a hotel in which he had rented a room.[58]

It becomes evident very quickly that it is nearly impossible for a terrorist planning an attack to not intermingle with the general public at some point during his planning process. The private sector affords the logistical support necessary to carry out an attack—either alone or in a group. This underscores the importance of sharing indicators, trends, tactics and techniques and of establishing trip wires within the private sector communities. An informed and trained community is the first line of defense. A radicalized individual intending to do harm will undoubtedly and in some capacity cross the private sector's radar. Establishing solid and clear lines of communication with the public sector is necessary to stay "left of boom."

[58] Tom Hays, "Zazi Testifies at Subway Plot Trial," *Associated Press*, April 17, 2012, ABC News, http://abclocal.go.com/wabc/story?section=news/local/new_york&id=8624058 (accessed September 8, 2012).

THIS PAGE INTENTIONALLY LEFT BLANK

III. A QUICK REVIEW OF NATIONAL COUNTERTERRORISM STRATEGY DOCUMENTS

A. NATIONAL STRATEGY REVIEW

Having established that the threat of terrorism within the U.S. is real and persistent, this chapter will examine the national directives and counterterrorism strategies and policy guidance developed since 9/11. While a number of the documents called for better and more active outreach and engagement with the private sector, ***none*** outlined the "how to" piece of the puzzle. For purposes of this review, government generated documents such as Presidential Directives, executive orders and national security strategies will be scrutinized. Additionally for comparison purposes, documents drafted from the private sector's point of view will be appraised.

B. GOVERNMENT DIRECTIVES, ORDERS AND STRATEGIES

The concept of protecting our critical infrastructure was not born post-9/11. In fact, Presidential Decision Directive 63, published in 1998, "created a national goal to protect the nation's critical infrastructure from international attacks. To meet this goal, the directive called for a 'public-private partnership to reduce vulnerability.'"[59]

Following the catastrophic attacks of 9/11, President George W. Bush signed the first of two significant executive orders. On October 9, 2001, only days after the assaults and while the nation was still staggering from the fatal blows dealt by al-Qa'ida, the President signed Executive Order 13228. This order created the Office of Homeland Security and the Homeland Security Council. The offices' mandates were to develop comprehensive strategies whereby the U.S. would be protected from other terrorist threats as well as to secure the nation's critical infrastructure.[60]

---

[59] National Infrastructure Advisory Council, *Critical Infrastructure Partnership Strategic Assessment: Final Report and Recommendations* (Washington, DC: National Infrastructure Advisory Council, 2008).

[60] John Moteff and Paul Parfomak, *Critical Infrastructure and Key Assets: Definition and Identification* (Washington, DC: Congressional Research Service, 2004), 9.

Executive Order 13231 followed shortly thereafter on October 16, 2001. This edict established the President's Critical Infrastructure Protection Board. Part of the board's responsibilities included outreach to and consultation with the private sector on a number of matters, including communication systems security. Furthermore, the order established the National Infrastructure Advisory Council (NIAC). The council, to be composed of 30 Chief Executive Officers, or their equivalents, from the private sector, academia and state and local government was charged with "responsibilities for the security of information infrastructure supporting the critical sectors of the economy, including banking and finance, transportation, energy, communications, and emergency government services."[61]

Reviewing the national strategy for homeland security directives published in July 2002, October 2007, *The Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* published in February 2010 and, finally, the *National Security Strategy* directive of May 2010 was a fascinating journey through the development of a comprehensive national security strategy following the most significant paradigm shift in national security policy in years. All of this tedious writing and strategizing was brought about by the horrific terrorist attacks on September 11, 2001. Each directive outlined a number of key strategies by which the President and Congress hoped to defend the nation against another serious attack from terrorists.

Each piece endeavored to specifically detail the function of the newly formed Department of Homeland Security and highlight the need for more robust intelligence collection and achieving shared cooperation across the tribal, local, state and federal levels of government—including the incorporation of the private sector. As with any major shift in thinking, some of the bold new steps have been very successful while others have fallen short. Particularly interesting was the proposed strategy on Preventing Terrorism and Enhancing Security.

---

61 "Critical Infrastructure Protection in the Information Age," Executive Order no. 13,231, October 16, 2001, National Communications Systems, http://www.ncs.gov/library/policy_docs/eo_13231.pdf, 3, 11 (accessed September 6, 2012).

Not surprisingly, the first strategic goals discussed in the February 2002 report outlined in order of priority: "Preventing terrorist attacks within the United States; Reducing America's vulnerability to terrorism; and Minimize the damage and recover from attacks that do occur."[62] At this snapshot in time, only months after the attacks of 9/11, defending the nation was described in very succinct terms—to identify, stop and disrupt terrorists.

As has been seen over the years, in reality this is not as easy as it sounds. In the aftermath of 9/11, the entire intelligence and federal law enforcement communities shifted their focus from other tasks like crime prevention and stopping the spread of communism to countering terrorism. Specifically within the FBI, this meant realigning resources and changing a hardened criminal-focused mindset. In 2002, the strategy called for a revamping of America's intelligence community to address the lack of human source coverage. This was particularly concerning for the FBI because, while there was tremendous source coverage in criminal matters, the FBI was not as well postured in the national security branch—specifically within the realm of terrorism.

Moreover, the report highlighted an inability to exploit "foreign language documents."[63] The FBI was sorely lacking in its foreign language capability—a trend that unfortunately continues today specifically in tribal-affiliated languages and local dialects within countries of interest. Lastly, the 2002 report conceptualized that "intelligence and information analysis is not a separate, stand-alone activity, rather an integral component of our Nation's overall effort to protect against and reduce our vulnerability to terrorism."[64] Clearly, the importance of intelligence in the war on terrorism cannot be overstated—the consequences can be debilitating.

In 2002, the strategy report focused heavily on identifying the importance of tactical and strategic intelligence. Tactical, actionable intelligence and analysis of the derived data are the cornerstones for all higher level intelligence analysis. Without real-

---

[62] Office of Homeland Security, *National Strategy for Homeland Security* (Washington, DC: Office of Homeland Security, 2002) vii.

[63] Ibid., 16.

[64] Ibid., 16.

time, on the ground eyes and ears, our national defense mechanisms are lost and will ultimately lose. This dovetails perfectly with the requirement for human source coverage (HUMINT). This tactical intelligence, sources on the ground, is at the foundation of developing a strong national security strategy and, more importantly, ensuring the execution of the strategy is working. Important, too, is strategic analysis. Developing a clear understanding of the terrorists' radicalization, their modus operandi, goals and objectives will assist in providing intelligence gaps that tactical collection and analysis may fill. This synthesis of information will better posture not only the FBI but also the whole U.S. government in combating terrorism. Glaringly, the report speaks directly to tearing down the walls between Intelligence Community and law enforcement partners but neglects to mention the integration of the private sector into the equation.

President Bush issued Homeland Security Presidential Directive 7 (HSPD-7) on December 17, 2003. This directive sought to elucidate roles and responsibilities related to the protection of critical infrastructure and key assets from terrorism. Additionally, it mandated the identification, prioritization and strategy for protection of these pieces of critical infrastructure and key resources. Notably, the directive specified, "Federal departments and agencies will work with State and local governments and the private sector to accomplish this objective."[65]

As the years went on, the 2007 strategy report continued to highlight the need to protect America against a terrorist attack. However, instead of simply restating this task, it outlined tools, some new, some old (such as the Foreign Intelligence Surveillance Act—"FISA"), that could be employed by those charged with the duty of protecting America from a terrorist attack. For example:

> …key legal reforms—such as the USA PATRIOT Act, the Intelligence Reform and Terrorism Prevention Act of 2004, and the Protect America Act of 2007—which promote security and help to implement both the 9/11 Commission and the [Weapons of Mass Destruction] WMD Commission recommendations while protecting fundamental liberties. Furthermore,

[65] *Compilation of Homeland Security Presidential Directives* (HSPD) (Updated through December 31, 2007), Prepared for the use of the Committee on Homeland Security of the House of Representatives (Washington, DC: U.S. Government Printing Office, 2008), 35.

> with the Military Commissions Act of 2006, the United States can prosecute captured terrorists for war crimes through full and fair trials.[66]

Arguably, Congress and the President recognized the importance of providing new and innovative legal tools for law enforcement use, allowing court oversight and a keen understanding and protection of civil liberties.

This report further narrowed the focus by encouraging "…the implementation of Intelligence-Led Policing in State, local and Tribal law enforcement…."[67] While the message is the same—to prevent terrorism and enhance security—this report continues to specify tasks and tools to use to successfully succeed. Moreover, this report highlighted the emergence of homegrown radicalization and the threat of terrorist's use of weapons of mass destruction as real possibilities. The report discussed the prospect of terrorists' use of chemical, biological and nuclear weapons as a viable method of attack.

In the *Quadrennial Homeland Security Review Report* of February 2010, the prevention of a terrorist event and enhancing security were two of many missions outlined for implementation. Again, as the reports morph, the understanding of the mission becomes clearly evident as each report builds upon the next and becomes more specific and detailed about goals and objectives within homeland security. For example, the 2010 Quadrennial Report demonstrates the need for stronger "…public-and private-sector activities designed to counter terrorist efforts to plan and conduct attacks."[68] Without public "buy-in," law enforcement's ability to have adequate human source coverage severely hampered. Along with HUMINT, the report outlined the necessity of not only understanding the threat, but also having the personnel and expertise to analyze raw information into actionable, easily disseminated intelligence.

Interestingly, the report outlined a number of great ideas and actions that should occur, such as deterring and disrupting operations, protecting against terrorist

---

[66] Homeland Security Council, *National Strategy for Homeland Security* (Washington, DC: Homeland Security Council, 2007), 6.

[67] Ibid., 20.

[68] Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (Washington, DC: Department of Homeland Security, 2010), 38.

capabilities, stopping the spread of violent extremism and engaging communities. That said, the document did not offer a single idea on how to accomplish any of these missions, goals and objectives.[69] The commentary was equally as nebulous when discussing the threat of WMD. While the chronicle did offer controlling the acquisition and movement of raw materials and technologies—all owned by the private sector—it did not offer the way forward in terms of the implementation of such a plan.

Finally, the *National Security Strategy* of May 2010 moved beyond the land borders of the United States and outlined a more global approach to national security. One of the "enduring national interests," of course, was security.[70] Undoubtedly, terrorism has no boundaries. As a result, engaging foreign partners and developing new partnerships is paramount to the success of securing the homeland. Herein, the private sector would certainly qualify as a new partner.

Undoubtedly, the U.S. must remain committed to reinforcing and reinventing its military defenses while continuing to rely upon and engage with foreign allies. A global approach to securing the borders, while seemingly counter-intuitive, may be the best use of limited resources. As the report states, "…we are working with partners abroad to confront threats that often begin beyond our borders. And we are developing lines of coordination at home across federal, state, local, tribal, territorial, nongovernmental, and private-sector partners, as well as individuals and communities."[71] This strategy effectively strengthens the U.S.'s ability to protect the homeland because of the increased numbers of people both at home and abroad watching for and understanding threat indicators and pre-operational activities. In all, this report very succinctly and effectively outlines the way forward while maintaining a pragmatic approach to securing the nation. Unfortunately, the missing link remains a "how to" manual on incorporation of the private sector into the homeland security fold.

---

[69] Department of Homeland Security, *Quadrennial Homeland Security Review*, 39.

[70] White House, *National Security Strategy* (Washington, DC: White House, 2010), 17.

[71] Ibid., 18.

The NIAC *Critical Infrastructure Partnership Strategic Assessment*, published on October 14, 2008, outlines several key points regarding roles and responsibilities of both the government and private sector. In part, it recognizes the importance of the private sector as providing essential goods and services to the nation and the world. It also identified that the protection of this precious life blood is a shared responsibility between both parties. As such, the report focuses on information sharing between the government and private sector as a critical piece in leveraging collective capabilities. The study found, that while information sharing has improved, it is still woefully inadequate. Interestingly, the report also concluded that some corporations' perceptions of the government are that it lacks understanding of private sector needs. Other key outcomes included the necessity of the establishment of trusted relationships to foster the sharing of sometimes sensitive information and the compulsion to not get bogged-down in the bureaucracy of information sharing.[72]

Finally, the NIAC study published in 2012 examined the current intelligence sharing environment with an eye on determining whether or not the right information is getting to the right people within the private sector. The group acknowledged improvements in information sharing across the government but pinpointed shortcomings within the information sharing network with the private sector. The study highlighted a lack of bi-directional information sharing and the ensuing gaps between collaborative security efforts. Importantly, the study hit upon trust as an essential factor in a successful information sharing system. Trust is highlighted as the "essential glue" to making partnerships work. Furthermore, the report states:

> Trust results when partner capabilities are understood and valued, processes are tailored to leverage these capabilities, and these processes are tested and proven valuable to all partners. When breakdowns in information sharing occur, it erodes trust and is counterproductive to risk management.[73]

---

[72] National Infrastructure Advisory Council, *Critical Infrastructure Partnership.*

[73] National Infrastructure Advisory Council, *Intelligence Information Sharing: Final Report and Recommendations* (Washington, DC: National Infrastructure Advisory Council, 2012).

In short, the study found that the passage of timely, actionable and tailored information pertinent to the protection of critical infrastructure and key assets within the private sector is, more often than not, not happening. This includes the fact that the private sector is not informing the government as it finds the information sharing network confusing and too complex. The study also concluded that the expertise, skills, abilities and capabilities inherent to the private sector are not only misunderstood but not being leveraged in support of securing the homeland. Finally, the review discovered that the Department of Homeland Security, who has the lead on outreach to the private sector, is failing to spearhead the cause regarding bi-directional information sharing on behalf of the private sector.

C. IN CONCLUSION

Without a doubt, the government documents underscore the importance of the protection of the nation's critical infrastructure and key resources. Indeed, not one argues against the inclusion of the private sector into the circle of the homeland security arena. However, none provides a road map for the execution of what is undoubtedly a necessary evolution. Conversely, the NIAC studies point out that the private sector fully understands the gravity of receiving timely intelligence information. After all, they are the owners and operators of the critical resources that allow America to thrive. Protecting these assets is not only pragmatic from a business and money-making perspective but an absolute. In all, both identify the need for private sector inclusion, but fall short on the "how to" regarding the implementation of this great idea.

IV. THE FBI'S CURRENT OUTREACH FOOTPRINT

A. EXISTING OUTREACH PROGRAMS WITHIN THE FBI

Having shown there is a definite need for practical counterterrorism engagement between the U.S. government and the private sector, this chapter will detail two of the FBI's many outreach programs. A pair, InfraGard and the Domestic Security Alliance Council (DSAC), will be reviewed and their outreach protocols examined. These two particular programs have been chosen because they most closely resemble the Touchstone project in Washington, D.C. The stated objectives of each program are to develop relationships with private sector partners and share information. In reality, neither of these programs builds the trusted relationships necessary to accomplish these goals.

B. CURRENT OUTREACH

The importance of information sharing and building alliances cannot be undersold. As FBI Director Robert S. Mueller, III said, "Every day, in every community, we are working together to stop gang activity…to root out public corruption and fraud…to protect our children…and to prevent terrorism. We in the FBI know that information sharing is crucial to our collective success."[74] The FBI manages at least seven private sector outreach programs. The FBI's outreach footprint includes InfraGard, fusion centers, the Domestic Security Alliance Council, the Internet Crime Complaint Center, the National Cyber Forensics and Training Alliance, the National Gang Intelligence Center and the Counterintelligence Division's Strategic Partnership Initiative. While they are all under the FBI umbrella, not all of them focus on the same

[74] Robert S. Mueller, III, "Watchmen on the Walls of our Freedom" (speech National Academy Associates Annual Training Conference, Grapevine, Texas, July 31, 2012), Federal Bureau of Investigation, http://www.fbi.gov/news/speeches/watchmen-on-the-walls-of-our-freedom (accessed August 25, 2012).

issues—some directly support investigative efforts while others are seen as platforms for "information sharing that help us to better understand emerging threats and foster crime prevention initiatives."[75]

C. INFRAGARD

InfraGard was started in 1996. Its creation was based on an identified need for greater investigative expertise in the areas of cyber and (post-9/11) physical security within the nation's critical infrastructure. In the Cleveland Field Office of the FBI, agents and subject matter experts from various private sector entities and academia untied forces to address these emerging threats. With this partnership came great success—so much so that InfraGard was adopted as a nation-wide initiative headquartered in Washington, D.C. Each of the FBI's 56 field offices was delegated local chapter obligations.[76]

At its heart, InfraGard is an information sharing platform between the private sector, the U.S. government and the FBI in particular. According to its Website, "InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States."[77] In 1998, program management responsibilities for InfraGard were under the National Infrastructure Protection Center (NIPC). However, after the attacks on 9/11, program management for NIPC was transferred to the Department of Homeland Security. Nonetheless, the FBI retained responsibility for InfraGard in conjunction and coordination with the DHS's efforts to protect our nation's infrastructure. Within the FBI, programmatic guidance for

[75] Federal Bureau of Investigation, "Partnerships and Outreach," http://www.fbi.gov/about-us/partnerships_and_outreach/ (accessed July 15, 2012).

[76] InfraGard pamphlet.

[77] InfraGard, "About InfraGard," 2012, http://www.infragard.net/about.php?mn=1&sm=1-0 (accessed August 25, 2012).

InfraGard fell to the Cyber Division circa 2003. Moreover, InfraGard attempted to expand its outreach to assist in counterterrorism matters as well as its cyber proficiency.[78] InfraGard's Website states:

> The goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes.

The group's objectives are many. They include increasing the extent and frequency of information sharing between members and the FBI on all matters of interest to both the private sector and law enforcement.

For instance, threats to critical infrastructure and key resources, identifying susceptibilities, ensuring interdependencies are highlighted and addressed in regard to safety, promoting information exchange especially as it relates to threat information, encouraging interaction between the private sector and all levels of government and finally facilitating education and training opportunities to the private sector to foster a better understanding of the current threats facing the nation. InfraGard does not solely focus on counterterrorism issues; instead, the group takes more of an all-hazards/all-threats approach.[79]

Each FBI office appoints an InfraGard coordinator. This person is responsible for recruiting and facilitating the membership process for interested persons. *Anyone* can become an InfraGard member. However, every individual who applies is subjected to database checks for quality assurance purposes. Additionally, each pledge must sign and abide by Rules of Behavior. InfraGard estimates its nation-wide membership currently exceeds 51,000 (including FBI personnel).[80]

The benefits of being an InfraGard member are described as inclusion in a network of private sector contacts, privileged access to a secure FBI Web-based portal of

---

[78] InfraGard, "About InfraGard."

[79] Ibid.

[80] InfraGard, "Become a Member of InfraGard," n.d., http://www.infragard.net/member.php?mn=2 (accessed August 26, 2012).

information, access to information provided by both the FBI and DHS related to critical infrastructure and key resources issues and concerns, and training and educational opportunities, finally, there is no cost to becoming an InfraGard member.[81]

Notably, each InfraGard chapter is independently operated and governed by its own elected board of private sector associates. It is only sponsored by the FBI—it is not FBI run, only affiliated. It is this local managerial panel that sets the agenda for its group's activities. InfraGard chapters meet regularly to discuss topics of interest and may even invite speakers to further educate their contingencies on issues affecting their locale. Some may offer a newsletter, additional training and educational opportunities, and even "contingency plans" in the event of a failure or attack on the communication infrastructure.[82]

Information shared through InfraGard includes items such as the DHS *Daily Open Source Infrastructure Report*. This report "is collected each business day as a summary of open-source published information concerning significant critical infrastructure issues. Each Daily Report is divided by the critical infrastructure sectors and key assets defined in the National Infrastructure Protection Plan."[83] Also included may be information from the Internet Crimes Center, the American Red Cross, incidents reported to SANS Institute Computer Virus Alerts and Warnings, as well as reporting from the U.S. Department of Justice, Computer Crime and Intellectual Property Section. Other articles and bulletins pertinent to the private sector are posted and accessible via the InfraGard Website: http://www.infragard.net. [84]

D. MISSING THE MARK

There are some positive aspects to the all-inclusiveness of InfraGard. Casting a wide net in regard to information sharing is not necessarily negative. Indeed, the more

---

[81] InfraGard, "Become a Member of InfraGard."

[82] Ibid.

[83] Department of Homeland Security, *Daily Open Source Infrastructure Report*, 2009, http://www.dhs.gov/dhs-daily-open-source-infrastructure-report (accessed August 25, 2012).

[84] InfraGard, "Links/In the News," n.d., http://www.infragard.net/about.php?mn=1&sm=1-0 (accessed August 26, 2012).

people that can be reached, the better awareness becomes—especially as it relates to innocuous, threat indicator-type disseminations. This is evidenced by the DHS's "See Something, Say Something" campaign that focuses on reaching the widest audience possible. However, uncontrolled broadcastings of sensitive information can result in dire consequences if it falls into the wrong hands.

So, while InfraGard is successful in its wide distribution of news, it misses the mark on a number of fronts. For one, allowing anyone to join based on the passage of a simple records check causes great disparity among group members. Its indiscriminate membership rolls becomes troublesome when information sharing reaches the ragged edges of becoming sensitive.

For instance, an InfraGard meeting may have in its audience the chief security officer for Boeing Corporation who holds a top secret security clearance. Now, sitting next to the Boeing executive is the owner of the local Chinese restaurant who has been in the United States for only 10 years. There is a glaring difference between the two as far as vetting and proven trustworthiness. Simply passing a criminal history check does not by any stretch indicate there should not be some measures of control placed on sensitive information sharing.

Moreover, because anyone can join InfraGard, the prestige and exclusiveness of being a member becomes watered-down. Furthermore, the idea of all-inclusiveness eliminates the ability to develop personal, trusted relationships. To further illustrate, imagine Company X has 12 employees that are members of InfraGard. The Company X employees decided each would take a turn attending InfraGard meetings. If their InfraGard chapter hosts a meeting on a monthly basis, each Company X representative may only attend one InfraGard meeting per year. Resultantly, the opportunity to get to know someone and develop a trusted relationship is lost. The all-inclusiveness of InfraGard's rolls may discourage decision-makers within key sectors and subsectors from attending InfraGard meetings or even becoming members at all. Again, this underpins the inability for members to develop close, personal trusted relationships.

Interestingly, as well, InfraGard is an FBI sponsored not FBI controlled program. In fact, the FBI coordinator does not always attend InfraGard meetings. FBI InfraGard coordinators are not involved in the day-to-day operations of their InfraGard groups as each local chapter is independently managed and sets its own agenda without the influence of the local FBI office. The chapter can ask for FBI guidance or assistance, but beyond that, the FBI's role is that of a facilitator.

Additionally, information generated and disseminated through InfraGard is often open source materials to which everyone has access. Beyond the convenience of having one portal to review, there is little value added. The bulletins and posts are often bland, vague and lack timely, actionable intelligence necessary to elicit a reaction from the private sector. In other words, they lack the "how does this affect my business/assets" pointedness desired by the private sector.

The lackluster information, while nice to know, is arguably a result of the position of the InfraGard coordinators. They are too far away from the threat—specifically the threat from terrorism (which is the focus of not only this thesis but also Touchstone). In fact, in many FBI offices the InfraGard coordinator position is a collateral duty. As such, an agent-coordinator is generally not privy to the strategic goings-on of efforts outside of their purview. Therefore, they are not in a position to provide insight and context to published bulletins. Because of these points, InfraGard members quickly lose interest in attending meetings largely because the information provided does not provide context or offer needed and desired guidance and insight. Not only are coordinators generally removed from the counterterrorism threat, as previously stated, they rarely direct the activities of their local chapter.

E. THE DOMESTIC SECURITY ALLIANCE COUNCIL

DSAC was created in 2005 as a domestic-based organization modeled after the U.S. Department of State's Overseas Security Advisory Council.[85] The council evolved out of a need for information. Chief security officers representing businesses crossing all sectors and subsectors called upon the FBI to bridge the gap with the private sector and threat information.[86] DSAC is described as:

> a strategic partnership between the FBI, the Department of Homeland Security and the private sector, [that] enhances communications and promotes the timely and bidirectional effective exchange of information keeping the nation's critical infrastructure safe, secure and resilient. DSAC advances elements of the FBI and DHS missions' in preventing, deterring, and investigating criminal and terrorism acts, particularly those effecting interstate commerce, while advancing the ability of the U.S. private sector to protect its employees, assets and proprietary information.[87]

Membership to the council is more selective than that of InfraGard. DSAC operates at the corporate or executive level. It is open to companies that have distinct security departments with a managing corporate-level security officer, or its equivalent, responsible for the company's overall security and intelligence requirements. Most participants represent Global 1000 companies or "maintain one billion dollars in annual revenue and possess an organized…intelligence component…."[88] Reporting indicates that as of 2010, membership included a representative from every sector and subsector. Additionally, "companies participating in DSAC account for approximately 34% of the U.S. Gross Domestic Product, and account for 8.1% of total U.S. employment."[89]

Preferably, requests for DSAC affiliation are handled via a nomination from a current affiliate or the resident FBI office. However, companies may nominate

---

[85] According to OSAC, "The Overseas Security Advisory Council (OSAC) was created in 1985 under the Federal Advisory Committee Act to promote security cooperation between American private sector interests worldwide and the U.S. Department of State." Overseas Security Advisory Council, "About OSAC," n.d., https://www.osac.gov/Pages/AboutUs.aspx (accessed August 27, 2012).

[86] Domestic Security Alliance Council, "Enhancing Security for American Businesses" [brochure], n.d. http://www.dsac.gov/Pages/DSAC_Brochure.pdf, 2 (accessed August 27, 2012).

[87] Ibid.

[88] Ibid.

[89] Ibid.

themselves, which requires the corporation undergo a vetting process. Additionally, all participants are required to acknowledge and abide by rules of conduct which outline roles, responsibilities and expectations. An organization's DSAC primary point of contact is their corporate security officer. This does not, however, eliminate others from within the company access to DSAC publications, bulletins and portals. Analytical cadres within the private sector are encouraged to seek access to the same.[90]

Association benefits include access to security information provided by all government entities with a role in homeland security, outreach to a diverse group of security experts from across the government and private sector, semi-annual training at the Domestic Security Executive Academy for Chief Security Officers and intelligence analyst professional development training through quarterly symposiums as well as opportunities for participation in DSAC special committees.[91]

Another service offered by DSAC is the Leadership Board which is a collection of about 25 envoys from a cross section of sectors and subsectors. The Leadership Board acts as the subject matter experts for their relevant businesses. Table 1 contains the 29-listed corporations that currently serve as board members: [92]

[90] The Domestic Security Alliance Council, "Domestic Security Alliance Council," n.d., http://www.dsac.gov/Pages/join.aspx (accessed August 27, 2012).

[91] Domestic Security Alliance Council, "Enhancing Security for American Businesses," 3.

[92] Domestic Security Alliance Council, "DSAC Leadership Board," n.d. http://www.dsac.gov/Pages/dlb.aspx (accessed July 28, 2012).

Table 1. Current DSAC Leadership Board Members

3M	Archer Daniels Midland
American Express	Bank of America
Barclays	Boeing
Bristol-Myers Squibb	Bridgestone Firestone
CIGNA	Citigroup
Coca-Cola	ConocoPhillips
Ernst & Young	FedEx Corp
DuPont	General Electric
Kellogg's	KMPG International
JetBlue	MasterCard
Medco Health Solutions	Merck & Company
NextEra Energy	RBS/Citizens
USAA	Walmart
Walt Disney Company	Time Warner
United Airlines	

Finally, DSAC offers yearly instruction for both corporate security officers and the intelligence analyst cadre. For the security corps, the Domestic Security Executive Academy (DSEA) is a week-long training session offered bi-annually and in coordination with the DHS, FBI Academy and the Leadership Development Institute. This instructional session includes approximately 25 private sector chief security officers from various Fortune 1000 companies, about five federal law enforcement partners and roughly 10 FBI Special Agents in Charge from various field offices. The conference offers guidance on information sharing and affords participants the opportunity to mingle and develop professional relationships.[93]

The Intelligence Analyst Symposium (IAS) is a two and a half day FBI Headquarters-based course offered to private sector intelligence and security analysts, federal law enforcement partners and FBI and DHS field intelligence analysts. The

[93] Domestic Security Alliance Council, "DSAC Leadership Board."

program is designed to highlight "collecting and sharing information on domestic criminal threats" to "people, property and [have the potential to] disrupt the normal flow of commerce in the United States."[94] Each IAS assembly is comprised of approximately 40 total intelligence staff from various Fortune 1000 companies, FBI Field Intelligence Groups (FIGs) and fusion centers. The curriculum includes discussion about analytical approaches, best practices, small group exercises, understanding tradecraft and offers an opportunity to develop relationships. A focus of both conferences is to encourage "greater collaboration and cooperation."[95]

E. DSAC: GOOD, BUT NOT GREAT

DSAC is perfectly postured to have a tremendous impact on information sharing and true collaboration with the private sector. Their audience is spot-on. It includes organizational level security professionals representing all sectors and sub-sectors that virtually blanket the U.S. economy. Equally as important, and oftentimes the most challenging aspect of any successful initiative, is that companies *want* to be DSAC members. Unfortunately, DSAC falls short in a number of areas.

DSAC does not have the analytical cadre to support sufficient information sharing with the private sector. Currently, DSAC does not produce specifically tailored products with private sector considerations in mind. In total, DSAC does not provide timely and actionable intelligence information to its customers. To be the most efficient, DSAC should expand its analytical staff. The staff can in turn prepare and publish a meaningful product custom-made for the private sector. The DSAC analytical component should troll through local, national and international news outlets in search of items of interest and usefulness to the private sector. Like its OSAC counterparts, DSAC should strive "to keep constituents informed of security issues around the world [and locally in DSAC's case], as well as to feature…analytic reports, upcoming events, and surveys."[96]

---

[94] Domestic Security Alliance Council, "DSAC Leadership Board."

[95] Ibid.

[96] Overseas Security Advisory Council, "Newsletter," n.d., https://www.osac.gov/Pages/NewsLetter.aspx (accessed August 28, 2012).

Moreover, while DSAC has an impressive constituency, it lacks the consistent and practiced interaction with chief security officers and their government equivalents. Sponsoring a once-a-year conference is not enough time to develop trusted, personal relationships necessary to provide 360 degrees of total homeland security. Moreover, DSAC does not foster bi-directional dialogue and feedback. Aside from exchanging business cards at the yearly symposium, interface between the government and key private sector stakeholders is spotty at best.

F. IN SUM

This chapter exemplifies how the FBI's existing programs are sub-par in terms of fostering true and complete assimilation with the private sector. While each of the reviewed programs, InfraGard and the Domestic Security Alliance Council, respectively, offer positive interactions between the FBI and the private sector, both have faults. InfraGard lacks a continuous influential FBI presence; it does not afford opportunities to develop trusted personal relationships; its membership is indiscriminate and it does not produce or provide meaningful intelligence products that answer the question "What does this mean for my company?"

Equally, DSAC misses the mark on encouraging and providing opportunities to develop trusted individual relationships between the private sector and the FBI. In contrast, their target audience is the executive-level decision-maker, which is ideal. However, DSAC fails to encourage regular interaction and liaison building between the group and the FBI. Aside from its regular seminars, DSAC does not routinely share information that fosters bi-directional dialogue, feedback and responsiveness between the FBI and its members. This is further exemplified by its lack of disseminated intelligence products or routine engagements.

Neither program offers the private sector an interactive and coordinated response to threats on a geographic versus sector specific level. To illustrate, consider the following scenario: A terrorist group parks a truck bomb in front of a well-known government contracting office building they intend to attack. Irrespective of whether or not the bomb has exploded, the mitigation of this terrorist situation requires complete

collaboration between businesses within the affected neighborhood. The targeted company at 123 Main Street, while the principal target, is unfortunately not the only target. Others within 123 Main like the building's security firm and the cleaning crew, the dry cleaner across the street, the deli next door, the coffee shop behind, and so on, are now unintentionally involved. Arguably, to ensure this vulnerable neighborhood is networked and working together as a community robust outreach, training, exercises and interaction between both local and federal law enforcement is required. The commitment to reduce neighborhood weaknesses and ensure collateral damage is reduced in the event of an attack should occur routinely. To date, neither the DSAC nor InfraGard engage in this level of interaction.

Neither of the described programs spearheads table top exercises, for example, to encourage information sharing and the development of common security interests. As described above, this is crucial to a whole of community approach to security. Participation in exercises opens dialogue between neighboring businesses, local police and the FBI. Other important lessons include the identification of gaps in contingency planning. Equally important as the exercise is the follow-up training such as red cell teams that neither of the programs promotes. Red cell exercises are designed to test in-place procedures and identify weaknesses and vulnerabilities in a controlled and non-threatening environment.

Finally, neither of the existing programs has built a mechanism for bi-directional intelligence sharing—specifically intelligence coming to the FBI from the private sector. For instance, as the private sector becomes more aware and trained on threat indicators and the like, more useful intelligence would be made accessible to the FBI. This may manifest itself in the form of source coverage, at risk or possibly radicalized staff and even CCTV coverage. In addition, because neither outcome of the described programs is the development of trusted relationships, access to private sector properties, assets and staff as described above are likely missed.

V. A GLIMPSE INTO THE PRIVATE SECTOR

A. THE PRIVATE SECTOR

As previous chapters have considered the threats to the U.S. from all forms of terrorism, determined that the U.S. government's policy response are unfulfilling and that the FBI's current outreach efforts are insufficient, this chapter will examine the private sector in more detail. After all, "Working together the public and private sectors are stronger than either is alone."[97] This chapter will provide a glimpse into the world of the private sector through the eyes of the Marriott International, Inc. Who are they, what they do and how they can help the United States homeland security enterprise by becoming partners in the fight to secure the nation. The Marriott has been chosen as the representative private sector company because of its domestic and international footprints, the size and diversity of its workforce, its innovative and aggressive security postures and the fact that the Marriott has been the victim of a number of terrorist attacks.

B. THE PRIVATE SECTOR IN GENERAL

Within the United States, the private sector represents the part of the economy that is neither government nor state controlled. What separates the private sector from the government is they are owned and operated by persons seeking to generate revenue. The private sector, in most free-market societies, encompasses the majority of the labor force.[98]

In the U.S., the private sector cuts across all facets of everyday life. Goods and services provided by the private sector include food that is grown and consumed; a home's heating and cooling; cheering for a favorite sports team; shopping for new clothes or other goods—numerous goods and services all the way to the smart phone that globally connects its user to the world. Notably, the aforementioned chattels and services fall within one of the identified 18 critical infrastructure and key resources categories as

---

[97] "NYPD Shield," n.d., http://www.nypdshield.org/public/about.aspx (accessed April 12, 2011).

[98] "Private Sector; Definition of 'Private Sector,'" n.d., Investopedia, http://www.investopedia.com/terms/p/private-sector.asp (accessed August 31, 2012).

set forth by the DHS. According to the DHS, "Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof."[99] Significantly, "the vast majority of critical infrastructure in the United States is privately owned and operated."[100]

C. THE PRIVATE SECTOR PRE AND POST-9/11

Prior to the attacks on 9/11, the nation as a whole and the private sector in particular downplayed and oftentimes dismissed the threat from terrorism. After all, acts of terrorism were relegated to bombings, hijackings and hostage-taking made famous in the '70s and '80s. These were more often than not acts that happened "over there" in some far away land many Americans would have been hard-pressed to find on a map. Not to mention, the U.S. was deadlocked in a battle against the spread of communism and the threat of nuclear war manifested and propagated by the Soviet Union. Therefore, it is not surprising that private sector executives scorned security professionals within their own ranks, viewing security allotments as a waste of money and a drain on profits. Arguably, the private sector's chief security concerns included petty crime and insider theft—threats that did not warrant exaggerated spending to thwart and prevent.

September 11 marked a watershed moment not only in history but in the way America thought about security. Less than a month after the attacks, President Bush signed an Executive Order that specifically addressed, among other issues, critical infrastructure protection.[101] This landmark order proved to be the largest restructuring of the U.S. government in over 50 years. It brought a conglomeration of government activities and responsibilities under the auspices of one department, the Department of

[99] Department of Homeland Security, "Critical Infrastructure," n.d., http://www.dhs.gov/critical-infrastructure (accessed February 28, 2012).

[100] Department of Homeland Security, "About the Office of Infrastructure Protection," n.d., http://www.dhs.gov/about-office-infrastructure-protection (accessed September 4, 2012).

[101] Moteff and Parfomak, *Critical Infrastructure*, 9.

Homeland Security, whose mandates included the lead on protecting critical infrastructure and key resources—and thus the lead on outreach to the owners and operators of said assets—the private sector.[102]

Beyond government reform, following the 9/11 attacks the private sector began to view security differently. Financial losses resulting from the assaults were estimated to be "between $30 and $40 billion."[103] These losses coupled with increased costs, especially for insurance, resulted in amplified prices passed on to consumers. In fact, Robert Hartwig, president of the Insurance Information Institute underpinned the importance of the 9/11 on the insurance industry by stating, "It's safe to say that no event has more fundamentally transformed how insurers think about risk than the Sept. 11, 2001 terrorist attack; not Hurricane Katrina, not the Japanese earthquake, nothing, on a global scale."[104]

Security costs incurred by the private sector prior to the attacks were estimated to be nearly $40 million to $55 million dollars annually. According to economic specialists:

> Nearly half of the total spending for security by the private sector is composed of a single category, security guards and other protective service employees. The rest of the spending falls into such categories as alarms systems, computer security, locks and safes, fencing, surveillance cameras, safety lighting and guard dogs.[105]

---

[102] Department of Homeland Security, "Proposal to Create the Department of Homeland Security," n.d., http://www.dhs.gov/proposal-create-department-homeland-security (accessed September 4, 2012).

[103] Michael Meulemans, "Insurance: 9/11 Changed Insurance Sector Forever," September 14, 2011, http://insurance.about.com/od/Property/a/9-11-Changed-Insurance-Sector-Forever.htm (accessed August 31, 2012).

[104] Jay MacDonald, "How 9/11 Redefined Insurance," Insurance Blog, September 9, 2011, http://www.bankrate.com/financing/insurance/how-911-redefined-insurance/ (accessed September 5, 2012).

[105] Patrick Lenain, Marcos Bonturi, and Vincent Koen, "OECD Economics Department: The Economic Consequences of Terrorism" (working paper no. 334, Organization for Economic Co-operation and Development, Paris, France, 2002), 31.

It was further surmised the price tag for post-9/11 security measures would increase between 50 percent to 100 percent—again, not including the cost of insurance.[106]

D. PUBLIC VERSUS PRIVATE SECURITY

Law enforcement officers within the varying levels of government—federal, state, municipal and tribal—are charged by law to keep society safe from all enemies foreign and domestic. Within the auspices of their law enforcement powers, these officers can make arrests and conduct all types of investigations with the ultimate goal of keeping society safe and free of crime. Notably, sworn law enforcement officers may use deadly force as deemed necessary in order to execute their law enforcement duties.

Law enforcement officers at all of these levels are required to have a crime-free background and must successfully pass entrance screening and examinations. They are required to complete formalized training in all variables of the job, including a working knowledge of laws, policies and procedure, the deadly force policy and associated continuum, and regular firearms training and proficiency testing. Applicants applying for the FBI, as well as many other federal law enforcement agencies, must have a four-year college degree from and accredited institute of higher learning, be a U.S. citizen and have at least three years of previous work experience. Lastly, these law enforcement officers are paid by the government, at whichever level, and significantly must answer to the people they have sworn to protect.

On the contrary, private sector security in this instance refers to a person hired by privately owned organizations to act as a guard. These guards are hired to protect private sector assets that may include property, personnel and proprietary information. Private sector security guards do not have law enforcement powers and, therefore, are limited in their abilities to generally observe and report real or perceived violations of the law to law enforcement authorities. They are not authorized to use force and may not make arrests. This fact becomes especially concerning to the public as some security

[106] Total cost estimates denoted as $40 million and $50 million are taken from documents denoted in footnotes 10 and 11, respectively. Office of Homeland Security, *National Strategy for Homeland Security*, 77.

companies deploy guards equipped with firearms and maintain little to no proficiency requirements. In general, guards act as a deterrent to crime. Significantly, private sector security is accountable to the person/organization that pays them. A contributing factor to private sector security is the disparities in the pay scale. Some private sector security guards make little more than minimum wage. Ominously, there are no universal standards within the private sector security apparatus. There are no minimum training criterions, educational minimums, background checks or even citizenship requirements.[107]

The private sector thinks about security much differently than the government does. Security is not fundamental to daily business. Instead, security is an additional cost of doing business. It is a drain on profits and must therefore be weighed carefully. A business's allocation of security is based on the probability something bad will happen. Within limited operating budgets, organizations must make calculated decisions on where best to allocate resources to reduce the risk of something malicious occurring. Risk is measured as:

Risk = Threat x Vulnerability x Consequences.

Simply, security budgeting can be equated to gambling. Private businesses take calculated chances on how robust their security postures should be in order to address real or perceived threats, their known weaknesses and the results or outcome should the business succumb to a breach.[108]

E. THE MARRIOTT INTERNATIONAL, INC.

The private sector is a sundry of all things non-state owned. The U.S. economy thrives on privately owned and operated assets not only within the U.S. but also outside of its borders. American owned and operated companies have an extensive footprint in foreign lands, which makes them extremely important to the stability of the global

[107] Cassandra Cochrun, "What are the Differences between Private and Public Sector Security?" n.d., http://www.ehow.com/about_5106799_differences-private-public-sector-security.html (accessed September 8, 2012).

[108] Ted Lewis and Rudy Darken, Critical Infrastructure: Vulnerability, Analysis and Protection course (course notes, Naval Postgraduate School, Monterey, CA).

economy. To demonstrate the magnitude of its reach and capabilities, the Marriott International, Inc. ("Marriott") will be examined. According to the Marriott, "Travel and tourism is one of the world's largest industries."[109] Because of its popularity, appeal, international ties and impact on global economics, the vastness of Marriott's assets, capabilities and workforce will be reviewed as an example of one small piece of what the private sector offers.

The Marriott is classified as part of the commercial facilities sector and finds its home within the lodging sub-sector. Despite this categorization, the Marriott straddles other private sector delineations—frankly, as do most private sectors. In fact, the Marriott is dependent upon countless other sectors in order to function. For example, they rely upon the transportation sector to receive needed supplies; the telecommunications sector to stay connected with customers and the financial and banking sector to safe keep their operating funds.

The Marriott affords accommodations both within the continental United States and across the globe. There are 18 separate brands within the Marriott portfolio, including recognizable names like the Ritz-Carlton, Renaissance Hotels and the Fairfield Inn and Suites. Significantly, Marriott diversified to include "limited service to luxury hotels and resorts."[110] A part of this collection also consists of executive apartments, furnished extended-stay locations and convention centers.[111] Within a number of the Marriott's assets, there are restaurants and bars often frequented by non-registered hotel guests. Likewise, countless both registered and non-registered guests attend conferences, seminars and other special events at Marriott assets.

Marriott owns and operates "more than 3,700 properties in over 73 countries and territories."[112] From 2010–2011, the corporation reported owning and operating 643,196

---

[109] Marriott, "Corporate Responsibility," n.d., http://www.marriott.com/corporate-social-responsibility/corporate-responsibility.mi (accessed September 6, 2012).

[110] Marriott, "Marriott," n.d., http://www.marriott.com/culture-and-values/jw-marriott-jr.mi (accessed September 5, 2012).

[111] Ibid.

[112] Ibid.

rooms world-wide.[113] Marriott employs approximately 300,000 [people] across the globe.[114] Moreover, Marriott employment opportunities are as diverse as their portfolio. Marriott careers are two-pronged—managerial and non-managerial—and are broken down into major thematic categories: accounting and finance; revenue management; food and beverage; rooms operations and guest services; and sales and marketing.[115] Marriott recorded over $12 million in proceeds for the 2011 fiscal year.[116]

The magnitude of the Marriott's domestic and international influence is phenomenal. They provide overnight accommodations for hundreds of thousands of individuals around the clock and around the globe. Similarly, their hospitality services are used for meetings, seminars, conferences and special events. The Marriott hotels are located in some of the most sought after locations in the world. Equally, they are located in several non-permissive environments in high-risk countries that are not generally thought of as tourist attractions. Perhaps most significantly, Marriott hotels are seen as beacons of American capitalism and prowess. By virtue of their symbolism, U.S.-based companies such as the Marriott are often targeted by those seeking to destroy not only western ideals but certainly the U.S. Indeed, many westerners and Americans in particular find their home away from home, especially in unfriendly territories, in American-owned corporations such as the Marriott.

The Marriott has always emphasized security and safety for its customers. Their protocols and assessments are compliant with Department of Homeland Security and Department of State procedures.[117] As the Marriott corporation began expanding into the overseas marketplace, so too did they expand their internal security protocols. They created a crisis management package, authored a crisis manual and selected crisis teams.

---

[113] Marriott, *Marriott 2011–2012 Sustainability Report*, 2012, http://www.marriott.com/Multimedia/PDF/CorporateResponsibility/MarriottSustainabilityReport_2011and2012condensed10MB.pdf (accessed September 5, 2012), 11.

[114] Marriott. "Marriott."

[115] Ibid.

[116] Marriott, *Marriott 2011–2012 Sustainability Report*, 9.

[117] Marriott, "Safety and Security Information," February 1, 2012, http://news.marriott.com/safety-and-security-information.html (accessed September 8, 2012).

They engaged in rigorous training including table top exercises. The Marriott receives countless intelligence assessments and bulletins to maintain visibility on the state of world affairs. They employ full-time intelligence analysts based in both Washington, D.C. and Hong Kong, which provides the company with "twenty-four hour capability of assessing risk."[118] They also developed a coded system equated to threat conditions. The cycle consists of Blue, Yellow and Red, blue being the lowest and red the most severe level of security. Marriott highlighted, "Our risk assessments are critical to the allocation of resources." The Marriott has created further training for security guards located in high-risk areas. In the aftermath of the Mumbai attacks, they authored an active shooter training program "combining physical security with operational security and awareness programs." [119]

Despite their best efforts, the Marriott is no stranger to terrorism attacks. In today's threat environment, "…yesterday's embassies are today's hotels. The threat against diplomatic targets persists but due to target hardening, the terrorists seek to attack international hotels. As westerners frequent international hotels, they should be considered second embassies."[120]

From 2004 to 2008, the Islamabad Marriott hotel was attacked three times. The attack on September 20, 2008 was considered the most dramatic and devastating as a vehicle-borne improvised explosive device carrying a payload of approximately 600 kg (1,320 pounds) of explosives was detonated by its suicide driver. While the vehicle was stopped from entering the hotel premises by security barriers, it somehow ignited and ultimately burned for two days. The attack injured 265 and killed 56 people many of whom (30 people) were hotel staff employees.[121]

---

[118] "Statement of Alan Orlob, Vice President Corporate Security and Loss Prevention, Marriott International Lodging; On behalf of the Real Estate Roundtable American Hotel and Lodging Association; Before the Senate Committee on Homeland Security and Government Affairs; Hearing on Lessons from the Mumbai Terrorist Attacks, Part II," January 28, 2009, www.hsgac.senate.gov/download/012809orlob (accessed September 5, 2012).

[119] "Statement of Alan Orlob."

[120] Rohan Gunaratna, *The Islamabad Marriott in Flames: Attack on the World's Most Protected Hotel* (Singapore: International Centre for Political Violence and Terrorism Research, 2008), 3.

[121] Gunaratna, *The Islamabad Marriott*, 2.

Prior to the Marriott attack, the security posture consisted of 62 CCTV cameras monitored full-time by three security personnel. The training of their CCTV monitors is unknown. Additionally, windows were reinforced with blast retention films in order to diminish the amount of glass fragmentation during blow-out. They had bolstered vehicle inspections to include under-vehicle inspection cameras and license plate recorders projected into their manned security booth. Manned security, totaling 196 security personnel and four explosives trained K-9s, were both visible and covert and included armed security at the hotel's entrances. In addition, the Marriott had expanded the street to hotel stand-off distance and installed more security barriers including the emplacement of new bollards, drop-down and "hydraulic Delta barriers."[122] After the attack and as a result of greater industry awareness, the Marriott's security posture changed to include the security enhancements described in the next section.

F. LESSONS LEARNED: NEW SECURITY ENHANCEMENTS

After the Islamabad attack and the Mumbai assault, the Marriott collaborated to identify lessons learned for properties in high-risk environments. In part, they realized terrorists often stay at their target hotels disguised as guests. They use their rooms as staging areas and command posts providing unfettered access to the hotel's layout and internal procedures. To mitigate this, Marriott developed awareness training so hotel employees can recognize suspicious activity. Additionally, when practicable, undercover counter-surveillance teams were identified, trained and deployed to detect hostile reconnaissance activities.

Marriott found responders were unfamiliar with building lay-outs as most of the plans they had been supplied were outdated. They encouraged all of their hotels to develop relationships with local authorities and to conduct joint training. Lastly, they provided up-to-date building architecture plans to first responders in an effort to eliminate unnecessary delays in responding to an incident. Marriott also suggested distributing recent and comprehensive pictures and applicable video footage to their authorities.

[122] Gunaratna, *The Islamabad Marriott*, 7–8.

From the Mumbai attacks, it was learned the Taj Hotel executives decreased their security posture allegedly as a result of information provided by Indian powers that be.[123] The resultant lessons learned included building an in-house intelligence capability where manageable. Resultantly, security personnel training in the identification and interpretation of threat indicators can determine mitigation actions that can then be executed by hotel staff. Finally, it was determined that enhanced physical security measures significantly slow and may even deter an attack.[124]

Marriott ensures each property has employed a number of additional security measures such as on-going staff training, available traveler safety tips, no room numbers on room keys and secondary deadlock bolts. Furthermore, Marriott developed security procedures. Unfortunately, these procedures are proprietary and therefore unavailable for review by the public. Finally, Marriott hotels are required to have up-to-date emergency plans. At the very least, the plans are required to include "fire protection systems and procedures, natural disasters, procedures for handling immediate evacuation of the hotel, emergency reporting procedures, power failures and terrorism." These plans too are unavailable because they are confidential.

G. MARRIOTT'S ABILITIES

The Marriott's capabilities are immense. As has been discussed, the Marriott workforce exceeds 300,000 people, including expertise in countless job roles with varying responsibilities. The size of its staff provides law enforcement with access to potential sources and front line detectors of suspicious activity. Indeed, an improvised explosive device attack on the Marriott in Jakarta discovered the "control-centre (for the terrorists) was a room at the JW Marriott, room number 1808, where anti-terror police found explosive materials and an unexploded bomb."[125] Certainly, the Marriott's housekeeping staff may have been the first to stumble onto this operation as they went

[123] There was no further information available as to exactly who or specifically which Indian authority provided the alleged information to the Taj hotel executives.

[124] "Statement of Alan Orlob," 4.

[125] B. Raman, "Terrorist Target Hotels Again: This Time in Jakarta; International Terrorism Monitor" (Paper no. 543), July 17, 2009, South Asia Analysis Group, http://www.southasiaanalysis.org/%5Cpapers34%5Cpaper3310.html (accessed September 7, 2012).

about their daily duties. Training the staff to look for suspicious activity is crucial for the early detection of possible plots. Simply, the staff is an enormous underutilized intelligence base. Equally, the diversity of the private sector's staff presents language skills and capabilities not necessarily intrinsic to or readily at the disposal of the government.

As further described, the Marriott employs aggressive security measures including physical security enhancements, manned security staff and CCTV. The CCTV coverage in particular is extremely useful to law enforcement whether it is during an event or previously recorded footage that can assist in an investigation. CCTV footage is evidence and is always deemed important. As was validated during the review of CCTV coverage from the Islamabad attack, the security staff responded in accordance with Marriott's established policies and procedures. In fact, the actions of the security staff undoubtedly saved countless lives.

Lastly, the private sector as a whole has assets all over the globe. As exhibited by this example, the Marriott has a foothold in 73 different countries around the world. This affords law enforcement access to friendly locations wherein both intelligence and overt operations can take place. It allows for some measure of control in often times non-permissive environments and conflict zones.

H. PRIVATE SECTOR CHALLENGES

Information sharing has been and remains of paramount importance to the success of the protection of private sector assets. Arguably, the private sector is more innovative and assertive when it comes to information sharing. Notwithstanding, the private sector recognizes the necessity of protecting proprietary information. Even so, private industry places more emphasis on the need for and necessity of sharing actionable information whereas the government often maintains the "need to know" posture in respect to sharing information. Regardless, overwhelming cultural differences between the two remains a hurdle. Furthermore, the development of trusted relationships and a workable information sharing platform also remain challenges.

There are economic pressures attached to both security and engagement with law enforcement. The private sector walks a fine line between security and maintaining an open, inviting and appealing façade. The public wants to feel safe, yet open and free to move around unfettered. This proves challenging for the private sector's security apparatus as an overly visible security presence may be seen as a turn off. Probably most importantly, the private sector is in the business of making money. Because of this, they have to balance their security costs against their projected profits. Certainly shareholders are not going to stand for reduced earnings in exchange for amplified security measures countering a risk that may never come to light.

The private sector must weigh the impact of negative press against future returns. For instance, if the Marriott chooses to neglect security measures which results in the loss of life will their decision withstand the scrutiny from the news media? How will the company's lack of response be perceived among its customers, stakeholders and future customers? Unlike the government which does not rely on generating revenue, the members of the private sector must ensure their public message and image are always favorable.

The Marriott is extremely forward-leaning in training its employees on security and crisis management. Similarly, they teach all of their employees about suspicious activity and threat indicators. Undeniably, people play as they practice. In other words, vigorous training for any number of stressful situations will pay dividends in the long run. According to author Rohan Gunaratna:

> Both the security and non-security personnel at the Islamabad Marriott had conducted exercises on emergency evaluation. In a crisis, most security and non-security staff are likely to respond the way they have been trained. In the crucial seven minutes, several hundred lives were saved because Marriott security and non-security staff collaborated to move guests away from harm's way. If not for the staff training and exercises, several hundred guests might have become casualties.[126]

[126] Gunaratna, *The Islamabad Marriott*, 14.

Arguably, good training leads to good intelligence. Knowing what to look for and what the identified inconsistencies could mean may prove to be incredibly helpful for law enforcement.

The U.S. government should interact with the private sector at all levels. Government outreach initiatives target varying levels of private sector engagement. Importantly, law enforcement in particular stands to gain more from an inclusive relationship. It is necessary to recognize that everyone is important within the private sector. As has been discussed, it is most certainly the housekeeping staff who will discover nefarious activities taking place in a hotel room they are charged to clean—not the global security executive who may sit thousands of miles away.

I. IN SUMMARY

Without the private sector many significant aspects of an American's everyday life would be drastically altered. As has been demonstrated, the private sector accounts for not only the production of what we eat but also where we shop, how we travel and how we stay connected with the world. The magnitude of the private sector's influence on everyday lives is astounding. Moreover, the private sector is the backbone of the U.S.'s economy and a significant player in the global economy.

The private sector is truly an underutilized asset. Their infrastructure, personnel and germane security are, in many respects, beyond reproach. The Marriott hotel example makes evident what one corporation brings to the table. Truly, "to integrate and synergize capabilities, government-private sector partnership is crucial. To better understand and respond to the threat environment, future hotels [and the private sector as a whole] should build robust and lasting partnerships with the government."[127] Indeed, developing a trusted relationship with security officials, such as within the Marriott, will likely result in access to internal, proprietary security protocols that may then be shared to other trusted partners.

[127] Gunaratna, *The Islamabad Marriott*, 14.

As an example, the Marriott has the ability to influence government outreach efforts by providing real-life examples of how best to secure their assets with the U.S. and in both friendly and hostile environments overseas. They are seasoned and experienced having learned through trial and error. The Marriott can teach others how to employ an analytical staff to assist in assessing risk from threats both within and outside of the U.S. Also, the Marriott experience in developing and deploying innovative and comprehensive crisis plans. As has been described, the Marriott can support others in best practices for operating outside of the United States. Lastly, because Marriott is a demonstrated leader in corporate security, they can significantly assist others both within and outside of the private sector by sharing their in-house staff training platforms. In all, Marriott is a first-rate example of a company with an innovative, ever evolving security mindset that can benefit others.

There are dozens of private companies such as the Marriott that the U.S. government and FBI could better utilize for improved security against terrorism within the U.S. The question remains on how best to mobilize them. The next chapter considers how the U.K. addresses this challenge within the four corners of their counterterrorism strategy. Three premier U.K. private sector outreach programs will be examined to include a comparison between the U.K. and the U.S.

VI. AN EXAMINATION OF THE UNITED KINGDOM'S EFFORTS

A. THE UNITED KINGDOM AS A MODEL

This chapter will discuss CONTEST, the United Kingdom's (U.K.) strategy for national security. It will delve into a number of British outreach programs including *Project Griffin*, *Project Argus* and *London First* identified as examples of integration of the private sector into national security. Finally, the chapter will culminate with a side-by-side comparison between the U.K. and U.S. programs.

B. HOW THE U.K. SUCCESSFULLY ENGAGE THE PRIVATE SECTOR

The United Kingdom's counterterrorism strategy, as set forth by the Home Office,[128] is in its third iteration and is known by the moniker "CONTEST." CONTEST's primarily goals are to address the terrorist threat posed by al-Qa'ida and its affiliated groups as well as the danger from Northern Ireland Related Terrorism (NIRT).[129] The strategy states, "The aim of CONTEST is to reduce the risk to the U.K. and its interests overseas from terrorism, so that people can go about their lives freely and with confidence." CONTEST takes into account the rule of law and personal rights and protections. Moreover, through CONTEST and in conjunction with the Strategic Defence [*sic*] and Security Review (SDSR), the U.K. understands that in order to fully defeat terrorism, not only must the immediate threat be addressed but also the long-term factors that contribute to terrorism and radicalization. They realize the importance of integration with other agencies and programs is absolutely necessary.[130]

---

[128] The United Kingdom's Home Office is the government agency in charge of immigration, security and order. Within the Home Office are the police, Border Security, and their intelligence component, Security Service (MI5). The Home Office sets policy for counterterrorism, drugs, ID cards and other security-related matters. *Wikipedia*, s.v. "United Kingdom's Home Office," n.d., http://en.wikipedia.org/wiki/Home_Office (accessed March 14, 2012).

[129] United Kingdom Home Office, *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, 2011, http://www.homeoffice.gov.U.K./publications/counter-terrorism/counter-terrorism-strategy/contest-summary?view=Binary, 3, 5 (accessed November 18, 2011).

[130] United Kingdom Home Office, *CONTEST*, 3, 5.

CONTEST is centered on four main principles: "Pursue—to stop terrorist attacks; Prevent—to stop people becoming terrorists or supporting terrorism; Protect—to strengthen our protection against a terrorist attack; and Prepare—to mitigate the impact of a terrorist attack."[131] Within this framework the U.K. does an admirable job of integrating the private sector—especially regarding the context of Protect.[132] For purposes of this comparison, however, only the Prevent and Prepare subcategories will be considered.

Prevent has been designated as a key component of the CONTEST strategy. Within Prevent, the U.K. has renewed efforts to ensure the Prevent prong is more effective and has changed its scope to include thwarting all forms of radicalization. The U.K. recognizes the importance of free speech and therefore will not seek to change any of its laws. Rather, it will promote healthy discourse in regard to terrorists' rhetoric. Within Prevent, the U.K. will work to empower communities, improve social integration and mobility.[133] Notably, the U.K.'s successful hosting of the 2012 international Olympic Games is evidence of their commitment to the flawless execution of their strategy.

The Prepare category has a more general response allowing for maximum flexibility to address any number of situations. The U.K. has outlined success within Prepare to include:

- Our planning for the consequences of all civil emergencies provides us with the capabilities to respond to and recover from the most likely kinds of terrorist attacks in this country
- We have in place additional capabilities to manage ongoing terrorist attacks wherever required; and
- We have in place additional capabilities to respond to the highest impact risks.[134]

---

131 United Kingdom Home Office, *CONTEST*, 3, 5.

132 Ibid., 12, 13.

133 Ibid., 8, 9.

134 Ibid., 14.

As the U.K. *National Security Strategy* opines, "…we need to build a much closer relationship between government, the private sector and the public when it comes to national security."[135] The strategy advocates for a "whole of government" approach to national security.[136] The integration of the private sector is specifically highlighted within Prepare stating:

> Moreover, we also depend on close relationships with the private sector, who own much of the infrastructure and the systems that need to be protected. We will continue to be as transparent as we can in sharing our understanding of the threats we face and wherever possible will collaborate in the development of security solutions.[137]

It is within this spirit that the U.K. integrates the private sector as full partners in securing their country, specifically within their *Project Griffin*, *Project Argus* and *London First* outreach programs.

C. AN OCEAN APART, YET CLOSER THAN WE THINK

The United Kingdom is no stranger to conflict. Throughout their storied history they have been involved in wars and other skirmishes both at home and abroad. They are especially practiced in dealing with guerilla warfare and later terrorism stemming from the unrest between the British government and Northern Ireland. More recently, however, the U.K. experienced an al-Qa'ida-inspired terrorist attack perpetrated by its own citizenry. A group of four British-born young men killed 52 people and injured more than 700 on July 7, 2005 when they executed a coordinated attacked on the U.K.'s public transportation system during the morning rush hour. The BBC reported the homegrown violent extremists were "motivated by a 'fierce antagonism to perceived injustices by the West against Muslims' and a desire for martyrdom."[138]

---

[135] *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, 2010, http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy (accessed November 19, 2011).

[136] Ibid., 12.

[137] Ibid., 11, 12.

[138] "7 July Bombings: Introduction," *BBC News*, n.d., http://news.bbc.co.uk/2/shared/spl/hi/uk/05/london_blasts/investigation/html/introduction.stm (accessed April 21, 2012).

Resultantly, to better defend itself, the U.K. welcomed the idea of integrating its population, especially security professionals within the private sector, into its overall national security apparatus. The U.K. accomplished the assimilation by way of the creation of a variety of specifically designed private sector outreach programs. Are there lessons that the U.S. can learn from the British integration? A comparative analysis of three of the U.K.'s outreach initiatives are described herein. The projects examined included: *Project Griffin, Project Argus* and *London First.*

D. PROJECT GRIFFIN

Project Griffin was born within the City of London[139] Police Department and was officially underway in April 2004 as a collaborative endeavor between the City of London Police and the Metropolitan Police. The project is completely voluntary and not-for-profit. The *Project Griffin* Webpage suggests, "Its remit was to advise and familiarize managers, security officers and employees of large public and private sector organisations across the capital on security, counter-terrorism and crime prevention issues."[140] Because of its effectiveness and adaptability, *Project Griffin* has been deployed throughout the United Kingdom and has even been exported internationally to places such as Australia, the United States, Singapore, Canada and Hong Kong. The impetus behind the project was to develop a comprehensive, community-based approach to thwarting threats from terrorism. The project incorporates, among others, the police, business and private sector.[141] The project's primary mission is to:

> …engage, encourage and enable members of the community to work in partnership with the police to deter, detect and counter terrorist activity and crime. Project Griffin seeks to enlist the help and support of individuals or groups responsible for the safety and security of buildings,

[139] For clarity, the City of London lies within central London, England and encompasses an area of approximately one square mile. Notably, the City of London, among other things, maintains its own police force. *Wikipedia*, s.v. "City of London," n.d., http://en.wikipedia.org/wiki/City_of_London (accessed November 18, 2011).

[140] "Project Griffin," n.d., http://www.projectgriffin.org.U.K./ (accessed June 22, 2102).

[141] Ibid.

> businesses, districts or neighbourhoods. It provides an official and direct channel through which the police can share and update vital information relating to security and crime prevention.[142]

Project Griffin targets security managers and lower-level security personnel. Approximately 24,000 security professionals have been trained throughout the U.K. and internationally, according to the City of London *Griffin* team.[143] *Project Griffin* training benefits both law enforcement and the private sector in immeasurable ways. For example, security professionals receive the same, standardized training which, among other things, ensures uniform reporting and reporting protocols. Assets are undoubtedly better protected and the trained community becomes the "eyes and ears" for the police—able to identify and report things such as hostile reconnaissance and suspicious activity. It is estimated that a majority of the police's tips and leads come from *Griffin* alumni.[144] *Project Griffin* accomplishes its mission vis-a-vi a four pronged approach: *Griffin* Awareness Days, an On-Line Refresher Course, Bridge Calls and Public Assistance.

Griffin's Awareness Day is a day-long indoctrination training session consisting of a number of briefings provided by police officers. The topics vary and start with a chilling video memorializing a number of terrorist attacks throughout the world. The first agenda item is a very detailed, thorough threat briefing provided by Special Branch.[145] Spoken in laymen's terms, the threat briefing delivers a comprehensive account of the most notable terrorist organization threatening the U.K.—al-Qa'ida. The briefing outlines the history of al-Qa'ida, highlights al-Qa'ida's goals and objectives and provides a time-line recollection of major al-Qa'ida operations culminating with the 9/11 attacks on the U.S. The segment also touches on al-Qa'ida today and threats faced from al-

---

[142] "Project Griffin."

[143] Ian Mansfield, Teresa Russell, Matt Hone, and Trevor Dyson in discussion with author, January 12, 2012.

[144] Ibid.

[145] Special Branch is part of the Metropolitan Police's Counter-Terrorism Command, SO15. Special Branch is responsible for, among other things, national security matters, protection of VIPs (non-royal), sea and airport examining officers and intelligence work. Special Branch works hand in glove with MI-5. *Wikipedia*, s.v., "Special Branch," n.d., http://en.wikipedia.org/wiki/Special_Branch (accessed June 22, 2012).

Qa'ida-inspired homegrown radicals. Additionally, because of its significance to the U.K., Northern Irish Related Terrorism is discussed.

The Awareness Day carries on with other comprehensive briefings, such as recognizing explosive devices. This discussion hits upon topics such as person-borne improvised explosive devices and vehicle-borne improvised explosive devices. Crime scene management and current crime trends and methods of operation are also discussed. Briefings on the subjects of identifying suspicious activity and hostile reconnaissance provide attendees with examples of nefarious activity. The goal is for each participant to walk away from the training with an understanding of how suspicious activities may manifest themselves—albeit criminal or terrorist in nature. Importantly, the group is trained to recognize hostile reconnaissance. Distinguishing pre-operational surveillance may very well be a key to thwarting an intended evil action—the importance of which is not underestimated by the *Griffin* staff.

Armed with these indicators, the goal is to teach the participants about nefarious activities and raise their levels of understanding and alertness. Consequence management is discussed with special emphasis placed on business continuity of operations. At the end of the training course, each participant receives a *Project Griffin* certificate and becomes part of the network of *Griffin* graduates. *Griffin* training has become so popular and well respected it is "fully endorsed and supported by the Security Industry Authority (SIA)[146] and Skills for Security."[147] *Griffin* graduates form an interconnected net that blankets the city (of London, in this example) able to assist the local police force by virtue of their heightened awareness and basic training in recognizing things/activities that, for them, are out of the ordinary.

The On-Line Refresher Course is an interactive, scenario-based computer module. The refresher rehashes some of the Awareness Day training and serves as a simple and

[146] The Security Industry Authority is governing body responsible for setting, maintaining and regulating the private security industry within the U.K. "Home Office," n.d., http://www.sia.homeoffice.gov.U.K./Pages/home.aspx (accessed March 21, 2012).

[147] "Project Griffin." "Skills for Security, the skills body for the security industry, works with employers to improve security skills and standards of professionalism, by providing access to security training courses and security qualifications, for people employed in private security roles across the U.K.." "Skills for Security," n.d., http://www.skillsforsecurity.org.U.K./ (accessed March 21, 2012).

cost effective method for *Griffin* registered personnel to stay informed and receive important messages from the police without having to leave their home or office. A year after completing the *Griffin* Awareness Day, graduates are eligible to partake in the refresher course. The refresher consists of an hour long series of "interactive, video clips and question and answer sections guiding learners as they work through each module."[148] In each, various scenarios are presented to the participant who must "select the correct course of action" in order to successfully complete and receive recognition for the course.[149] Upon completion, participants are better attuned to the latest techniques, tactics and procedures used by terrorists and criminals. Moreover, scenarios may be viewed multiple times to ensure the delivered message and the proper courses of action are understood by the student.

Bridge Calls are used to push information very quickly to the *Griffin* network. They occur regularly and may take place using a SMS, email, pager or conference calls. Bridge Calls, by whatever method chosen, are an excellent way for critical information to reach a large audience very quickly. They assist in keeping the community both informed and aware of events that may affect them. Information delivered may include "updates and intelligence on terrorism/extremism and other crime-related issues. They are also used for specific local situations, such as measures to be employed in times of an emergency."[150] Importantly, based upon the communication received, security personnel are able to react—perhaps resulting in 100 percent identification checks or vehicle sweeps with a canine.

Public Assistance may be called upon in times of emergency. For instance, the police may muster *Griffin* graduates to assist with cordons or perhaps a high visibility neighborhood watch.[151] In fact, *Project Griffin* alumni assisted officials in the aftermath of the 7/7 bombings in London. They were asked to help with spearheading general public awareness and guide the community on how to react to a terrorist event. And,

---

148 "Project Griffin."

149 Ibid.

150 Ibid.

151 Ibid.

Griffin alumni were tasked to display a heightened presence of security staff so as to provide a visible message of reassurance.[152] The formation of a well-informed, uniformly trained brigade of private citizenry is a force multiplier for police—especially in crisis situations. Notably in April of 2009, "*Project Griffin* guards deployed for [the] G20."[153]

In sum, *Project Griffin* is a very effective police outreach program that enlists the influence and passion of the public by empowering them to recognize and report suspicious activity, become cognizant of current threats, gather and share information, garner and maintain trust in the police and feel like part of the solution to problems facing their community. *Project Griffin* is also recruiting the participation of highly targeted infrastructure such as Gatwick Airport—the first airport to join *Griffin*—effective March 2008 and, as of January 2010; *Griffin* is piloting a project with the Safer Transport Command with London Buses.[154]

E. PROJECT ARGUS

Project Argus was started in 2007 and dovetails with *Project Griffin*. While in the same vein, *Argus* differs in that it is program-managed by the National Counter Terrorism Security Office (NaTSCO). The NaCTSO:

> …is a police unit co-located within the Centre for Protection of National Infrastructure….(CPNI)…. NaCTSO contributes to the U.K. government's counter terrorism strategy (CONTEST) supporting the Protect and Prepare strands of the strategy…. NaCTSO counter terrorism and security work is divided into three areas: Protection of crowded places; Protection of hazardous sites and dangerous substances; and Assisting the CPNI to protect the Critical National Infrastructure.[155]

The *Project Argus* initiative was designed to assist businesses, whether small, individually owned or national chains, to plan for, prevent, handle and recover from a

---

[152] David Warner (SO20 Counter Terrorism Protective Security Command at New Scotland Yard), personal correspondence, June 2012.

[153] Ibid.

[154] Ibid.

[155] National Counter Terrorism Security Office, "NaCTSO: Who We Are and What We Do," n.d., http://www.nactso.gov.uk/Default.aspx (accessed June 22, 2012).

terrorist attack. The project accomplishes these tasks by directing businesses through a simulated terrorist attack. The driving idea behind the exercise is to demonstrate the significance of being involved in a major terrorist event, identifying lessons learned, and developing best practices that will ultimately protect the individuals' businesses, their staff, assets, customers and overall community.[156]

The *Argus* training is a free event and focuses on decision makers versus the private sector's lower-level security professionals pin-pointed in the *Griffin* training. *Project Argus* employs the use of technology to reach a wide audience at little expense to the customer. *Argus* uses an interactive DVD that presents a number of terrorist situations from a night club scene to a Mumbai-style hostile attack.[157] The *Project Argus* DVD is an approximately two to three hour multi-media simulation exercise during which the participants make decisions and answer questions in a workbook they keep as a reference. Among other things, the scenarios focus on spotting and assessing hostile reconnaissance. This project encourages private sector security decision makers to consider their current reaction plans for handling an unexpected event. Topics include: shelter-in-place versus evacuation, contingency plans and planning, "go kits" and continuity of operations plans. [158]

Project Argus cuts across traditional sector specific lines and encourages community and neighborhood involvement. *Argus* inspires information sharing beyond established personal relationships and endeavors to inform versus alarm its constituency.[159] The exercise is designed around "a series of questions and challenges… [which] are put to…[the participant], both individually and as a group. [Each participant]…will work in small syndicate groups with other local business representatives and develop… [appropriate] responses to the attack."[160]

---

[156] National Counter Terrorism Security Office, "NaCTSO."

[157] Richard Prior (Inspector, New Scotland Yard), personal meeting, January 12, 2012.

[158] This information originated from a personal meeting with members of the National Counter Terrorism Security Office (NaCTSO); London, England; January 11, 2012.

[159] Prior, personal meeting.

[160] National Counter Terrorism Security Office, "Project Argus," n.d., http://www.nactso.gov.U.K./OurServices/*Argus*.aspx (accessed March 18, 2012).

In addition to the business-focused *Project Argus*, the NaCTSO launched *Argus Professional* in 2008. *Argus Professional* is designed:

> …to target planning, architect and design professionals to raise awareness of designing in counter terrorism protective security measures at the design concept stage. These professions have been identified as being able to play a significant role in reducing vulnerability, hence the aim of Argus Professional is to encourage debate, and demonstrate that counter terrorism measures can be designed into structures and space to create safer crowded places.[161]

The success of both Projects *Griffin* and *Argus* should not be understated. The programs are highly touted by both the police and private sector. For example, the private sector found that participation in these two projects identified a major gap in their own security in that they found private businesses were not talking with each other. Participation in these projects highlighted this kink and facilitated a solution through community interaction vis-a-vi Projects *Griffin* and *Argus*. Part of the solution, simply stated, involved meeting fellow neighbors and exchanging contact information. Moreover, membership in these projects enables private security staff to access, share and gather information that was otherwise unavailable or not shared—it is now only a telephone call away.[162]

F. LONDON FIRST

London First is a not for profit delegation representing 32 industries and blue-chip London-based businesses serving to bring together the government and private sector. The project identified 24 specific sectors such as "financial and business services, property, transport, ICT, creative industries, hospitality and retail."[163] *London First's* membership "also includes higher education institutions and further education colleges."[164] Within each division, representatives were chosen to act as a principal lead for the distribution and collection of information from within their respective regions.

---

[161] National Counter Terrorism Security Office, "Project Argus."

[162] Rajeev Pradham (Operations Director for Lynx), personal meeting, January 13, 2012.

[163] "London First," n.d., http://www.londonfirst.co.uk/about-us/ (accessed June 22, 2012).

[164] "London First."

The sector leads are conduits between information provided by the police and the sharing of that information throughout their own trusted subdivision networks. *London First* hinges on the understanding that sharing information with the private sector is paramount.[165] *London First* sets forth to "…provide our members with an effective conduit for communication with [the] government and [establish] a voice in the public arena."[166]

London First, in cooperation with th**e** National Counter Terrorism Security Office, Metropolitan Police, produced and distributed pamphlets to local entities across the U.K. The brochure's topics included, among others, counter terrorism and continuity of business operations. Inasmuch as London was the host city for the 2012 Olympic Games, through *London First's* Security and Resilience Network, materials such as "London 2012 Olympic and Paralympic Safety and Security Strategy (2011) and "Home Office London 2012 Olympic Safety and Security Strategic Risk Assessment (OSSSRA) and Risk Mitigation Process (2011)" were made available to the network of *London First* participants.[167] It is estimated, prior to the distribution of Olympics materials, over 500 businesses were positively affected by the literature. This endeavor has been touted as a success through *London First's* Safer Business focused efforts.[168] Arguably, the achievement lies in the vastness of the distribution of information and the connectivity it encouraged and facilitated.

As mentioned above, within *London First* sits the Security and Resilience Network. The network encourages the police, security services and businesses to work jointly in furtherance of promoting safety, building resistance and thwarting terrorism and other crimes. The Resilience Network is "supported by the Metropolitan Police, City of

---

165 Chris Wilson (London First member) and Graham Brown (Communities Together Strategic Engagement Team), personal meeting, January12, 2012.

166 "London First."

167 "Security and Resilience Network: Guidance," n.d., London First, http://www.londonfirst.co.uk/networks2/security--resilience/security-and-resilience-networ2/ (accessed June 21, 2012).

168 "Our Sucesses," n.d., London First, http://www.londonfirst.co.U.K./our-successes/, (accessed April 26, 2012).

London Police, British Transport Police and the Home Office."[169] To exemplify their information sharing capabilities, "police message alerts" are dispatched during crisis events. These alerts are "cascaded by *London First*."[170] Members actively collaborate to produce publications outlining best practices and other guides in addition to playing a part in exercises designed by police, security and business experts. The Network, as highlighted above, ensures useful guides are available to its constituency covering a variety of topics, aside from the Olympics, to "Secure in the Knowledge: Building a Secure Business" and "Chemical, Biological and Radiological Threats: Good Practice for Business." [171] The Network provides "one stop shopping" for businesses seeking advice, best practices or simply information on unfamiliar topics. Equally important, is the material is all available on-line and at no cost to the customer.

Cooperation with the police has proven to be unparalleled within *London First's* Leadership Exchange program. The scheme "encourages the sharing of leadership and management expertise to improve [the] operational effectiveness of London's police services."[172] The Leadership Exchange is an innovative approach to bridging the gap between business and police leaders. In the hopes of bringing together years of knowledge and experience, the Leadership Exchange partners capable leaders, on a voluntary basis, from business and police and fosters information sharing in a "joint mentoring scheme."[173] It is estimated that over 400 individuals have participated in the program since its creation in 2001.[174]

Attendees of the program from the private sector are senior, executive-level managers within their respective business. The law enforcement participants are similarly comprised of senior police officers and staff from the three principle police

---

[169] "Networks," n.d., London First, http://www.londonfirst.co.U.K./networks2/ (accessed March 18, 2012).

[170] Ibid.

[171] "Security and Resilience Network."

[172] "Making a Difference," n.d., London First, http://www.londonfirst.co.U.K./about-us/making-a-difference/ (accessed March 18, 2012).

[173] Leadership Exchange, *Sharing Expertise between Police and Business Leaders* (London: Leadership Exchange, n.d.), 4.

[174] Ibid., 4.

forces across London, "and increasingly from services across the U.K."[175] The underpinnings of the program are to exchange knowledge on leadership, swap management best practices and lessons learned as well as develop a better understanding of the challenges facing each respective organization. All of this takes place in a non-confrontational positive setting.

The time commitment associated with participation in the exchange amounts to an hour-long meeting once a month for a year's time. At the end of the year, participants can opt to continue meeting with the same colleague with whom they have been interacting, or may choose to be matched with someone new. The Leadership Exchange coordinators take great care in carefully matching participants based on skill sets and needs of participants. In an effort to stave off issues, program coordinators periodically check with the participants to gauge levels of overall satisfaction. While problems may occur, such as guarded conversations, time commitment discrepancies or personality conflicts, each participant is aware of and is asked to abide by the three core principles of the scheme: Diversity, Confidentiality and Integrity.[176]

The following partner testimonials bring to light the significance of the Leadership Exchange:

> Janet Williams, Deputy Assistant Commissioner, Metropolitan Police Service (matched with the Director, National Portrait Gallery)—"The Leadership Exchange Program has enabled me to have the freedom to explore ideas about creativity, management challenges and effective leadership with a wonderfully generous and skilled person in a safe but intellectually challenging environment. Oh, and it's been fun!"[177]
>
> And, her colleague:
>
> Sandy Nairne, Director, National Portrait Gallery—"The Leadership Exchange Programme has offered me a great chance to share important thinking with a fascinating person from a very different walk of life than my own—someone that I would never otherwise have had the opportunity to talk with. We swap ideas about management—about priorities and

[175] Leadership Exchange, *Sharing Expertise*, 4.

[176] Ibid., 6, 8, 9, 11, 13.

[177] Ibid., *Sharing Expertise*, 8.

> pressure within work—as well as trying to help each other to think creatively about the challenges that we each face."[178]

London First is an excellent example of the police tapping into an existing private sector organization and exploiting its effectiveness to reach a common goal. Within this community, everyone understands the importance of providing *something*—any information—even if it appears unimportant or meaningless. Moreover, everyone recognizes *timely* information passage is paramount. There is an overall awareness that information is being provided to the private sector in order for them to make a decision. Within this culture of cooperation, the U.K. is attempting to break down barriers, manage expectations and realize the importance of sharing information.[179]

G. A SIDE-BY-SIDE LOOK: THE U.K. AND U.S.

The feasibility of incorporating some version of the U.K.'s private sector outreach programs in the U.S. is limitless. The cost of employing any or all of these programs would be minimal inasmuch as there are arguably only two major expenses. The bigger of the two expenditures would be the start-up costs associated with developing the training curriculum and materials. Secondly, the price of human capital, which should be accounted for as a part of the overhead. Specifically, training and deploying instructors and accounting for time away from everyday duties is an incidental cost to the deployment of these programs within the U.S.

Furthermore, while there are significant differences between the U.S. and U.K., namely size and population, there are many valuable lessons to be learned from the existing, highly successful, British programs. According to the *Report of the Official Account of the Bombings in London on 7th July 2005*, over 6,000 hours of CCTV footage were reviewed in conjunction with the investigation.[180] CCTV, largely owned by the private sector, proved to be invaluable in producing a time line of the events on that

---

[178] Leadership Exchange, *Sharing Expertise*, 10.

[179] Wilson and Brown, personal meeting.

[180] London Stationery Office, *Report of the Official Account of the Bombings in London on 7th July 2005*, 2006, BBC News, http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/11_05_06_narrative.pdf (accessed April 22, 2012).

fateful day in July of 2005. Yet another example of the importance of maintaining a trained community includes the realization that three of the four suicide attackers may have conducted at least one recce of their targets prior to the actual attacks. Again through the use of CCTV, it appears the three had engaged in pre-operational surveillance by taking the same route only days before the attacks on the seventh.[181] Perhaps a better trained security staff would have identified the hostile reconnaissance and at the very least alerted authorities to the suspicious behavior.

Project Griffin's adaptability is evidenced in the U.S. at the local police municipality level. The New York Police Department (NYPD) morphed *Project Griffin* into what they call the NYPD Shield. The Shield is an information sharing platform specifically focusing on combatting terrorism. The Shield sprang from *Project Griffin* and "…is a public-private partnership based on providing best practices, lessons learned, counterterrorism training opportunities, and information sharing. The Shield seeks to partner with private sector security managers with the goal of protecting New York City from terrorist attacks."[182] The Shield incorporates many of the same principles and ideals as *Project Griffin*. New York City was an excellent location in which to attempt an adaptation of the U.K.'s initiative because of its population, number of private sector entities and the size of their police department. One city police department and, therefore, one chain of command undoubtedly helped with the implementation of the project, as well.

Scalability from the U.K. to the U.S. would be a significant hurdle. As of March 2010, the U.K. reported 56 police and constabulary forces with approximately 175,248 police officers.[183] Conversely, data indicates the United States employs approximately 900,000 sworn law enforcement officers.[184] Moreover, the United States maintains thousands of state, local, federal and tribal police forces within our borders. These facts

---

[181] London Stationery Office, *Report of the Official Account of the Bombings*, 24.

[182] "NYPD Shield."

[183] *Wikipedia*, s.v., "Table of Police Forces in the United Kingdom," n.d., http://en.wikipedia.org/wiki/Table_of_police_forces_in_the_United_Kingdom (accessed April 4, 2012).

[184] *Wikipedia*, s.v., "Police," n.d., http://en.wikipedia.org/wiki/Police (accessed March 18, 2012).

alone will make the incorporation of a standardized police outreach program with the private sector extremely challenging. Additionally, because of the sheer size of the United States, the threat from terrorism, for example, is much greater in Washington, D.C. than it is in Valparaiso, Indiana. For this reason alone, a roll-out at the federal level would be much easier to accomplish. Incorporation at the federal level, specifically within the FBI, allows for standardization across 56 field offices as opposed to countless disparate police entities. Moreover, if the fusion occurs at the field office Special Agent in Charge (SAC) level, this will ensure top-level support as well as consistency.

There is no question public acceptance of government to private sector outreach would be welcomed. In its study, the 2012 National Infrastructure Advisory Council (NIAC)[185] found:

> The Council strongly believes that the government is missing an opportunity to better leverage the capabilities and resources of private sector owners and operators to reduce risks to critical infrastructures. To meet this challenge, however, significant improvement will be needed on how intelligence information is identified, developed, and shared among public and private partners. The Council believes that the voluntary public-private partnership is the best long-term strategy to secure our critical infrastructures. [186]

The majority of the United States' critical infrastructure, sectors and sub-sectors are privately owned. If the aforementioned statement is any indication of the feelings within the private sector, it is undeniable they would support more government outreach and certainly better intelligence information sharing.

Research indicates there is no legal or Constitutional prohibition to government engagement with the private sector. In fact, as previously indicated, there are a number of Presidential Directives and strategies highlighting the need for developing a more robust relationship between the government and the private sector. Not unlike the U.K.,

---

[185] The National Infrastructure Advisory Council (NIAC) is a presidential appointed committee consisting of approximately 30 members representing the private sector, state and local government and academia all of whom are charged with advising the President on the security of critical infrastructure and their information systems. Department of Homeland Security, "National Infrastructure Advisory Council," n.d., http://www.dhs.gov/files/committees/editorial_0353.shtm (accessed March 18, 2012).

[186] National Infrastructure Advisory Council, *Intelligence Information Sharing*, 15.

the U.S. should enlist a holistic approach to protecting the homeland and must incorporate the necessity of community outreach in its every day operating procedures.

Politically, engaging the private sector has been a topic of discussion since at least 1998 when it was written about in the 1998 Presidential Decision Directive 63. Most recently, the 2012 NIAC study recommended a whole of government approach to securing the homeland that should be accomplished either through Presidential Policy Directive or whatever other means are available.[187] Indeed, enacting White House directives is not enough to ensure success. A cultural shift must be enacted within traditional law enforcement and the intelligence community wherein the "need to know" mentality is replaced with one of a "need to share."

H. COMPARED TO INFRAGARD

Certainly, the U.K.'s *Project Griffin* and *Project Argus* align closely with the U.S.'s InfraGard program. They all encourage open and all-inclusive participation. They all strive to inform their constituents about threat indicators and updated terrorist tactics, techniques and procedures. None fosters trusted relationships between private sector participants and the police.

They differ in that neither of the two British programs involves on-going meetings, which InfraGard holds routinely. And, whereas the U.K. programs are police led, InfraGard is only sponsored and not directed by the FBI. Also, training from the U.K. programs is relevant, evolving and specific to threats from terrorism. Conversely, InfraGard focuses on all threats and was founded based on the threat to critical infrastructure from cyber-attacks.

I. WHAT WE GAIN

There is no down side to encouraging community participation in making neighborhoods safer. A whole of community approach is essential to fostering a ubiquitous sense of well-being. Specifically within the homeland security framework,

[187] National Infrastructure Advisory Council, *Intelligence Information Sharing*, 15.

incorporating versus alienating private sector owners and operators is long overdue. The private sector has a tremendous amount of personnel and assets available which, if tasked and properly managed, can assist the government.

The private sector, for example, employs thousands of people. Access to staff, either as "eyes and ears" on the ground and/or as intelligence collection platforms would be genuinely helpful to law enforcement. Moreover, access to records, assets and indigenous CCTV footage could potentially provide priceless investigative assistance to law enforcement officials. As evidenced in the Post-7/7 report, CCTV coverage proved invaluable to piecing together the relationship of the suicide attackers and the timeline of the event.

J. IN CONCLUSION

The United Kingdom is very forward leaning in their approaches to combatting terrorism through a whole of community stand point. Their national strategy, CONTEST, succinctly breaks down strategy into four manageable subcategories: Pursue, Prevent, Protect and Prepare. The British people seem to understand the dire importance of corralling all possible resources and thinking outside of the proverbial box to address a problem. *Projects Griffin, Argus* and *London First* are examples of this innovative thinking put into action. These initiatives fully integrate its citizenry in the security of their nation. There are many positive aspects of these programs that are transferable to the United States such as training and information sharing. While scalability is an issue, nothing is insurmountable. Integrating the private sector into the U.S.'s security battles is an absolutely necessary paradigm shift that is long overdue.

VII. THE FBI'S ANSWER IS "TOUCHSTONE"

A. INTRODUCTION TO TOUCHSTONE

Having discussed the successful private sector outreach programs within the U.K, this chapter will describe the FBI's own innovative private company outreach efforts—Touchstone. The business process for the development and deployment of an FBI office's Touchstone group will be explained in detail. Touchstone answers the "who, what, when, where and why's" regarding the integration of the private sector as full partners in the homeland security enterprise. By the end, a Special Agent in Charge (SAC) will be able to export the D.C. Touchstone model to his or her own field office thereby closing the loop on collaboration within his or her areas of responsibility in order to better address today's threats.

B. TOUCHSTONE—AN EXAMPLE OF INNOVATIVE AND DISRUPTIVE THINKING

According to the American Heritage® Dictionary of the English Language, "touchstone" is defined as: "An excellent quality or example that is used to test the excellence or genuineness of others: 'the qualities of courage and vision that are the touchstones of leadership' (Henry A. Kissinger)."[188] This definition epitomizes the concept behind the Touchstone Project underway in Washington, D.C.

The Touchstone Project, "Touchstone," is an example of breaking free of traditional roles and responsibilities and creating new avenues aimed at robust information sharing and overall engagement by the FBI with key private sector stakeholders. Touchstone is a ground breaking proposal that moves beyond the out-of-date "meet and greet" level of engagement with the private sector and into the realm of making key private sector stakeholders genuine partners within the homeland security enterprise. Deploying Project Touchstone in the FBI is an example of a seismic shift in

[188] *American Heritage Dictionary of the English Language* (4th ed.), s.v. "Touchstone," 2009, http://www.thefreedictionary.com/touchstone (accessed July 11, 2012).

thinking for an organization made famous for investigating historic gangsters like Al Capone, John Dillinger and Bonnie and Clyde.[189]

Strategically, the long-term vision is to establish a Touchstone group in each of the FBI's 56 field offices throughout the United States and Puerto Rico. A SAC, or designee, should lead his or her respective field office's Touchstone group. This is an example of planning for the uncertain future—especially as it relates to today's threats.

C. WHY TOUCHSTONE IS A NECESSARY EVOLUTION

Through legislation and otherwise, the stove-piping of information within the law enforcement and intelligence communities (IC) has been, to a large extent, reduced. State, local, tribal and other federal partners have been fully integrated within Joint Terrorism Task Forces (JTTFs) throughout the country. The citizenry has even been asked to partake in homeland security through the Department of Homeland Security's "See Something; Say Something" campaign. Rendering the private sector full partners will lead to the fortification of especially enticing soft targets—soft because they afford open access to the public and little to no security. As the *National Strategy for Counterterrorism* points out, "Presenting the United States as a 'hardened' target is unlikely to cause al-Qa'ida and its affiliates and adherents to abandon terrorism, but it can deter them from attacking particular targets or persuade them that their efforts are unlikely to succeed."[190]

Notwithstanding, when information materializes that is specific and believed credible, the FBI has a duty to warn its citizens of harm that may potentially befall them. Here's a scenario to consider: It is days after Usama bin Laden is killed in Abbottabad, Pakistan by U.S. Special Forces during a highly secret, extremely dangerous assault. The extremist world erupts in anger vowing to avenge the death of their beloved patriarch. Extremist Websites are flooded with posts. One Website in particular, known for its influential administrator and contributors, contains more than rhetoric. This Website has

---

[189] "Famous Cases and Criminals" n.d., Federal Bureau of Investigation, http://www.fbi.gov/about-us/history/famous-cases/ (accessed July 16, 2012).

[190] White House, *National Strategy for Counterterrorism* (Washington, D.C.: White House, 2011), 8.

called upon the sympathetic to enact retribution against a specific U.S. company and their CEOs known to have supported the coalition war efforts in Iraq and Afghanistan. This company is headquartered within the Washington Field Offices' area of responsibility.

The SAC of the Washington Field Counterterrorism Division has a duty to warn this company and its employees of the impending threat so they can take appropriate security measures, as they deem necessary. How should the SAC go about making this notification as there is no established relationship with this company? Ultimately, the SAC would "cold calls" the business and speak with the head of security. The warning gets passed and the SAC's duty to warn is complete…or is it?

What the SAC failed to realize was the building in which this company resides is a multi-tenant building and they simply lease space. There are at least three other companies co-located in this particular office building, two of which are companies who also deal exclusively in contracting with the U.S. military. Moreover, the targeted company does not have its own security staff, instead opting to outsource their security to a locally renowned security firm. Upon further examination, it is learned there is an in-house parking garage located below the building with both employee and public parking spaces. The parking garage is owned and operated by a local parking company. The target company resides on a campus of other commercial buildings, parking garages and eateries. Not only that, but it is likely the reconnaissance for the operation will take place in the coffee shop across the street as it provides the cover of being a public location wherein it is not uncommon for patrons to stay for extended periods of time, often times while using computers and cell phones. Therefore, this coffee shop has an absolute interest in knowing about the reported threat.

It becomes evident very quickly that one telephone call to only the target company alone is simply not enough. An attack of any sort on the company described above leaves many others completely in the dark about a looming threat that could at the end of the day unwittingly harm them. It is easy to think of a number of additional uninvolved parties such as janitorial staffs and even trash collection that could also be affected.

This is where Touchstone enters the picture. Touchstone bridges the gap and, by virtue of the influence of its members, blankets the private sector. Eliciting the participation of the private sector in protecting the homeland is the last bastion in completing the homeland security continuum. It is time to enlist the members of the private sector and make them full partners in the combating of terrorism and the leaders in promoting security and resiliency.

D. WHY HAS THE PRIVATE SECTOR NOT BEEN INTEGRATED?

According to research by the Congressional Research Service, "Some argue that intelligence officials have tended to err on the side of maintaining the security of information even at the cost of not sharing essential data with those having a need to know."[191] Realistically, many within government and law enforcement do not even consider the private sector when they think of securing the homeland because they are not known as traditional partners. Yet, time and again, terrorist groups have attacked, or planned attacks, on privately owned assets. Looking at terrorist attacks in hindsight, had security managers, such as hotel security staff, been notified of threat information, proactive security measures could have been enacted which may have drastically altered the ill-fated outcomes. For example, perhaps security managers could have asked for increased police foot and mobile patrols in and around their property, or maybe they could have elicited K-9 units to make rounds as a very visible deterrent.

Others argue intelligence information sharing with the private sector is outside of their mandated responsibilities. In this case, non-traditional roles often fall to the wayside as one agency has or takes the time, personnel, budget or desire to stray off course from their designated mission set. In that same vein, the private sector is not generally seen as a contributor to fully comprehending today's threats. After all, the private sector is only concerned about making money, right? As a result, thinking continues on the micro versus macro level.

---

[191] Richard A. Best Jr., *Intelligence Issues for Congress* (Washington, DC: Congressional Research Service, 2011), 8.

Moreover, most in government do not understand the needs or capabilities of the private sector. Because of this, the idea of information sharing becomes clouded, marred with the attitude of, "I'll tell them what they need to know when I think they need to know it," versus the sharing of intelligence information that is actionable, timely, specific and encourages bi-directional feedback. Resultantly, the private sector is overlooked as necessary recipients of potentially crucial information.

There is no doubt today's information sharing network is complex and often times unruly (see Figure 1).

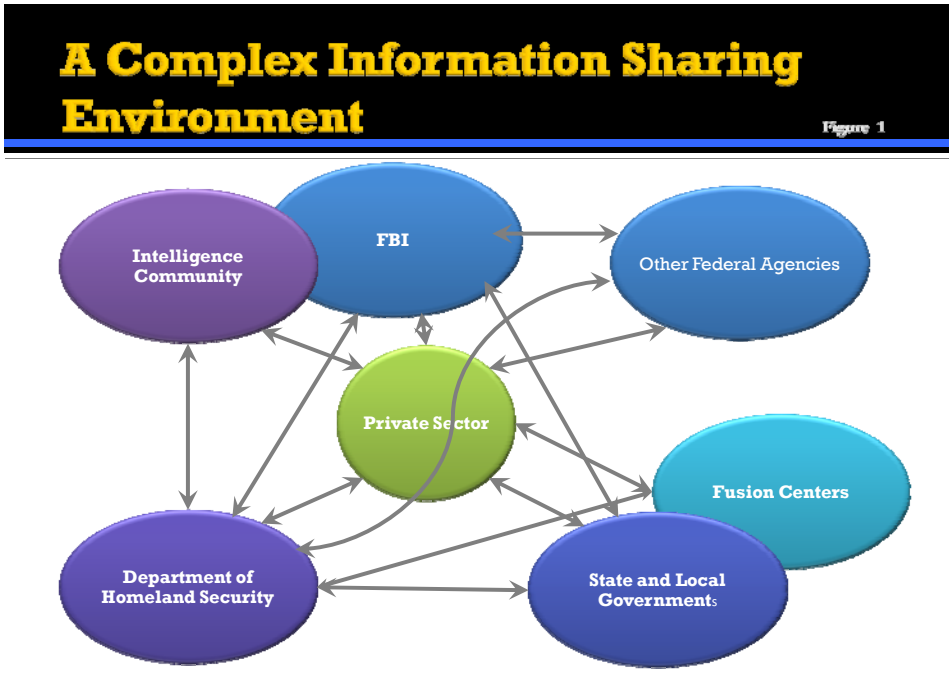

Figure 1. The Current Intelligence Sharing Network

The U.S. intelligence community alone is:

> …a coalition of 17 agencies and organizations…that work both independently and collaboratively to gather the intelligence necessary to conduct foreign relations and national security activities. … [Its] primary mission is to collect and convey the essential information the President

> and members of the policymaking, law enforcement, and military communities require to execute their appointed duties.[192]

Add in intelligence information collection at the fusion centers and at the state, local and tribal levels of government and the information sharing environment quickly becomes an example of a massive, disjointed complex adaptive system. In other words, "a system in which large networks of components with no central control and simple rules of operation give rise to complex collective behavior, sophisticated information processing, and adaptation via learning or evolution."[193]

> In part, the intricacy described above has manifested itself in the private sector's perception of our homeland security system as being perplexing and cumbersome. Because of these and other factors, the private sector has been relegated to the sidelines of the homeland security game. So, they started their own game in which they act as the coaches and captains begging for rules from the government referees—rules which have yet to materialize. Hence, private sector security apparatuses have relied upon established relationships and "reach back" to former colleagues, often in either the law enforcement or intelligence communities, to obtain greatly needed information.

Additionally, there is no single point of contact within government to act as the conduit with the private sector. Most every government agency has outreach programs, sometime multiple programs. For example, as has been discussed, the FBI has seven private sector outreach programs including InfraGard, fusion centers, the Domestic Security Alliance Council (DSAC), and the Counterintelligence Division's Strategic Partnership Initiative, among others.[194] To the private sector, the government looks disjointed and unorganized.

---

[192] "About the Intelligence Community," n.d., http://www.intelligence.gov/about-the-intelligence-community/ (accessed July 15, 2012).

[193] Melanie Mitchell, Complexity: A Guided Tour (Kindle version) (Oxford: Oxford University Press; 2009), 308.

[194] "Partnerships and Outreach."

While the DHS has the lead for critical infrastructure and key resource protection,[195] it does not own threat information. Therefore, allowing the DHS to unilaterally provide protection information without providing context to the message as it relates to the current threat picture is, in essence, providing the private sector with an incomplete picture. Without Touchstone, which integrates DHS and the FBI, there is no formal process to ensure cross-agency coordination.

E. THERE ARE SOME CHALLENGES

Embracing the idea of incorporating the private sector into the homeland security family requires a paradigm shift within the law enforcement and intelligence communities. Traditionally, both communities have been reticent about information sharing in order to protect sources and methods. While understandable, the other side of the equation involves a cultural mindset that has been extremely difficult to penetrate and change. Changing people's mindsets presents an especially interesting dilemma "because an organization's culture comprises an interlocking set of goals, roles, processes, values, communications practices, attitudes and assumptions. The elements fit together as an [sic] mutually reinforcing system and combine to prevent any attempt to change it."196 A chain is only as strong as its weakest link. Equally, Touchstone is only as resilient as its most unprotected partner.

As with any partnership, it is essential the atmosphere surrounding the alliance be collaborative versus competitive. While it is true, some of the members of an office's Touchstone group will be industry competitors, at no point should information divulged or provided during Touchstone sessions be used to further ones' competitive advantage.

---

[195] Reference Homeland Security Presidential Directive 7 (HSPD-7). "This directive establishes the U.S. policy for 'enhancing protection of the Nation's CIKR' and mandates a national plan to actuate that policy. In HSPD-7, the President designates the Secretary of Homeland Security as the 'principal Federal official to lead CIKR protection efforts among Federal departments and agencies, State and local governments, and the private sector' and assigns responsibility for CIKR sectors to Federal Sector-Specific Agencies (SSAs)." Department of Homeland Security, *National Infrastructure Protection Plan*, (Washington, DC: Department of Homeland Security, 2009), 2.

[196] Steve Denning, "How Do You Change an Organizational Culture?" *Forbes*, July 23, 2011, http://www.forbes.com/sites/stevedenning/2011/07/23/how-do-you-change-an-organizational-culture/ (accessed July 12, 2012).

In order for Touchstone to work, much like London First, it has to be a rivalry-free environment wherein information shared is used in furtherance of overall security and not to "get a leg up."

The protection of information should not be understated. According to research on Intelligence Issues at the behest of Congress, "Agencies that obtain highly sensitive information are reluctant to share it throughout the intelligence community out of a determination to protect their sources…. The unauthorized release of classified documents in 2010 by major newspapers and the Wikileaks website underscored, however, the risks of widespread dissemination of sensitive information."[197] The divulgence of critical, highly sensitive information can have extreme consequences on not only national security but human lives. Information security is an enormous concern when considering discussing sensitive information outside of traditional intelligence channels.

Perhaps most pointedly, on the surface there are seemingly no incentives for government to partner with the private sector. Unlike the colossal changes made based upon recommendations from the 9/11 Commission, integrating the private sector into daily operations is, to this point, only spoken about—a "good idea." Touchstone is a groundbreaking project that puts ideas into action. Significantly, a lesson learned from the Touchstone group in Washington, D.C. is there are enormous advantages to partnering with the private sector. For example, during an arrest of a Washington Field Office terrorism subject, a Washington, D.C. Touchstone member provided assistance by offering the use of their company's property as the arrest location. This allowed agents to operate in a relatively safe and controlled environment that proved to be especially helpful in executing their plan.

Another challenge to the project is managing the unintended consequences of its creation. For instance, initiatives such as InfraGard may lose their zeal and membership may drop. To mitigate this, InfraGard should enhance Touchstone. InfraGard sessions should be tailored to provide training/guest speakers specifically addressing today's

[197] Best, *Intelligence Issues for Congress*, 13.

threat—as briefed during Touchstone meetings. Members of InfraGard should be encouraged to participate in these training sessions in order to be better postured to become the "eyes and ears" on the ground. Therefore, another unintended consequence may ultimately be that InfraGard members will further augment law enforcement through both a top down and bottom up participation. Touchstone members, at the corporate/global security strata will provide information and guidance from their vantage point while the grassroots will be trained and keen to watch for nefarious activities which will then be reported up the chain. This non-linear thinking[198] will result in full integration, continuous information flow, bi-directional interaction and feedback.

F. TOUCHSTONE EXECUTES THE "PREVENTION" PRONG

The FBI's Threat Mitigation Strategy (TMS) for Homegrown Violent Extremists (HVEs) is outlined in four steps: Detect; Penetrate; Disrupt and Prevent (see Figure 2).

[198] Non-linear thinking has been defined as, "Human thought characterized by expansion in multiple directions, rather than in one direction, and based on the concept that there are multiple starting points from which one can apply logic to problem. Non-linear thinking is less constrictive—letting the creative side of you run rampant because of its inherent lack of structure." "Do we think differently? Linear vs. Non-Linear Thinking," *Chuck's Lamp* [blog] April 11, 2009, http://chuckslamp.com/index.php/2009/04/11/non-linearthinking/ (accessed July 7, 2012).

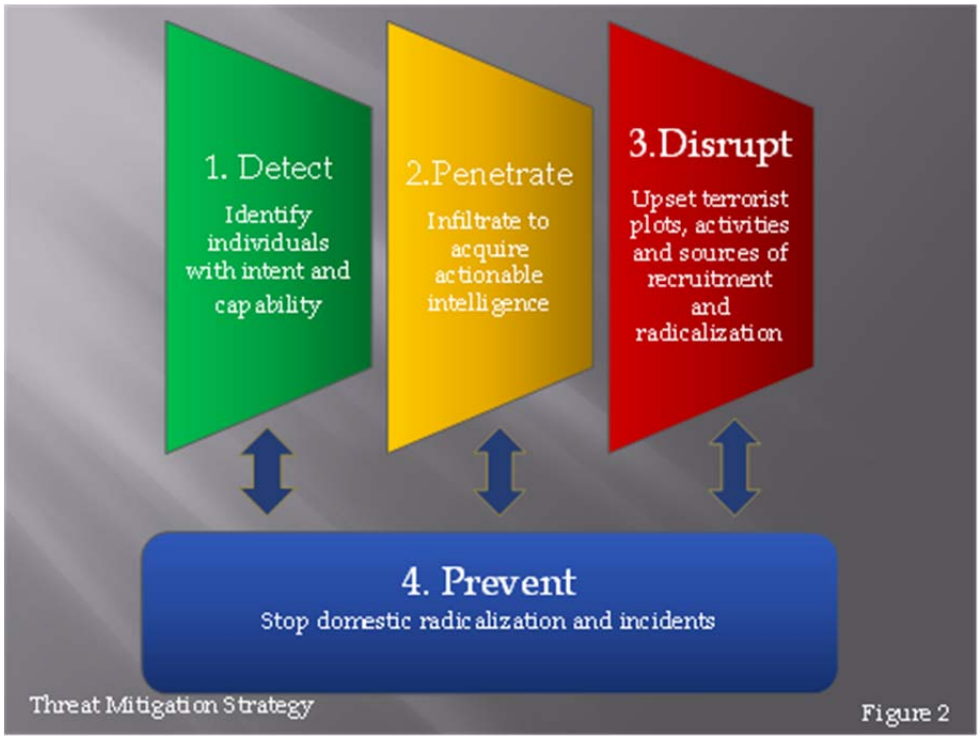

Figure 2. The FBI's Threat Mitigation Strategy for Homegrown Violent Extremists

Each piece of the strategy coalesces with the rest, with the prevention tine permeating throughout. The FBI uses traditional investigative methods to address the Detect, Penetrate and Disrupt categories of the strategy. However, the Prevention piece is not as well forged because it steps outside of established investigative techniques. As Figure 2 depicts, prevention entails stopping people from becoming radicalized. But, how? The standard answer to prevention is outreach.

Touchstone answers this call. Not only does Touchstone represent outreach to the private sector, it moves a step further by identifying, engaging with and training the first line of defense—the private sector security apparatus. Undoubtedly, the front line security guards, parking attendants, janitorial staff, or even every day citizens are the tip of the spear. They are closest to the threat and will be the first to respond—certainly more so than the police and definitely more than the FBI (see Figure 2). Giving the private sector the information necessary to understand and react to threats, real or perceived, better postures all involved detecting, penetrating and ultimately disrupting.

For example, in May, 2010, it was not the police who first noticed an unattended, smoking SUV parked in the heart of Times Square, New York City. Rather, it was an alert street vendor who first identified that something was amiss and subsequently alerted police to the Nissan Pathfinder Faisal Shahzad attempted to ignite during his failed bombing in Times Square. To further illustrate, a perceptive ambulance crew observed smoke coming from a Mercedes parked in front of Tiger Tiger nightclub in London. The crew immediately notified police. As reported by the BBC, "A controlled explosion was carried out on the car, packed with 60 litres [*sic*] of petrol, gas cylinders and nails." It is believed up to 1,700 people were inside the club during the time. Had it not been for the observation skills of the ambulance crew, the results could have been devastating had the car exploded as intended.[199]

G. THE ADVANTAGES OUTWEIGH ALL ELSE

The ability to harness the full capabilities of key private sector stakeholders by making them full cohorts offers tremendous benefits. For one, the wide array of collection capabilities among the private sector is sorely underestimated. Many senior level security executives within the private sector are former law enforcement or intelligence community members. This alone provides the ability to "speak the same language" when it comes to providing and understanding threat information. Additionally, inherent sector security assets can provide suspicious activity reports to law enforcement. These reports may result in the identification of pre-operational planning, for example, that could ultimately lead to the disruption of nefarious activity.

Moreover, private sector personnel are not only the first line of defense but also first responders. In today's threat environment, it is highly conceivable that nefarious pre-operational activities, such as hostile surveillance, will be discovered by private sector security personnel before anyone else in either law enforcement or the intelligence community. With the advent of the individually inspired jihadist, it is less likely traditional intelligence community reporting will highlight a person's radical tendencies.

---

[199] "Police Avert Car Bomb 'Carnage;' A Car Bomb Planted in Central London Would Have Caused 'Carnage' If It Had Exploded, Police Say," *BBC News*, June 29, 2007, http://news.bbc.co.uk/2/hi/6252276.stm (accessed April 21, 2012).

Rather, the shopping mall or hotel security guard will be the first to notice pre-operational reconnaissance conducted by a person or vehicle they know to be out of the ordinary. Without open lines of communication, training in detecting key indicators, actionable intelligence and the security reaction, thereafter the identification of possible lone actors or even homegrown violent extremist cells, will likely be missed. Therefore, the private sector should be employed as an early warning system as well as an enhancement to law enforcement's response to a terrorist attack or other event.

The private sector is aligned such that it offers tremendous interconnectivity within its own ranks. By design, the private sector's architecture crosses multiple commercial facilities and sectors allowing for rapid outreach, information sharing and response to alerts, events or otherwise. For law enforcement, this extraordinary ability to "light up" a network is extremely helpful in instances during which it is imperative information is distributed quickly and to as wide of an audience as possible. This acts as a force multiplier in support of mission objectives such as threat information or "Be on the Look Out" alerts.

Access to private sector assets and staff are benefits that should not be understated. According to a United States Government Accountability Office Report to Congressional Requestors dated October 2006, "Because approximately 85 percent of the nation's critical infrastructure is owned by the private sector, developing trusted partnerships between the federal government and the private sector across all sectors is critical to ensure the protection of these assets…."[200]

Beyond the percentage of critical infrastructure owned by the private sector that is quantified as "substantial," according to the U.S. Department of Labor Bureau of Labor Statistics, as of May 2011, the civilian labor force participation rate is approximately 64.2% which includes workers age 16 and older."[201] By virtue of their sheer size alone, the private sector provides law enforcement with access to countless people, places and

[200] Government Accountability Office, *Critical Infrastructure Protection Coordination Issues* (GAO-07-39), (Washington, DC: Government Accountability Office, 2006), 29.

[201] United States Department of Labor, Bureau of Labor Statistics, "Databases, Tables and Calculators by Subject," n.d. http://data.bls.gov/timeseries/LNS11300000 (accessed July 17, 2012).

things. Moreover, the FBI has everything to gain by empowering the masses of the workforce to act as the "eyes and ears" for law enforcement. "Working together the public and private sectors are stronger than either is alone."[202]

To illustrate, tapping into the private sector opens the door to information about staff, who may be suspects and/or potential sources of information. It also affords law enforcement the opportunity to access a plethora of resources inherent to the private sector, such as CCTV coverage and subsequent captured and archived footage. All of these provide invaluable support to operations whether they are overt or covert in nature. The vast majority of CCTV coverage is owned and operated by the private sector. The importance of this asset should not be understated. Access to historical and real-time footage is critical to supporting investigations and ultimately saving lives both "left and right of boom."[203]

Lastly, integrating the security apparatus of the private sector eliminates the gap. Securing the homeland is no longer a single agency-led mission. The multitude and volume of threats facing the U.S. requires a collaborative effort by government and non-government partners. According to the NIAC:

> This collaborative responsibility is best accomplished through a collaboration that leverages the respective capabilities of government and the private sector: the government provides intelligence about potential threats and mobilizes public resources for protection, response and recovery, and the informed private sector uses this information to effectively manage risks and operate infrastructures in the face of such threats.[204]

H. BUILDING THE TEAM—THE GOVERNMENT SIDE OF THE HOUSE

A field office SAC should head his or her respective Touchstone group. This SAC should be well versed in the current terrorism threat picture—both nationally and internationally. This knowledge will prove to be paramount for providing context to

---

[202] "NYPD Shield."

[203] The phrase "left of boom/right of boom" is demonstrative of activities pre-blast and post-blast. The phrase is often used by Paul Smith, adjunct professor at Center for Homeland Defense and Security.

[204] National Infrastructure Advisory Council, *Critical Infrastructure,* 4.

otherwise innocuous or uninformative news releases and bulletins. The SAC may wish to have another manager act as a second chair. In the case of the Washington, D.C. Touchstone group, a counterterrorism Supervisory Special Agent (SSA) works alongside the SAC. Their collective duties include setting agendas, documenting endeavors, accumulating releasable intelligence bulletins and other pertinent information as well as maintaining liaison with all of the involved partners.

The DHS's Protective Security Advisors (PSA) for the field office's AOR must be part of Touchstone. As described by the DHS, "The PSA are trained critical infrastructure protection and vulnerability mitigation subject matter experts." PSAs "also conduct specialized site visits and provide information and guidance on critical infrastructure issues" as well as "conduct briefings and outreach meetings with critical infrastructure protection partners, help private sector personnel obtain ***security clearances*** [emphasis added], and disseminate critical infrastructure-related information such as protective measures reports."[205]

DHS's ability to facilitate the acquisition of security clearances is an extremely important factor as well as asset to Touchstone. While Touchstone strives to operate in the unclassified environment solely, there may be rare occasions when it is necessary to disseminate classified information. Knowing that Touchstone members have been vetted via the clearance process also raises government officials' comfort level regarding sharing information that may be on the fringes of being classified. This becomes even more significant when consideration is given to the intrusiveness of the clearance process, not to mention the time and associated cost. The Office of Personnel Management (OPM) "which conducts over 90% of all federal security clearance investigations, conducts these investigations on a fee-for-service basis" estimated that, "based on the number and type of each investigation, the weighted average cost is about

[205] "Protective Security Advisors," n.d., http://www.dhs.gov/files/programs/gc_1265310793722.shtm (accessed July 22, 2012).

$1230 per investigation."[206] While there are no specific figures detailing the price of the investigation, adjudication, processing and handling, Figure 3 shows estimates of fiscal year 2011 OPM clearance prices:

INVESTIGATION	PRIORITY HANDLING	STANDARD SERVICE
NACLC	---------	$228
SSBI	$4,399	$4,005
SSBI-PR	$2,964	$2,711
PPR	$2,261	$2,009

(NACLC) = National Agency Checks with Law and Credit

(SSBI) = Single Scope Background Investigation

(SSBI-PR) = SSBI Periodic Reinvestigations

(PRP) = Phased Periodic Reinvestigations*[207]

Figure 3. FY2011 Prices of OPM Investigations

Beyond clearances, advice and the expertise the PSAs bring to the table, they also come with an arsenal of training packages that are tailored to the private sector. DHS training programs include, among others, Soft Target Awareness, Protective Measures and a Private Sector Counterterrorism Awareness Workshop.[208] Finally, the PSAs also bring with them geo-spatial mapping resources (described in more detail in *Let's Chat: Information Sharing within Touchstone*). In sum, including the DHS as part of Touchstone unifies the U.S. government critical infrastructure efforts, each partner providing the private sector with their own unique expertise and resources.

---

[206] William Henderson, "How Much Does It Really Cost to Get a Security Clearance?" August 7, 2011, http://www.clearancejobs.com/cleared-news/381/how-much-does-it-really-cost-to-get-a-security-clearance (accessed August 22, 2012).

[207] Henderson, "How Much Does It Really Cost?"

[208] "Bombing Prevention Training, n.d., http://www.dhs.gov/files/programs/gc_1265223119415.shtm (accessed July 21, 2012).

I. BEYOND THE GOVERNMENT—FINDING YOUR JOE[209]

Identifying private sector partners to participate in Touchstone may seem to be a daunting part of the endeavor. Following a few simple steps will help eliminate the angst. First, SACs should seek out a small group of executive-level owners and operators within the private sector security apparatus. Touchstone members have to be decision makers—the bosses. Within this stratum, singling out one's private sector partners will be based, in large part, on each field office's market.

Membership will obviously differ from city to city and field office to field office. "…there isn't one size that fits all" when it comes to building a Touchstone group. [210] Each Touchstone group should remain as small yet as inclusive as possible. Part of the appeal of Touchstone is each member is hand selected. Being chosen and asked to participate creates an environment of trust and confidence versus more ad hoc and all inclusive groups such as InfraGard where most anyone can join. Developing personal trusted relationships is paramount to Touchstone's success. Moreover, Touchstone membership is exclusive and limited to one chief participant and an alternate. This stabilizes continuity and helps in the development of personal, trusted relationships.

Membership criteria used to identify primary and alternate D.C. Touchstone members included the following:

- DSAC members
- Represent high profile/iconic ownership/management
- Represent a large market position within a "key resource" service such as security, parking operator, major real estate and major hospitality
- Has an effective network wherein each is able to very quickly "get the word out" within their own industry network

[209] This is a reference to Joseph B. Donovan, Senior Vice President, Beacon Capital Partners who chairs the Building Owners and Managers Association (BOMA) national preparedness committee, is Co-Chair of the Real Estate Roundtable, Homeland Security Taskforce, Co-Chairs the Commercial Facilities Sector Coordinating Council (CFSCC), is a Co-Chair of the NIAC Study Group and is unequivocally a key member of the D.C. Touchstone group.

[210] Kees van der Heijden, *Scenarios: The Art of Strategic Conversation* (2nd ed. and Kindle edition), (Hoboken, NJ: John Wiley & Sons, Ltd, 2004), 18.

- Confidence in each individual's ability to work and cooperate with other Touchstone members in a non-competitive manner
- Each has an existing security clearance or can and will obtain a security clearance

To further allay some fears, current D.C. Touchstone members will assist other SACs by identifying counterparts and colleagues throughout the different market cities. Within the Washington, D.C. Touchstone, the private sector partners are largely comprised of commercial facilities owners and operators. More specifically, the directors of security for the J.W. Marriott and Hilton Hotels are members of Washington, D.C.'s Touchstone as these two hotel chains represent the majority of the lodging subsector within the greater D.C. metropolitan area. In addition to the hotels (Lodging) mentioned above, the D.C. Touchstone group is comprised of the following sector and subsector groups: Public Assembly, Retail, Office, Security, Parking, Associations, Education, Finance and Government.

J. LET US CHAT: INFORMATION SHARING WITHIN TOUCHSTONE

All meetings should start with a current threat briefing. Simply putting the threat into context is extremely helpful for the private sector. For example, the FBI and DHS released a Joint Intelligence Bulletin (JIB) regarding the 10-year anniversary of the attacks on September 11, 2001. In the bulletin under the heading of "Key Findings" the bulletin stated:

> **We have no indication** [emphasis added] that al-Qa'ida, its affiliates, or its allies are plottingHomeland attacks to coincide with the 10-year anniversary of 9/11.
>
> As of February 2010 al-Qa'ida was contemplating large attacks in the Homeland on symbolic dates, to include the 10-year anniversary of the 9/11 terrorist attacks, but **we have no specific, credible information** [emphasis added] to indicate al-Qa'ida's aspirations have evolved into an active Homeland plot.
>
> Although we have not detected plots by HVEs targeting the 9/11anniversary, **we remain concerned** [emphasis added] that HVEs—

> motivated by al-Qa'ida propaganda that increasingly encourages them to act independently—could try to stage an attack with little or no warning.[211]

To the uninformed, this announcement appears as if there is nothing to worry about. The U.S. government just said it has no information to indicate an attack is going to occur. So, a head of security with a very tight budget and often times limited personnel may say there is no need to have extra guards on staff; or, there is no reason to enact more thorough identification checks. This reaction could not be farther from ideal.

Instead, Touchstone is the place where the "real story" should be told. What needs to be relayed to the private sector is yes, in fact, there is no articulated threat; but that does not mean we should not be extra alert for nefarious activity. It should be explained that al-Qa'ida has been planning attacks on the homeland continuously since the successful 9/11 attacks. Al-Qa'ida believes in symbolic dates and, if possible, will seize upon any opportunity to conduct an attack on such a day. Indeed, al-Qa'ida leader and mastermind Usama bin Laden's death could be a catalyst for an attack. Therefore, even though there is no *specific* information, it is recommended that private sector security be hyper-vigilant to anything out of the ordinary and report it to law enforcement immediately. Touchstone briefings add to as well as reinforce a bulletin's message by stressing the extreme importance of symbolic dates coupled with world events (i.e., in this example the death of bin Laden). This allows private sector security to take necessary precautions to harden their targets.

Another example involves an April 2012 Roll Call Release,[212] which discussed terrorists' interest in attacking theaters. The document highlighted two particular incidents specific to movie theaters—one involving an al-Shabaab female suicide bomber

---

[211] Federal Bureau of Investigation and Department of Homeland Security, "Ten-Year Anniversary of 9/11 Attacks: No Specific Threats, but a Potentially Attractive Terrorist Target" *Joint Intelligence Bulletin*, August 10, 2011.

[212] A Roll Call Release is a dual seal, FBI and DHS, bulletin often times distributed in conjunction with Interagency Threat Assessment and Coordination Group (ITACG) meant to inform state, local, tribal and federal law enforcement and the private sector about terrorism-related information.

who detonated explosives at the national theater in Mogadishu, Somalia.[213] The other example was of an al-Qa'ida linked extremist who suggested recreating attacks similar to the siege at the school in Russia as well as to engage in hostile take-overs of crowded places such as U.S. schools and movie theaters.[214] The impetus behind the bulletin was to bring to light the potential for terrorist attacks against U.S. theaters.

The Roll Call that was eventually drafted was very vague and provided only a few very general tips regarding potential indicators of an attack. Some of the discussion points included being on the look-out for suspicious or illegally parked vehicles, looking for persons or groups trying to gain unauthorized entry to the theater or restricted areas and watching for unattended packages. Conspicuously missing were specific considerations for theater owners and law enforcement. Had context been given to the announcement, perhaps the July 2012 tragedy at the movie theater in Aurora, Colorado could have been minimized.

In fact, recommendations were made with the intention of enhancing the bulletin's content. Some of the suggestions included: confirming all sensitive areas within the facility are properly secured and access is limited; confirm all CCTV and video systems are maintained, operating properly and are leveraged against perceived weak points and confirm emergency plans are current and up to date. These are a mere sampling of the 19 total recommendations made to augment this bulletin—instead, the released bulletin was extremely generic and offered no direction or guidance.[215] In the absence of informative, timely and actionable intelligence information, the private sector is left in a void to fend for itself. Touchstone fills that void. Touchstone is beyond "crying wolf." Instead, Touchstone is a vehicle by which information is shared. Touchstone helps to provide the private sector with the "how does this affect me" spin.

---

[213] Lee Ferran, Bazi Kanani, and Dana Hughes, "Theater Explosion Kills Several in Mogadishu," *ABC News*, April 4, 2012, http://abcnews.go.com/Blotter/al-shabaab-claims-theater-explosion-kills-mogadishu/story?id=16070499 (accessed August 22, 2012).

[214] Defense Intelligence Agency, *Intelligence Information Report 2 104 0256 12*, April 17, 2012.

[215] Department of Homeland Security and private sector entities, "Roll Call Release" (internal document draft) April 2012.

In fact, not only Roll Call Releases but Intelligence Bulletins are excellent pieces of information to discuss during Touchstone meetings—especially because many of them are also releasable to the private sector. Additionally, special topics can be discussed. For example, during Washington, D.C. Touchstone meetings, briefings on the London Olympics, the Mumbai attacks and HVEs have been conducted. Plus, Touchstone members should play a role in setting agenda topics. Notwithstanding, regardless of the topic, the key to Touchstone is information sharing through open and honest dialogue.

Now that what to talk about has been identified, how will this information be controlled? Each Touchstone member within the Washington, D.C. group agreed to and signed a non-disclosure agreement. Simply, the agreement affirms each person's adherence to strict information protocols. This moves beyond the informality of a "gentleman's handshake" and formalizes the arrangement. The execution of this document encourages trust and confidentiality among all involved.

In lieu of sit down meetings, which may occur bi-monthly as determined by the respective Touchstone chapter, Touchstone should utilize existing technology to encourage continuous information sharing. For example, within the D.C. Touchstone, emails and conference calls are routinely used to distribute timely and pertinent information. Nurturing robust and relevant information sharing via meetings, emails and telephone conference calls encourages continued participation by members.

In order to distribute information quickly, conference calls have been used in Washington, D.C. During the calls, which are intended to last no more than 10 or 15 minutes, important, timely and actionable information is disseminated to Touchstone partners. For example, recently a conference call was convened in D.C. to discuss the security implications surrounding a major Jewish event that was anticipated to attract nearly 90,000 participants in the Northeast. This was a significant event inasmuch as al-Qa'ida routinely disparages the U.S.'s support for Israel and would most certainly attack such an event if the opportunity presented itself. The conference call was organized so that Touchstone members would have visibility into the event, understand its significance and enact whatever security posture deemed necessary to secure their assets.

K. TOUCHSTONE OPERATES ON MULTIPLE LEVELS

Unlike other outreach initiatives, Touchstone functions at the local/neighborhood plane of interaction. As described in more detail below, Touchstone groups morph into neighborhood-specific outreach committees designed to engage with not only affected executive level security directors but also their regional, local and on-site managers and personnel. It is at this level where local police and municipalities plug into the Touchstone project.

By delving into specific neighborhoods, security conscientiousness is not only enhanced but conducted geographically versus sector specific. As outlined in an earlier example, dealing with one security manager who is responsible for only three floors of a multi-story, multi-tenant office building is insufficient. Instead, fostering a sense of collective security based on geographic location and proximity better serves neighborhoods at risk. Touchstone's involvement at the grassroots promotes the importance of constructive, non-competitive dialogue between private sector owners and operator at the most basic level and helps to foster a sense of community versus individualism.

L. LOOK TO THE SKIES

Touchstone is about developing a sustainable business process for timely, actionable, on-going and bi-directional intelligence information sharing between government and key private sector stakeholders to better address today's threat environment. Identifying vulnerable neighborhoods within an FBI field office's area of responsibility through the use of geo-spatial mapping is a great way of integrating neighborhood partners.

The DHS has the capability to assist with geo-spatial mapping through their:

> Spatial Data Infrastructure (SDI), a subset of the Enterprise Architecture, [which] consists of geographic information systems software and hardware, geospatial applications, data, standards, policies, programs, and the human resources necessary to acquire, process, analyze, store, maintain, distribute and otherwise use geospatial data as a strategic asset for the Department of Homeland Security (DHS or Department) and the nation…. Completing and maintaining an SDI with integrated

> applications and systems will provide the level of geospatial preparedness required to protect the nation's critical infrastructure, strategic assets, the economic base, and America's citizens.[216]

Each field office Special Agent in Charge in conjunction with their DHS PSA should start by mapping their area of responsibility (AOR) using a grid system to delineate manageable regions (see Figure 4). Figure 4 pictures Northern Virginia, Washington, D.C. and Prince George's County, Maryland. This region has been further divided into subsections approximately 3 x 1.5 miles in size. In total, the described area was subdivided into 49 distinct boxes and individually labeled. Each grid space was given an alpha designator starting with "A," which was used to name boxes progressing from west to east. Furthermore, each box was then numbered, starting with "1" moving north to south. Simply, the grid letters/numbers are a naming convention used for easy identification of a particular mapped space.

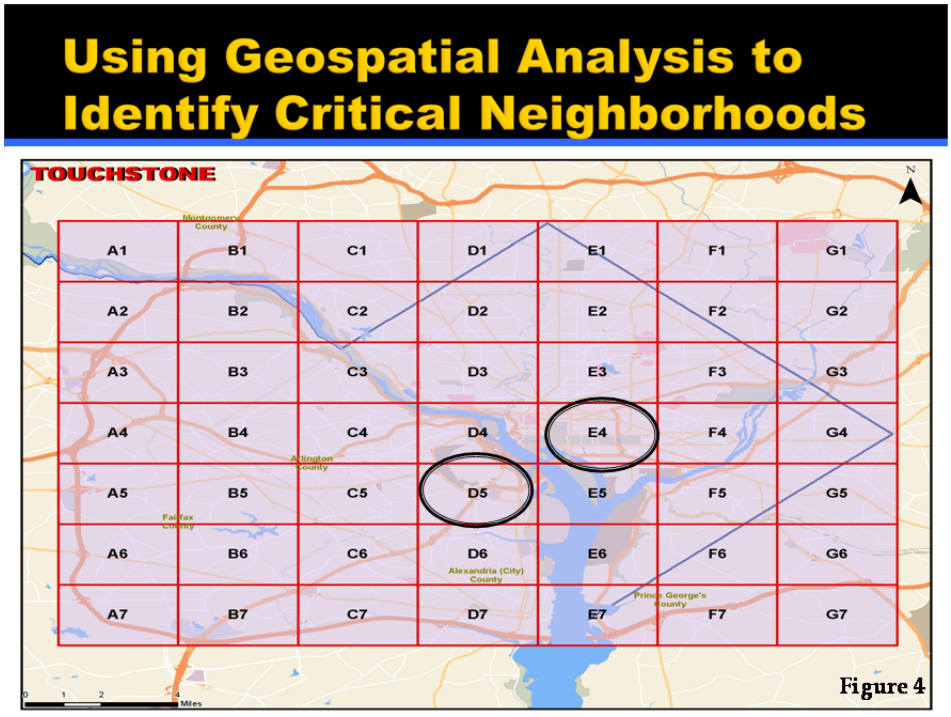

Figure 4. Geospatial Mapping of Greater Washington, D.C.

[216] Department of Homeland Security, "Management Directive System MD Number 4030," November 12, 2004, http://search.dhs.gov/search?utf8=%E2%9C%93&affiliate=dhs&query=geospatial (accessed July 20, 2012).

Once on a grid, significant sector and subsector assets should be identified. For example, within the Washington, D.C. Touchstone group the subsectors listed in Table 2 were plotted.

Table 2. Relevant Sub-Sectors

Entertainment/Media	Gaming
Lodging	Outdoor Events
Public Assembly	Real Estate
Retail	Sports Leagues

Next, likely targets should be added to identify cluster points. For example, public transportation hubs (Metro train stops in the Washington, D.C. metropolitan area) military/Department of Defense presence and facilities, the presence of Jewish establishments, high concentrations of government agencies and/or contractors, and other at risk locations, as identified by each SAC, within a respective AOR must be identified and mapped (see Figure 5).

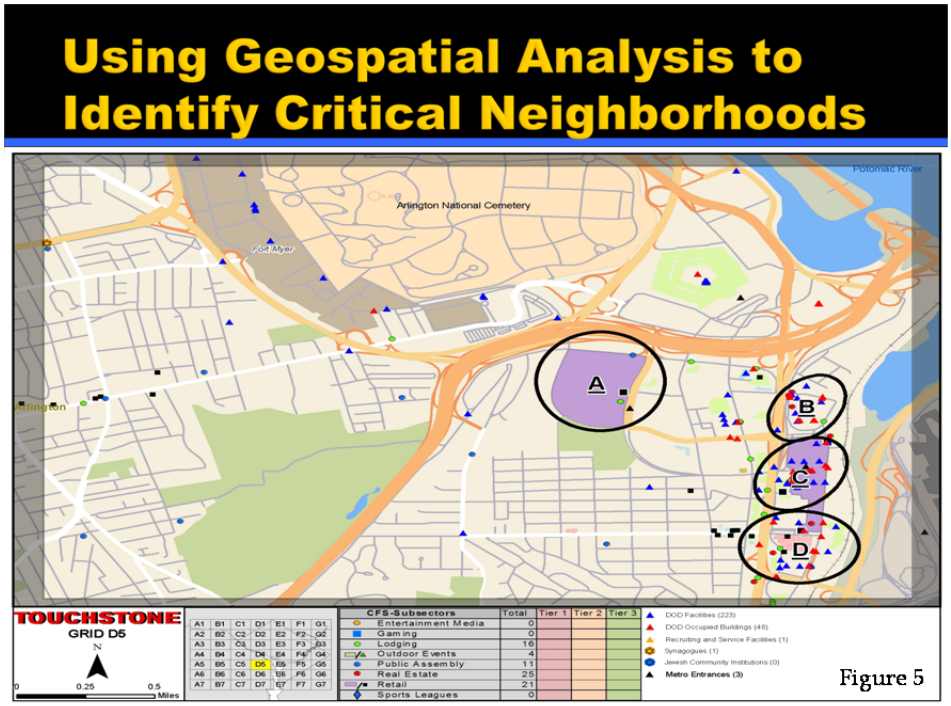

Figure 5. Geospatial Mapping: Critical Neighborhoods

As Figure 5 shows, within grid D5 four significant cluster points or neighborhoods materialized. Each of these neighborhoods, A through D, represents collections of potentially exposed assets. Furthermore, using a modified version of DHS's Level I and II Tiering model for critical infrastructure,[217] each region should be ranked as a Tier 1, Tier 2 or Tier 3 in priority—Tier 1 representing the biggest conglomeration of vulnerabilities while 3 is the least.

To further assist in the prioritization process, daytime and nighttime density mapping should be employed (see Figures 6 and 7).

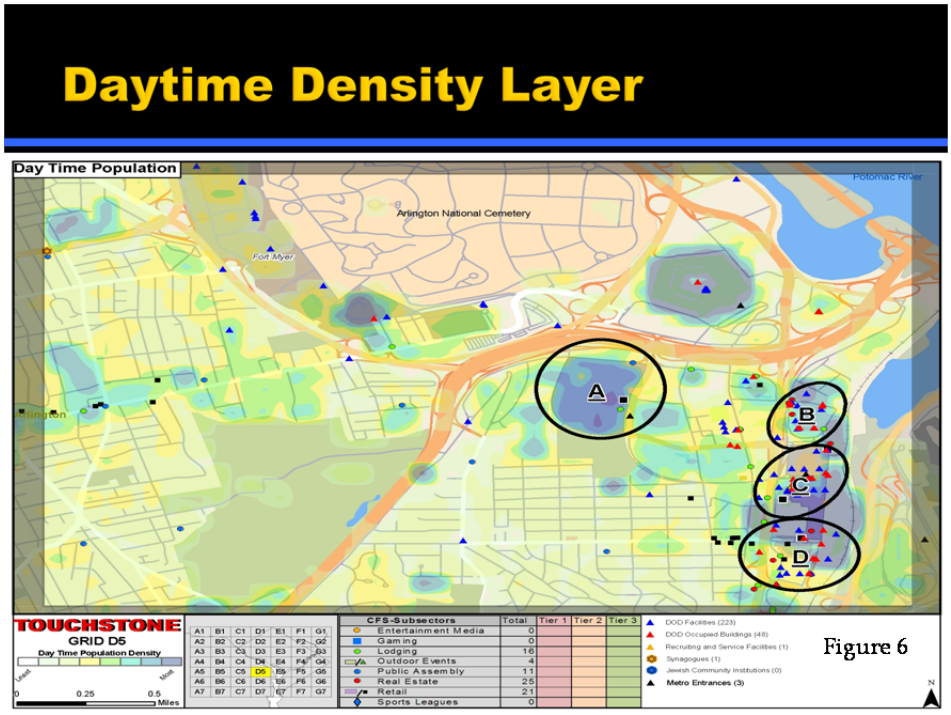

Figure 6. Daytime Density Layer

[217] "The DHS Tier 1 and Tier 2 Program identifies nationally significant critical assets and systems in order to enhance decision making related to CIKR protection. CIKR identified through the program include those that, if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, or widespread and long-term disruptions to national well-being and governance capacity." Department of Homeland Security, *National Infrastructure Protection Plan*, 41.

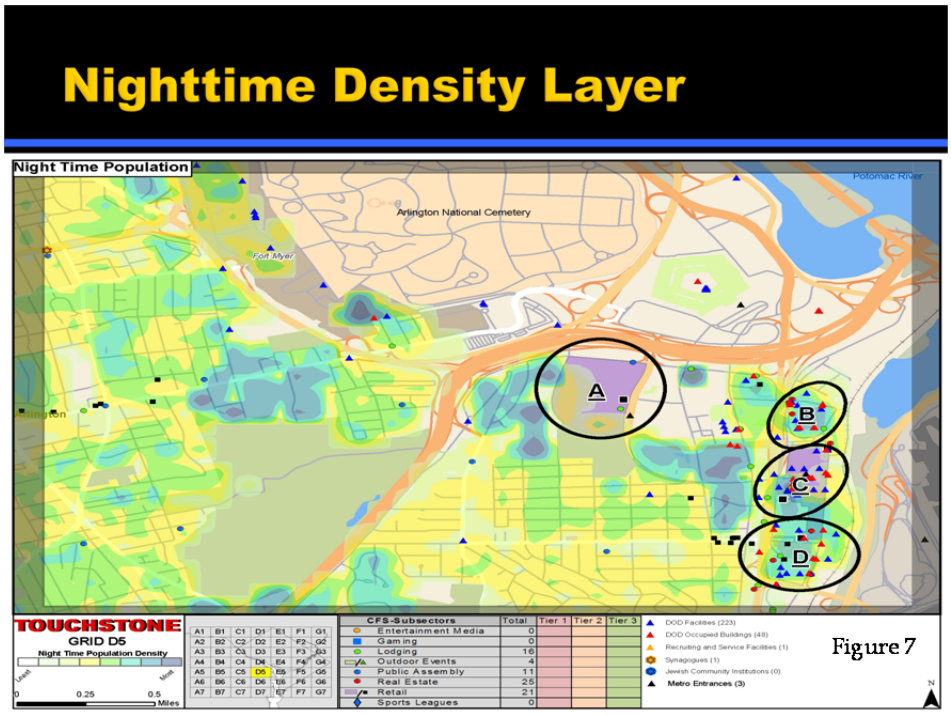

Figure 7. Nightime Density Layer

As depicted, within the D.C. area, neighborhoods A through D are most at risk during the daytime as that is when they are the busiest and most populated. Conversely, the threat to these areas drops significantly during the night. This information is extremely helpful for scenario building (table top exercises) and resource deployment.

Identification of vulnerable neighborhoods lends itself to conducting table top exercises. Table top exercises are an excellent way of moving through a scenario in a very non-threatening relaxed manner. Engaging in exercises helps identify strengths and weaknesses and, most importantly, encouraging interaction and better communication between neighbors. As highlighted in Scenarios: The Art of Strategic Conversation, "Rather than a 'tool' scenario-based planning is a paradigmatic way of strategic thinking that acknowledges uncertainty with all the consequences this entails."218

218 van der Heijden, *Scenarios*, 18.

The Washington, D.C. Touchstone group has spearheaded neighborhood table top exercises within three of its four identified high susceptibility areas (as depicted in Figures 4–7). The session objectives were to:

- Educate both the private sector personnel as well as the government as to standard operating procedures, capabilities, responses, etc. of both entities; and
- Raise awareness levels among both.

Participants were challenged to meet their own organizational objectives, to learn to think in new and different ways and to understand the capabilities of all involved. Each participant was expected (and sometimes forced) to participate with the understanding that operating in an unfamiliar and challenging environment is not easy. The exercise promoted thought-provoking questions and responses as if the scenario were actually taking place. Both private sector and government response protocols were discussed and reviewed for overall effectiveness. Areas of potential weakness or ineffectiveness were identified so they could be revamped and improved.

Throughout the course of the exercises, it was discovered that not only did neighbors not know each other, they were certainly not talking to one another about anything—the least of which was threats, suspicious activities or anything else that may have affected more than what was inside of their own four walls. Interestingly, using table top exercises as a tool to challenge neighborhoods teased-out this little known and alarming fact. Overwhelmingly, feedback from the exercises proved crucial in encouraging neighborhood collaboration and cohesiveness in the future.

Significantly, the exercises should not end with the identification of weaknesses and potential vulnerabilities. Rather, red cell exercises can be administered. According to the U.K. based Red Cell Security Company, "Red Cell training was created after identifying the need for businesses and organisations to continuously test and exercise their Incident Management Plans and assigned management teams."[219] Using red cells, vulnerabilities, weaknesses, decision making, communication, policies and procedures

[219] "Red Cell: Training and Exercises," n.d., http://www.redcellsecurity.co.uk/detail_page.php?ID=3 (accessed August 10, 2012).

can be tested during one afternoon. Evaluating a staff's response to a simulated event is an excellent way to fix problems prior to a crisis.

A red cell exercise involves an independent team, often not affiliated with the target company, used to test an organization's effectiveness. Red cells, often referred to as red teams, provide an adversarial point of view and test the target establishment's responses, policies and procedures—or whatever is deemed a potential weakness by the company's management. The thought is to identify vulnerabilities in a friendly, non-threatening environment in order to make changes prior to a malicious penetration.

For example, the D.C. Touchstone sponsored a table top exercise in the Pentagon City corridor (PCC) in northern Virginia. This area is a hub of critical sectors and subsectors including real estate, retail, hotels, transportation, parking and restaurants. The PCC is minutes from the Pentagon, U.S. National Parks and Monuments and Reagan National Airport. Amidst the PCC sits Pentagon City Mall, home to more than 170 stores, a movie theater and restaurants.[220] The mall is directly connected to the area's mass transit metro-rail, commonly referred to as the "metro." Importantly, during the daytime, this corridor experiences a tremendous influx of tourists and boasts a visible military presence making it a viable and symbolic target.

After the table top exercise, the Vice President, Corporate Security and Emergency Management for the mall's owner, Simon Properties,[221] agreed to put his security staff to the test. The decision to partake in the exercise was made at the executive level so as to not alert any staff to the exercise. A scenario is being built during which a small group of questionable characters will participate in suspicious activities while on the mall grounds. The staff's response and adherence to protocols will be assessed. The results will determine the staff's preparedness should a true event transpire. Red cells are an excellent way to identify positives and negatives in a controlled, non-threatening environment.

---

[220] "Simon Malls," n.d., http://www.simon.com/mall/?id=157 (accessed June 22, 2012).

[221] Referenced Vice President is a member of the D.C. Touchstone group.

M. TOUCHSTONE IS WORKING

The Washington, D.C. Touchstone project is extremely successful. The group has been meeting for over a year. Neither membership nor attendance has diminished. In fact, new participants have been identified and added to the D.C. group. These new members have added value without making the size of the group unmanageable and cumbersome. Significantly, Touchstone is being deployed to several cities, including Detroit, Newark, Indianapolis and Jacksonville. This growth is an example of crossing the chasm as Touchstone moves from its birthplace and spreads to other parts of the country.

The Touchstone Project exemplifies breaking expectations and venturing into uncharted territory. It is "restructuring information sharing in order to gain value."[222] The true value and success of Touchstone is yet to be determined; but, so far Touchstone is very well received among both the private sector and government alike.

N. SUMMARY

Touchstone executes the Prevention Prong of the FBI's Threat Mitigation Strategy for combatting homegrown violent extremists. It is an exportable model hinged upon the integration of the private sector in securing the homeland. The FBI, in partnership with the DHS, will lead the group from the government side of the house. Touchtone membership should be comprised of a small, hand-selected group of executive-level managers—decision makers—representing the field office's major markets. While each Touchstone will look a little different, the concept is the same—building trusted, personal relationships with the private sector in order to most effectively counter today's emerging threats.

Information sharing, developing two-way dialogue and providing context to today's threat information are the cornerstones of Touchstone's mission. Topics of discussion during Touchstone interactions can range from reviewing Intelligence Bulletins, Roll Call Releases, discussing events happening in and around the field office's

[222] Luke Williams, "Disruptive Thinking: Think the Unthinkable to Spark Transformation in Your Business," n.d., http://www.disruptive-thinking.com/ (accessed July 12, 2012).

area of responsibility or even areas of concern as denoted by Touchstone members. Touchstone groups should meet in person and use conference calls for the rapid dissemination of timely information.

Identifying a Touchstone group and vulnerable neighborhoods should be an evolving process enhanced by geo-spatial mapping. Because Touchstone operates on multiple levels, regional and local, table top exercise are an excellent way of identifying and teasing-out potentially at risk neighborhoods. Pinpointing vulnerable neighborhoods at the grassroots level allows for collective security because it is now geographic versus sector specific. A follow-up to table top exercises are red cell exercises. Red teams utilize an adversarial vantage point and are designed to test a region by highlighting positives and negatives in a controlled, non-threatening environment.

In short, Touchstone is a multi-faceted outreach program that goes beyond the "handshake and a smile" posture which so often characterizes outreach. Touchstone is easily replicated, sustainable and a necessary evolution to creating a whole of community approach to securing our nation.

> This collaborative responsibility is best accomplished through a collaboration that leverages the respective capabilities of government and the private sector: the government provides intelligence about potential threats and mobilizes public resources for protection, response and recovery, and the informed private sector uses this information to effectively manage risks and operate infrastructures in the face of such threats.[223]

Securing the homeland is no longer a single agency-led mission. The multitude and volume of threats facing the U.S. requires a collaborative effort by government and non-government partners. As the threat continues to evolve, so must the government's response.

[223] National Infrastructure Advisory Council, *Critical Infrastructure,* 4.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. CONCLUSION

A. CONCLUSION AND RECOMMENDATIONS

Threats to the U.S. homeland and interests abroad are alive and well. The death of bin Laden has not dissuaded radical Islamist extremists' desire to attack the West and Western interests. Moreover, a few tactical successes—specifically targeted drone strikes and other military actions—do not equate to strategic victory. Indeed, the threat from transnational terrorism remains a chief concern for homeland security authorities. However, the threats from homegrown violent extremists, lone offenders and domestic terrorists have become more concerning over the years. Alarmingly, the Arab Spring throughout the Middle East has sparked unrest throughout the region—this turbulence has resulted in an uptick of violence and anti-American rhetoric. Moreover, the world is increasingly connected by virtue of the Internet and other forms of social media. The Internet in particular has become the medium through which extremists export their recruitment, radicalization and proselytizing activities. As the threats become more disparate, disjointed and diverse, so must our counterterrorism tactics.

Neither legislation nor good ideas have manifested themselves in a sustainable business model for the integration of the private sector into the homeland security fold. Touchstone fills the gap and cements the private sector as permanent partners in the fight. Touchstone accomplishes this task through the development of personal, trusted relationships with a small, manageable group of executive-level security managers; through the timely dissemination of tailored, actionable intelligence information and by fostering an environment of bi-directional dialogue and feedback. Touchstone goes beyond the gentleman's handshake and recognizes the need to share versus the need to know.

This innovative project breaks down barriers and strives to operate at both the regional and neighborhood levels. At the neighborhood level, Touchstone takes on a geographic approach to countering today's threat and invites communities of businesses and key stakeholders to thwart dangers as a neighborhood. This horizontal methodology

of countering threats is very different from most other outreach programs which tend to focus on sectors. During neighborhood table top exercises Touchstone integrates affected targets, their unwitting neighbors and the local police to discuss threat mitigation plans and encourage communication. Touchstone has been underway in the greater Washington, D.C. Metropolitan area for about 16 months and is extremely successful. It is so efficacious, Touchstone is due to deploy to Newark, Jersey City, Atlantic City, Detroit, Jacksonville, Indianapolis and Los Angeles.

B. RECOMMENDATIONS

1. A Touchstone Group should be Established within All 56 of the FBI's Field Offices

Touchstone is an innovative sea change way of thinking for the FBI and government as a whole. In partnership with the DHS, Touchstone fully integrates the private sector into the homeland security fold by regularly sharing timely, actionable intelligence information to key private sector stakeholders. Touchstone's cornerstone is trust. Members share security concerns and viable solutions in a non-competitive environment. Additionally, Touchstone partners are executive level and, therefore, decision makers. Significantly, unlike other outreach programs Touchstone operates at both the regional and neighborhood levels. Within the neighborhood stratum the project identifies and exercises information sharing through table top exercises. Notably, Touchstone emphasizes a geographic approach to security at the neighborhood level. This approach ensures all involved, and seemingly uninvolved, businesses are aware of current and emerging threats in addition to the best way to thwart them as an entire community. Furthermore, identified gaps and vulnerabilities are tested and re-tested through the use of red cell training. Within an FBI field offices' area of responsibility, Touchstone spearheads and facilitates cooperation and coordination at all levels. Lastly, Touchstone fills the void where other outreach programs have fallen short. It is popular, it is necessary and it is working as has been demonstrated by the success of the D.C. Touchstone group.

2. A National Business Registry should be Developed in Conjunction with Touchstone Groups Nationwide

The national business registry will serve as a repository of private sector security points of contact for use by the FBI and, in some cases, other law enforcement personnel. Undoubtedly, this catalogue will be primarily comprised of Touchstone members from groups across the country. This storehouse will serve to reduce confusion and increase the efficiency with which the private sector assists authorities. Because the index is largely made up of trusted Touchstone partners, the FBI can feel confident these contacts are already trusted and vetted. Moreover, the members are in positions to make immediate decisions, take necessary actions—perhaps at the behest of the FBI—and quickly facilitate the needs of the FBI. The directory should be maintained by each field office's Touchstone SSA. This SSA should act as the gate keeper, ensuring appropriate use and dissemination of private sector points of contact.

3. Touchstone should be Integrated into the FBI's DSAC Program for Nationwide Management

Touchstone must have all encompassing oversight at an FBI headquarters level. DSAC is the appropriate place for this as its mission is to liaise with the private sector. Moreover, DSAC already has the infrastructure and has built the muscle-memory necessary to adopt Touchstone as a sub-program. Likewise, DSAC reports to the FBI Director's Office and, because of this, program management of Touchstone at this level within FBI headquarters will ensure continued FBI buy-in and support.

4. The DSAC Analytical Cadre and Support Staff should be Greatly Increased

To fully support the FBI's Touchstone groups around the country, the DSAC infrastructure must be enhanced with full-time analysts. Ideally, the analytical resources should mirror the private sector's demarcation with at least one team per sector. These analytical teams should author an intelligence product specifically tailored to the private sector. The piece should mirror that of DSAC's overseas Department of State counterpart. It should provide timely, actionable and tailored information particularly geared toward the private sector's security of their assets. DSAC products should be

regularly disseminated to Touchstone members and further discussed during Touchstone meetings and bridge calls.

5. DSAC Leadership Training should Incorporate a Leadership Exchange Program Much Like the British *London First* Docket

Such a program will encourage communication among government and business leaders on a more personal level. All will benefit from the exchange of ideas and the trusted relationships that develop. In addition, incorporating another facet to the DSAC portfolio should prove to increase its popularity and effectiveness as a leading proponent of private sector integration.

6. Infragard should Continue and Complement Touchstone in its Programing and Membership

InfraGard should incorporate a training curriculum similar to the U.K.'s *Projects Griffin* and *Argus*. InfraGard should incorporate in person and on-line refreshers in order to ensure consistency throughout the private security mid and lower-level security professionals. Accrediting the training programs, like the U.K.'s programs, will contribute to their importance and necessity within the security industry.

7. A Counterterrorism Supervisory Special Agent (SSA) Must Attend All Touchstone Meetings and Related Events

The permanent attendance of an FBI Supervisory Special Agent will ensure continuity of the program. Furthermore, it will demonstrate the FBI's commitment to the program. Additionally, this SSA should act as the main point of contact for all Touchstone members' concerns and requests. Finally, this SSA should work with the Touchstone members to develop meeting agendas and table top exercises within identified neighborhoods.

To most comprehensively address existing and emerging threats facing the nation, the private sector must be integrated into the homeland security enterprise. Touchstone is a necessary evolution and plausible solution to the current gap in our security enterprise. The D.C. Touchstone project joins private sector security executives with the FBI and DHS wherein trusted relationships are developed and nurtured, timely and actionable

intelligence information is disseminated, ideas are exchanged in a non-competitive environment and, most importantly, all know, understand and want to protect all aspects of the United States of America and America's way of life.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

"7 July Bombings: Introduction." *BBC News*. n.d. http://news.bbc.co.uk/2/shared/spl/hi/uk/05/london_blasts/investigation/html/introduction.stm. Accessed April 21, 2012.

21st Century's Phenomenon: Al-Qaeda New English On Line Magazine "*Inspire*." Global Jihad. N.d. http://globaljihad.net/view_news.asp?id=1535. Accessed July 23, 2011.

A Strong Britain in an Age of Uncertainty: The National Security Strategy. 2010. http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy. Accessed November 19, 2011.

"About the Intelligence Community." n.d. http://www.intelligence.gov/about-the-intelligence-community/. Accessed July 15, 2012.

"Al-Qaida/Al-Qaeda (The Base)." June 6, 2012. GlobalSecurity. http://www.globalsecurity.org/military/world/para/al-qaida.htm. Accessed August 24, 2012.

"Al-Qaeda and al-Shabab: Double the Trouble? We Ask What the Formal Merger of the Two Groups Means for the Conflict in Somalia." *Al Jazeera*. February 11, 2012. http://www.aljazeera.com/programmes/insidestory/2012/02/201221017451210571 8.html. Accessed August 23, 2012.

"Al-Aqaeda in the Arabian Peninsula: Who Are They? Channel 4 News Looks at the al-Qaeda Group in the Arabian Peninsula Linked to Explosives Found on Two Cargo Planes, and Public Enemy No 1 for the UK Intelligence Services, Anwar al-Awlaki." *Channel 4 News*. October 30, 2010. http://www.channel4.com/news/al-qaeda-in-the-arabian-peninsula-who-are-they. Accessed July 23, 2011.

American Heritage Dictionary of the English Language (4th ed.). s.v. "Touchstone." 2009. http://www.thefreedictionary.com/touchstone. Accessed July 11, 2012.

AQ Chef. "How to Make a Bomb in the Kitchen of Your Mom." *Inspire*. Summer 2010.

"AQAP Urges US Sympathizers to Attack Malls, Nightclubs." *New Media Journal*. N.d. http://newmediajournal.us/indx.php/item/995?sms_ss=newsvine&at_xt=4d94a71def0a6cae%2C0. Accessed September 8, 2012.

Aynte, Abdi. “Understanding the Al-Shabaab /Al-Qaeda ‘Merger.’” *African Arguments*. March 19, 2012. http://africanarguments.org/2012/03/19/understanding-the-al-shabaabal-qaeda-%E2%80%98merger%E2%80%99-by-abdi-aynte/. Accessed August 22, 2012.

Baker, Al and William K. Rashbaum. “Police Find Car Bomb in Times Square.” *New York Times*. May 1, 2010. http://www.nytimes.com/2010/05/02/nyregion/02timessquare.html?pagewanted=all. Accessed July 16, 2012.

BBC News. “Profile: Egypt’s Muslim Brotherhood.” June 26, 2012. BBC News, Middle East. http://www.bbc.co.uk/news/world-middle-east-12313405. Accessed July 7, 2012.

Bergen, Peter L. *Holy War, Inc.: Inside the Secret World of Osama bin Laden*. New York: The Free Press; 2001.

Best Jr., Richard A. *Intelligence Issues for Congress*. Washington, DC: Congressional Research Service, 2011.

“Bombing Prevention Training.” n.d. http://www.dhs.gov/files/programs/gc_1265223119415.shtm. Accessed July 21, 2012.

Burton, Fred, and Scot Stewart. Al Qaeda and the Tale of Two Battlespaces. *STRATFOR Global Intelligence Weekly*. October 1, 2008. http://www.stratfor.com/weekly/20081001_al_qaeda_and_tale_two_battlespaces Accessed July 23, 2011.

———. “Al Qaeda in the Arabian Peninsula: Desperation or a New Life?” *STRATFOR Global Intelligence Weekly*. January 28, 2009. http://www.stratfor.com/weekly/20090128_al_qaeda_arabian_peninsula_desperation_or_new_life. Accessed July 23, 2011.

Cilluff, Frank and Clinton Watts. “Countering the Threat Posed by AQAP: Embrace, Don’t Chase Yemen’s Chaos.” *Homeland Security Policy Institute Security Debrief*. July 14, 2011. http://securitydebrief.com/2011/07/14/countering-the-threat-posed-by-aqap-embrace-don%E2%80%99t-chase-yemen%E2%80%99s-chaos/ Accessed July 23, 2011.

Cochrun, Cassandra. “What are the Differences Between Private and Public Sector Security?” n.d. http://www.ehow.com/about_5106799_differences-private-public-sector-security.html. Accessed September 8, 2012.

Compilation of Homeland Security Presidential Directives (HSPD) (Updated through December 31, 2007), Prepared for the use of the Committee on Homeland Security of the House of Representatives. Washington, DC: U.S. Government Printing Office, 2008.

"Critical Infrastructure Protection in the Information Age." Executive Order no. 13,231. October 16, 2001. National Communications Systems. http://www.ncs.gov/library/policy_docs/eo_13231.pdf. Accessed September 6, 2012.

Curran, Cody, James Gallagher, Courtney Hughes, Paul Jarvis, Adam Kahan, Patrick Knapp, Matthew Lu, and Jared Sorhaindo. "AEI Critical Threats: AQAP and AQAP Suspected Attacks in Yemen Tracker 2010, 2011 and 2012." May 21, 2012. http://www.criticalthreats.org/yemen/aqap-and-suspected-aqap-attacks-yemen-tracker-2010. Accessed August 24, 2012.

Defense Intelligence Agency. *Intelligence Information Report 2 104 0256 12*. April 17, 2012.

Department of Homeland Security. "About the Office of Infrastructure Protection." n.d. http://www.dhs.gov/about-office-infrastructure-protection. Accessed September 4, 2012.

———. "Critical Infrastructure." n.d. http://www.dhs.gov/critical-infrastructure. Accessed February 28, 2012.

———. *Daily Open Source Infrastructure Report*. 2009. http://www.dhs.gov/dhs-daily-open-source-infrastructure-report Accessed August 25, 2012.

———. "DHS Snapshot: Yemen Explosive Packages on Cargo Aircraft; November 1, 2010 in Department of Homeland Security: Explosives Discovered in Packages on Cargo Aircraft Bound for the Homeland." November 1, 2010. Public Intelligence. http://publicintelligence.net/ufouo-dhs-snapshot-yemen-explosive-packages-on-cargo-aircraft/. Accessed July 23, 2011.

———. "Management Directive System MD Number 4030." November 12, 2004. http://search.dhs.gov/search?utf8=%E2%9C%93&affiliate=dhs&query=geospatial Accessed July 20, 2012.

———. "National Infrastructure Advisory Council." n.d. http://www.dhs.gov/files/committees/editorial_0353.shtm. Accessed March 18, 2012.

———. *National Infrastructure Protection Plan*. Washington, DC: Department of Homeland Security, 2009.

———. “Proposal to Create the Department of Homeland Security.” n.d. http://www.dhs.gov/proposal-create-department-homeland-security. Accessed September 4, 2012.

———. *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*. Washington, DC: Department of Homeland Security, 2010.

Denning, Steve. “How Do You Change an Organizational Culture?” *Forbes*. July 23, 2011. http://www.forbes.com/sites/stevedenning/2011/07/23/how-do-you-change-an-organizational-culture/. Accessed July 12, 2012.

Denson, Bryan. “FBI Thwarts Terrorist Bombing Attempt at Portland Holiday Tree Lighting, Authorities Say.” *The Oregonian*. November 26, 2010. Oregon Live. http://www.oregonlive.com/portland/index.ssf/2010/11/fbi_thwarts_terrorist_bombing.html. Accessed July 16, 2012.

District of Oregon, U.S. Attorney’s Office. “Oregon Resident Arrested in Plot to Bomb Christmas Tree Lighting Ceremony in Portland; Vehicle Bomb Left at Scene was Inert and Posed No Danger to Public” [press release]. November 26, 2010. Portland Division, Federal Bureau of Investigation. http://www.fbi.gov/portland/press-releases/2010/pd112610.htm. Accessed August 24, 2012).

“Do we think differently? Linear vs. Non-Linear Thinking.” *Chuck’s Lamp* [blog]. April 11, 2009. http://chuckslamp.com/index.php/2009/04/11/non-linearthinking/. Accessed July 7, 2012.

Domestic Security Alliance Council. “Domestic Security Alliance Council.” n.d. http://www.dsac.gov/Pages/join.aspx. Accessed August 27, 2012.

———. “DSAC Leadership Board.” n.d. http://www.dsac.gov/Pages/dlb.aspx. Accessed July 28, 2012.

———. “Enhancing Security for American Businesses” [brochure]. n.d. http://www.dsac.gov/Pages/DSAC_Brochure.pdf. Accessed August 27, 2012.

Ervin, Clark Kent. “Terrorism’s Soft Targets.” *Washington Post*. May 7, 2006. http://www.washingtonpost.com/wp-dyn/content/article/2006/05/05/AR2006050501754.html. Accessed July 27, 2012).

“Famous Cases and Criminals.” n.d. Federal Bureau of Investigation. http://www.fbi.gov/about-us/history/famous-cases/. Accessed July 16, 2012).

Federal Bureau of Investigation. “Partnerships and Outreach.” http://www.fbi.gov/about-us/partnerships_and_outreach/. Accessed July 15, 2012.

Federal Bureau of Investigation and Department of Homeland Security. “Ten-Year Anniversary of 9/11 Attacks: No Specific Threats, but a Potentially Attractive Terrorist Target.” *Joint Intelligence Bulletin*. August 10, 2011.

Ferran, Lee, Bazi Kanani, and Dana Hughes. “Theater Explosion Kills Several in Mogadishu.” *ABC News*. April 4, 2012. http://abcnews.go.com/Blotter/al-shabaab-claims-theater-explosion-kills-mogadishu/story?id=16070499. Accessed August 22, 2012.

“Future of the Global Muslim Population: Projections for 2010–2030.” January 2011. Pew Forum on Religion and Life. http://www.pewforum.org/future-of-the-global-muslim-population-main-factors-age-structure.aspx. Accessed September 13, 2012.

Giuliano, Mark F. “Post 9/11 FBI: The Bureau’s Response to Evolving Threats.” Speech to Washington Institute for Near East Policy Stein Program on Counterterrorism and Intelligence Washington, D.C., April 14, 2011. Federal Bureau of Investigation. http://www.fbi.gov/news/speeches/the-post-9-11-fbi-the-bureaus-response-to-evolving-threats. Accessed July 23, 2011.

Government Accountability Office. *Critical Infrastructure Protection Coordination Issues* (GAO-07-39). Washington, DC: Government Accountability Office, 2006.

Gunaratna, Rohan. *Inside Al Qaeda: Global Network of Terror*. New York: Berkley Books, 2003.

———. *The Islamabad Marriott in Flames: Attack on the World’s Most Protected Hotel*. Singapore: International Centre for Political Violence and Terrorism Research, 2008.

Hays, Tom. “Zazi Testifies at Subway Plot Trial.” *Associated Press*. April 17, 2012. ABC News. http://abclocal.go.com/wabc/story?section=news/local/new_york&id=8624058. Accessed September 8, 2012.

Henderson, William. “How Much Does It Really Cost to Get a Security Clearance?” August 7, 2011. http://www.clearancejobs.com/cleared-news/381/how-much-does-it-really-cost-to-get-a-security-clearance. Accessed August 22, 2012.

Hoffman, Bruce. *The Use of the Internet by Islamic Extremists* [Testimony before the Permanent Select Committee on Intelligence United States House of Representatives]. May 4, 2006. Rand Corporation. http://www.rand.org/content/dam/rand/pubs/testimonies/2006/RAND_CT262-1.pdf. Accessed July 23, 2011.

"Home Office." n.d. http://www.sia.homeoffice.gov.U.K./Pages/home.aspx. Accessed March 21, 2012.

Homeland Security Council. *National Strategy for Homeland Security*. Washington, DC: Homeland Security Council, 2007.

InfraGard. "About InfraGard." 2012. http://www.infragard.net/about.php?mn=1&sm=1-0 Accessed August 25, 2012.

———. "Become a Member of InfraGard." n.d. http://www.infragard.net/member.php?mn=2 Accessed August 26, 2012.

———. "Links/In the News." n.d. http://www.infragard.net/about.php?mn=1&sm=1-0 Accessed August 26, 2012.

Joscelyn, Thomas. "Analysis: Two Ex-Gitmo Detainees Featured in Al Qaeda's Inspire Magazine." *Long War Journal*. October 13, 2010. http://www.longwarjournal.org/archives/2010/10/analysis_two_exgitmo.php. Accessed July 23, 2011.

Khan, Azmat. "Understanding Yemen's Al Qaeda Threat." May 29, 2012. PBS. http://www.pbs.org/wgbh/pages/frontline/foreign-affairs-defense/al-qaeda-in-yemen/understanding-yemens-al-qaeda-threat/. Accessed August 24, 2012.

"Killing of Awlaki Is Latest in Campaign Against Qaeda Leaders." *New York Times*. September 30, 2011. http://www.nytimes.com/interactive/2011/09/30/world/middleeast/the-killing-of-anwar-al-awlaki.html. Accessed September 8, 2012.

Kohlmann, Evan F. "A Beacon for Extremists: The Ansar al-Mujahideen Web Forum." February 3, 2010. Combatting Terrorism Center at West Point. http://www.ctc.usma.edu/posts/a-beacon-for-extremists-the-ansar-al-mujahideen-web-forum. Accessed July 23, 2011.

Lakshmi, Rama, "Indian Police Arrest Key Suspect in 2008 Mumbai Attack Case." *Washington Post*. June 26, 2012. http://www.washingtonpost.com/world/asia_pacific/indian-police-arrest-key-suspect-in-mumbai-attack-case/2012/06/25/gJQAXrnG1V_story.html. Accessed September 30, 2011.

Leadership Exchange. *Sharing Expertise between Police and Business Leaders*. London: Leadership Exchange, n.d.

Lenain Patrick, Marcos Bonturi, and Vincent Koen. "OECD Economics Department: The Economic Consequences of Terrorism." Working paper no. 334, Organization for Economic Co-operation and Development, Paris, France, 2002.

"London First." n.d. http://www.londonfirst.co.uk/about-us/. Accessed June 22, 2012.

London Stationery Office. *Report of the Official Account of the Bombings in London on 7th July 2005*. 2006. BBC News. http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/11_05_06_narrative.pdf Accessed April 22, 2012.

Marriott. "Marriott." n.d. http://www.marriott.com/culture-and-values/jw-marriott-jr.mi. Accessed September 5, 2012.

———. *Marriott 2011–2012 Sustainability Report*. 2012. http://www.marriott.com/Multimedia/PDF/CorporateResponsibility/MarriottSustainabilityReport_2011and2012condensed10MB.pdf. Accessed September 5, 2012.

———. "Corporate Responsibility." n.d. http://www.marriott.com/corporate-social-responsibility/corporate-responsibility.mi. Accessed September 6, 2012.

———. "Safety and Security Information." February 1, 2012. http://news.marriott.com/safety-and-security-information.html. Accessed September 8, 2012.

MacDonald, Jay. "How 9/11 Redefined Insurance." Insurance Blog. September 9, 2011. http://www.bankrate.com/financing/insurance/how-911-redefined-insurance/ Accessed September 5, 2012.

"Making a Difference." n.d. London First. http://www.londonfirst.co.U.K./about-us/making-a-difference/. Accessed March 18, 2012.

Meulemans, Michael. "Insurance: 9/11 Changed Insurance Sector Forever." September 14, 2011. http://insurance.about.com/od/Property/a/9-11-Changed-Insurance-Sector-Forever.htm Accessed August 31, 2012.

Mitchell, Melanie. *Complexity: A Guided Tour* (Kindle version). Oxford: Oxford University Press; 2009.

Moteff, John and Paul Parfomak. *Critical Infrastructure and Key Assets: Definition and Identification*. Washington, DC: Congressional Research Service, 2004.

Moyers, Bill. “Brief History of Al Qaeda.” *Bill Moyers Journal*. July 27, 2007. PBS. http://www.pbs.org/moyers/journal/07272007/alqaeda.html. Accessed July 7, 2012.

Mueller, III, Robert S. “Watchmen on the Walls of our Freedom.” Speech National Academy Associates Annual Training Conference, Grapevine, Texas, July 31, 2012. Federal Bureau of Investigation. http://www.fbi.gov/news/speeches/watchmen-on-the-walls-of-our-freedom. Accessed August 25, 2012.

National Counterterrorism Center. “Al-Qa’ida in the Arabian Peninsula (AQAP).” National Counterterrorism Center. n.d. http://www.nctc.gov/site/groups/aqap.html. Accessed July 23, 2011.

National Counter Terrorism Security Office. “NaCTSO: Who We Are and What We Do.” n.d. http://www.nactso.gov.uk/Default.aspx. Accessed June 22, 2012.

National Counter Terrorism Security Office “Project Argus” n.d. http://www.nactso.gov.U.K./OurServices/*Argus*.aspx. Accessed March 18, 2012.

National Infrastructure Advisory Council. *Critical Infrastructure Partnership Strategic Assessment: Final Report and Recommendations*. Washington, DC: National Infrastructure Advisory Council, 2008.

———. *Intelligence Information Sharing: Final Report and Recommendations.* Washington, DC: National Infrastructure Advisory Council, 2012.

“Networks.” n.d. London First. http://www.londonfirst.co.U.K./networks2/ Accessed March 18, 2012.

Northern District of Texas, U.S. Attorney’s Office. “FBI Arrests Jordanian Citizen for Attempting to Bomb Skyscraper in Downtown Dallas” [press release]. September 24, 2009. Dallas Division, Federal Bureau of Investigation. http://www.fbi.gov/dallas/press-releases/2009/dl092409.htm. Accessed August 24, 2012.

“NYPD Shield.” n.d. http://www.nypdshield.org/public/about.aspx. Accessed April 12, 2011.

Office of Homeland Security. *National Strategy for Homeland Security*. Washington, DC: Office of Homeland Security, 2002.

“Our Successes” n.d. London First. http://www.londonfirst.co.U.K./our-successes/. Accessed April 26, 2012.

Overseas Security Advisory Council. “About OSAC.” n.d. https://www.osac.gov/Pages/AboutUs.aspx Accessed August 27, 2012.

———. “Newsletter.” n.d. https://www.osac.gov/Pages/NewsLetter.aspx. Accessed August 28, 2012.

“Police Avert Car Bomb ‘Carnage;’ A Car Bomb Planted in Central London Would Have Caused ‘Carnage’ If It Had Exploded, Police Say.” *BBC News*. June 29, 2007. http://news.bbc.co.uk/2/hi/6252276.stm. Accessed April 21, 2012.

“Private Sector; Definition of ‘Private Sector.’” n.d. Investopedia. http://www.investopedia.com/terms/p/private-sector.asp. Accessed August 31, 2012.

“Project Griffin.” n.d. http://www.projectgriffin.org.U.K./. Accessed June 22, 2102.

“Protective Security Advisors.” n.d. http://www.dhs.gov/files/programs/gc_1265310793722.shtm Accessed July 22, 2012.

Raghavan, Sudarsan. “Awlaki Hit Misses al-Qaeda Bomb Maker, Yemen Says.” *Washington Post*. October 1, 2011. http://www.washingtonpost.com/world/anwar-al-aulaqi-us-born-cleric-linked-to-al-qaeda-killed-yemen-says/2011/09/30/gIQAsoWO9K_story.html. Accessed August 24, 2012.

Raman, B. “Terrorist Target Hotels Again: This Time in Jakarta; International Terrorism Monitor” (Paper no. 543). July 17, 2009. South Asia Analysis Group. http://www.southasiaanalysis.org/%5Cpapers34%5Cpaper3310.html. Accessed September 7, 2012.

“Red Cell: Training and Exercises.” n.d. http://www.redcellsecurity.co.uk/detail_page.php?ID=3 Accessed August 10, 2012.

Ross, Brian, Rhonda Schwartz, Jason Ryan and Richard Esposito. “Forty Names Appear on Terrorists’ Hit List.” *ABC News, The Blotter*. June 16, 2011. http://abcnews.go.com/Blotter/forty-names-terrorists-hit-list/story?id=13861410. Accessed July 27, 2012.

Saeed, Ali. “AQAP, Military Fight Pitched Battles Abyan.” *Yemen Times*. June 8, 2011. http://www.yementimes.com/defaultdet.aspx?SUB_ID=36179. Accessed July 23, 2011.

"Security and Resilience Network: Guidance." n.d. London First. http://www.londonfirst.co.uk/networks2/security--resilience/security-and-resilience-networ2/ Accessed June 21, 2012.

"Skills for Security." n.d. http://www.skillsforsecurity.org.U.K./. Accessed March 21, 2012).

"Simon Malls." n.d. http://www.simon.com/mall/?id=157. Accessed June 22, 2012.

Southern District of New York, U.S. Attorney's Office. "Faisal Shahzad Sentenced in Manhattan Federal Court to Life in Prison for Attempted Car Bombing in Times Square" [press release]. October 5, 2010. New York Field Office, Federal Bureau of Investigation. http://www.fbi.gov/newyork/press-releases/2010/nyfo100510.htm. Accessed August 24, 2012.

Statement of Alan Orlob, Vice President Corporate Security and Loss Prevention, Marriott International Lodging; On behalf of the Real Estate Roundtable American Hotel and Lodging Association; Before the Senate Committee on Homeland Security and Government Affairs; Hearing on Lessons from the Mumbai Terrorist Attacks, Part II." January 28, 2009. www.hsgac.senate.gov/download/012809orlob. Accessed September 5, 2012.

"Terrorist Attacks in the US or Against Americans." 2011. http://www.infoplease.com/ipa/A0001454.html. Accessed September 30, 2011.

Tiku, Nitasha. "The Terrorists Are Coming from Inside the Country! American Citizens Now Our Biggest Threat." *New York Magazine*. September 10, 2010. http://nymag.com/daily/intel/2010/09/american_citizens_are_now_our-_biggest_threat.html. Accessed July 23, 2011.

"Topic: Anwar Al-Awlaki." *The Washington Times*. 2012. http://www.washingtontimes.com/topics/anwar-al-awlaki/. Accessed July 23, 2011.

United Kingdom Home Office. *CONTEST: The United Kingdom's Strategy for Countering Terrorism*. 2011. http://www.homeoffice.gov.U.K./publications/counter-terrorism/counter-terrorism-strategy/contest-summary?view=Binary. Accessed November 18, 2011.

United States Department of Labor, Bureau of Labor Statistics. "Databases, Tables and Calculators by Subject." N.d. http://data.bls.gov/timeseries/LNS11300000. Accessed July 17, 2012.

van der Heijden, Kees. *Scenarios: The Art of Strategic Conversation* (2nd ed. and Kindle edition). Hoboken, NJ: John Wiley & Sons, Ltd, 2004.

Wikipedia. s.v. “City of London.” n.d. http://en.wikipedia.org/wiki/City_of_London. Accessed November 18, 2011.

Wikipedia. s.v. “Infidel.” n.d. http://en.wikipedia.org/wiki/Infidel. Accessed July 8, 2012.

Wikipedia. s.v., “Police.” n.d. http://en.wikipedia.org/wiki/Police. Accessed March 18, 2012.

Wikipedia. s.v. “Special Branch.” N.d. http://en.wikipedia.org/wiki/Special_Branch. Accessed June 22, 2012.

Wikipedia. s.v. “Table of Police Forces in the United Kingdom.” n.d. http://en.wikipedia.org/wiki/Table_of_police_forces_in_the_United_Kingdom. Accessed April 4, 2012.

Wikipedia. s.v. “United Kingdom’s Home Office.” n.d. http://en.wikipedia.org/wiki/Home_Office. Accessed March 14, 2012.

White House. *National Strategy for Counterterrorism*. Washington, D.C.: White House, 2011.

———. *National Security Strategy*. Washington, DC: White House, 2010.

Williams, Luke. “Disruptive Thinking: Think the Unthinkable to Spark Transformation in Your Business.” n.d. http://www.disruptive-thinking.com/. Accessed July 12, 2012.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Brenda L. Heck
   Disney Corporation
   Burbank, California

4. Joseph B. Donovan
   BeaconCapital Partners
   Arlington, Virginia

5. James W. McJunkin
   Federal Bureau of Investigation
   Washington, D.C.

6. R. J. Holley
   Federal Bureau of Investigation
   Washington, D.C.

7. C. Bryan Paarmann
   Federal Bureau of Investigation
   Washington, D.C.