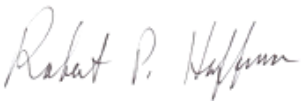
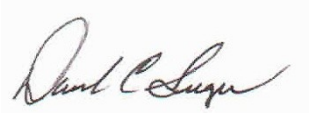
PRIVATIZING HOMELAND SECURITY:
HOW TO EFFICIENTLY INVOLVE THE PRIVATE FINANCIAL SECTOR
IN COMBATING TERRORIST FINANCING IN THE UNITED STATES

by

Sven A. Moeller

Project Committee:

Robert Hoffman, Sponsor 

David Surges, Reader 

Approved May 13, 2010

Submitted in partial fulfillment of the requirements for the degree of Master of Business Administration, The College of St. Scholastica.

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

Abstract

This paper investigates terrorist financing in the United States and how it is currently combated and prevented by the government agencies that operate under the Department of Homeland Security (DHS). It examines what specific areas and practices of the DHS could be improved through deeper integration with the private financial sector and better utilization of its intelligence, technology, and human resources. Out of the regulatory and operational tools the DHS has access to, this paper finds the Cornerstone partnerships and Trade Transparency Units (TTUs) - as initiated by the Immigrations and Customs Enforcement (ICE) - the most successful so far; representing two important ways financial institutions can be further integrated to better combat terrorist financing. Mandatory Cornerstone partnerships between financial institutions and local law enforcement agencies could help raise a higher awareness of current suspicions of terrorist financing and generate more qualitative reporting to authorities. An increase in TTUs, or equivalent partnerships between nations, would greatly simplify future investigations and detection of illegal transactions tied to terrorist cells and organizations in support of terrorism.

Keywords: terrorist financing, money laundering, financial institutions, USA PATRIOT ACT, Department of Homeland Security, Immigrations and Customs Enforcement, privatization, Cornerstone, Trade Transparency Units, Suspicious Activity Reports.

Table of Contents

PRIVATIZING HOMELAND SECURITY: HOW TO EFFICIENTLY INVOLVE THE PRIVATE FINANCIAL SECTOR IN COMBATING TERRORIST FINANCING IN THE UNITED STATES

In the aftermath of the 9/11 terror attacks, several major legislative initiatives were created to prevent or deter future attacks on United States soil. The "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" (USA PATRIOT ACT) of 2001 increased the ability of government agencies to detect terrorist activities within the country through improved communications surveillance and expanded intelligence gathering, and it allowed the Secretary of the Treasury to impose new regulations on financial institutions to stop terrorist financing (United States Congress, 2001).

In 2002, the Homeland Security Act initialized the establishment of the Department of Homeland Security (DHS): an umbrella organization with an annual budget of over $50 billion that oversees all domestic intelligence and law enforcement agencies (United States Congress, 2002) (DHS, 2010). This dramatically changed the way existing agencies such as the Federal Bureau of Investigation (FBI), and the newly founded Immigrations and Customs Enforcement (ICE) could access and utilize government resources and work together on issues of national security. Alongside a major transformation of federal and state law enforcement legislation, the Homeland Security act imposed numerous changes to the financial sector: regulating financial institutions to better detect and prevent terrorist financing.

Statement of Problem

When agencies within DHS were given additional funding and authority to stay ahead of the evolving threat of terrorism and be able to enforce the new, stricter regulations concerning terrorist financing; most financial institutions also increased employment and knowledge in areas such as financial security, fraud examination and anti-money laundering to secure their assets

and comply with the new laws; resulting in a private financial sector better suited to avoid being exploited by terrorist organizations for financing their operations. But while federal agencies across the DHS are successfully utilizing private businesses and organizations in areas such as immigration and border protection to amplify their effectiveness in protecting the nation from terrorism; they are not yet using the private financial sector to its full potential.

Purpose

The purpose of this paper is to gain a better understanding of the role financial institutions play in the war on terror, and to expose areas in which they can better be used to support the current duties of law enforcement agencies and investigative bureaus of the DHS. The intention of such utilization of the private financial sector is to increase the department's efficiency in use of resources; while maintaining or improving overall effectiveness in detecting, preventing, and eliminating terrorist financing in the United States.

In this paper, I will illustrate the current effectiveness of the ICE cooperative initiative called Cornerstone, and argue that it could be further improved through a deeper integration with the private sector. Also, so called Trade Transparency Units (TTUs) could become a better tool in the fight against international sources of terrorist financing if they were included as legally mandated parts of the operating strategies of all private banks in the United States.

Method

This paper consists of a literature review including official documents such as government reports and strategic proposals used to reveal areas in which the private financial sector could be better engaged in combating terrorist financing. Regulatory and legislative publications provide a framework for a feasibility analysis of privatizing a law enforcement agency such as DHS. Finally, investigations by media and independent organizations that encompass the privati-

zation of other governmental functions are included to reveal whether or not such functions have succeeded in the past.

Definitions

Terrorist financing. According to studies conducted by the United States General Accounting Office (2003), terrorist networks, such as al Qaeda, are to some extent similar to traditional criminal organizations in how they receive financing. By selling smuggled goods, counterfeit merchandize, illegal drugs and weapons, or through human trafficking, terrorist organizations commonly generate large amounts of cash. Since individuals and organizations related to any form of terrorism or to nations in support of terrorism - as classified by the Treasury's Office of Foreign Assets Control (OFAC) - are restricted or blocked from using financial institutions in this country, terrorist networks must find ways to circumnavigate a myriad of controls and regulations in order to send and receive their cash (FinCEN, 2004).

A common way this is accomplished is through so-called money laundering, which occurs when criminal organizations attempt to disguise the origin of funds generated from illegal activities, to appear as revenue from legitimate trade. By introducing such funds to publicly available financial institutions in which they are then invested in, or by other means distributed to, legal third parties, terrorists are able to conclude the "laundering" process of the funds (FATF-GAFI, 2010).

However, the methods of money laundering alone are no longer sufficient to describe how today's terrorist organizations receive their funding. Traditionally, the term anti-money laundering was consistently used in legislation controlling law enforcement divisions or task forces assigned to disrupt the financing of terrorist organizations. But in the post 9/11 war on terrorism, evolving financial methods used by terrorists and terrorist supporters have led to the need

for the United States Congress to establish the term terrorist financing as a unique form of financial crime not necessarily related to the use of illegal money (Weiss, 2005). According to CIA intelligence in the 9/11 Commission Report, the attacks in 2001, for example, were almost entirely funded through donations and fund-raising from supporting mosques and other organizations throughout the Middle East. Islam is known for heavily encouraging charity and gifts, a practice referred to as *zakat* (The National Commission on Terrorist Attacks Upon the United States, 2004). Terrorist organizations get help from these legitimate charitable organizations or from businesses operating in ill-regulated foreign markets to funnel funds in and out of the United States.

Financial institutions. For all purposes of this paper, the term financial institution encompasses any business entity that: provides financial services; fall under the authority of the U.S. Department of the Treasury; and may be exploited for terrorist financing (U.S. Department of the Treasury, 2008). Such entity includes: banks, credit unions, and other depository institutions; industrial loan companies, mortgage companies, thrift institutions, casinos, brokerage firms, insurance companies, securities dealerships; and any money services businesses (MSBs) such as Western Union (FinCEN, 2010).

Literature Review

Current Areas of Privatization

The Department of Homeland Security (DHS) coordinates and utilizes a broad variety of resources from federal, state, and local agencies to achieve its mission to ensure the security of the United States. The department operates within four distinct areas of national security: "the protection from dangerous people, dangerous goods, securing critical infrastructure, and the preparedness and response to national emergencies" (DHS, 2009). Since its initiation in 2003, the agencies of the DHS have created multiple partnerships with private businesses and organizations; and several of its functions have been partially of fully outsourced to the private sector.

The McCormick Tribune Foundation (2006) has found that reasons for privatizing a government function most commonly stem from the need for: unique, hard to come by intelligence; "surge capacity" and fast deployment of human and financial resources; expertise in highly detailed or advanced subject matter; or cost savings and efficiency in use of resources. The federal government often needs to maintain a more diverse and less specialized knowledgebase compared to the private sector, in order to adequately address all of their responsibilities. With a larger, more bureaucratic organizational structure than corporations, government agencies may also lack the ability to quickly tackle a unique threat or urgent situation on their own. Following are examples of areas in which the DHS has used the help of private businesses and organizations, with both positive and negative outcomes.

Border protection and immigration. The ever-evolving war on terror brings an endless need for new and advanced technology and expertise in highly specialized areas – border protection and immigration being one of them. To stay ahead of the criminal organizations, government agencies often rely on private industry leaders to provide innovative solutions. The Trans-

portation Security Administration (TSA) and United States Immigration and Customs Service (USCIS) frequently use private contractors on large projects (TSA, 2010).

In 2004, management and technology consulting company Accenture was awarded a $10 billion contract to help develop and implement the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program at major ports of entry throughout the country (Accenture Newsroom, 2004). The program involves gathering and sharing information on aliens arriving and departing from the United States, such as fingerprints and digital photos.

Similarly, in 2010, Perot Systems – a subsidiary of Dell - won a $120 million contract to process citizenship and immigration applications at over 60 USCIS field offices (BusinessWire, 2010). Among many other functions, the Virginia-based company will help USCIS simplify the application process as well maintain and facilitate FBI fingerprint and name checks.

An example of an unsuccessful attempt by a private company to undertake border protection functions of the DHS is the failed deal with foreign Dubai Ports World (DP World). In late 2005, the state-owned firm acquired the British Peninsular and Oriental Steam Navigation Company (P&O), which held leases to operate six major ports in the U.S., from New York to Miami, as well as several other smaller ports. It is common that foreign companies own and run operations, such as loading and unloading, in ports across the country; but this particular case started a fierce debate in both media and Congress due to the Arab ownership of the firm, and what possible security threats that could bring (Washington Post, 2006). Due to the controversy, DP World decided to withdraw from the negotiations in March of 2006, and voluntarily transfer their leases to an American firm (Sanger, 2006).

Critical infrastructure. Over 90 percent of the security of critical infrastructure in the United States is under the control of the private sector (McCormick Tribune Foundation, 2006).

Several military assets throughout the country, like Fort Bragg, NC are guarded by private security firms. For example, the Chicago Skyway Bridge was privatized in 2007 after a $1.8 billion deal with Cintra-Macquarie, a private consortium (Southern Illinoisan, 2004). The Skyway is a 7.8 mile toll road that connects the Indian Toll Way with an expressway leading into downtown Chicago, serving over 17 million drivers per year.

However, due to factors such as the economic climate, complications sometimes arise when private investors attempt to undertake large government contracts. In 2009, the city of Chicago gave a private consortium, Midway Investment and Development Company (MIDCo) the rights to privatize the Midway Airport; making it the first major passenger airport in the United States under private contract. However, in the wake of the economic recession, the firm could not come up with the $2.5 billion up-front payment, so the contract was put on ice. As of February of 2010, the city is still looking for ways to pursue a successful privatization in the near future (Merrion, 2010). The Federal Aviation Administration (FAA) initiated a pilot program in 1997 to find ways to privatize airport hubs, with the intent to develop and improve existing facilities and procedures (FAA, 2010). While the program has reviewed and approved applications from non-major airport hubs in New Orleans and Puerto Rico, for example; the Midway Airport in Chicago is so far the only major airport hub approved by the administration (Sechler, 2009) (Eggler, 2009).

Private security and law enforcement. In the post- Cold War era, the United States Armed Forces have relied heavily on private military contractors (PMCs) for support and manpower in their operations. For example, during the second quarter of 2009 there were over 17,000 contractors providing security in the war zones of Iraq and Afghanistan, according to the Department of Defense (DoD) (United States Government Accountability Office, 2009). But not

only in conflicts abroad does the U.S. government utilize the support of private security; within the nations' borders, agencies throughout the DHS are a engaging in partnerships and collaborations with security firms from the private sector.

In law enforcement, the most common way public authorities work together with private security is through so-called crime prevention partnerships (Bureau of Justice Assistance, 2005). In many metropolitan areas, local police agencies are stretched thin due to the increase in workload from facing the new challenges of terrorist threats. Further, the manpower and expertise needed to sort and monitor the exchange of information in today's high-tech society in order to detect or prevent crimes and terrorism is far beyond what most public authorities can mobilize on their own.

In New York City, NY, for example, the Area Police/Private Security Liaison (APPL) connects the New York Police Department (NYPD) with over 1000 private security firms through various outreach programs, lectures, and security surveys; to raise awareness of security issues and increase the city's readiness for another attack like 9/11. By working together to improve daily security functions such as visitor identification processes, scanning of arriving packages and vehicles, and building evacuation plans; the private firms can ensure a higher level of security at the businesses or locations they operate, while the NYPD can take advantage of the exchange of valuable information. For example, qualitative leads on suspicious activity or developing trends of criminal organizations can surface faster when the police have direct access to intelligence gathered by liaison members, allowing the police to use its limited resources more efficiently (Gunter & Kidwell, 2004).

A form of private security that has come under sharp scrutiny due to recent reports on lacking anti-terrorist safety procedures and questionable management is private security firms

protecting the nation's more than one hundred nuclear power plants (Holt & Andrews, 2009). Terrorist threats against nuclear plants have long been known by both the government and the industry. In fact, the 9/11 Commission Report concluded that nuclear plants were among the original targets for the 2001 attacks (The National Commission on Terrorist Attacks Upon the United States, 2004).

9/11 did bring about security enhancements of more than $1.2 billion across the industry, including a general increase in staffing and, in some cases, training of security personnel, but many sources point out just how vulnerable the plants still are (Faddis, 2010) (GAO, 2006). Compared to private security forces in Iraq and Afghanistan, the firms patrolling our nuclear plants do not have the same opportunities to train in real, high-stress combat situations. GAO (2006) points out that even though attempts have been made to increase the realism and scope of training scenarios, nuclear security firms still lack concrete plans for many of the possible scenarios in which terrorist could attempt to destroy or infiltrate the power plants, also known as Design Basis Threats (DBTs) (Holt et al, 2009). For example, the firm that provides security to almost half of all plants in the country, Wackenhut Corp., was criticized for lacking procedures during so called force-on-force exercises in which security firms defend the plants against a simulated enemy (Service Employees International Union, 2009). The firm used its own guards to act as adversaries, which made authorities question how realistic the exercises actually were.

Emergency preparedness. After Hurricane Katrina, the Federal Emergency Management Agency (FEMA) was widely criticized for shortcomings in dealing with the catastrophic scenarios in New Orleans (FEMA, 2009). In the Congressional hearings that followed the disaster, private industry leaders were questioned on how they had responded to the disaster, and how efficiently FEMA had collaborated with them and used their help (Committee on Homeland Se-

curity and Governmental Affairs, 2007). It became apparent that the emergency preparedness of individual businesses, and their involvement in providing disaster aid to the public was, in many cases, quite exceptional - and a deciding factor in limiting the casualties of the hurricane.

By using existing infrastructure and technology, private businesses such as Wal-Mart and IBM were able to help the public in ways that FEMA alone was not. For example, IBM deployed their Crisis Response Team to help re-establish internet communications and develop missing-person registries together with the Red Cross. They also worked with the Center for Decease Control (CDC) to create fast access to critical hospital records for the field hospitals treating hurricane victims. Wal-Mart, who had 171 facilities affected by the hurricane, utilized their efficient and reliable supply chain systems of trucks and warehouses to keep their operations running, providing customers with goods necessary for survival.

While FEMA was able to establish some collaboration with private suppliers and contractors during Katrina, they were not adequately taking advantage of all what the private sector could offer. As a way to better include private industries in future natural disasters and national emergencies, FEMA established the Private Sector Division in 2007 (FEMA, 2010). The division works to create better emergency response plans for both businesses and public agencies, and seeks to establish direct lines of communication between the parties.

In Washington state, for example, the Washington State Emergency Management Division (EMD) has established a Corporate Relations Program to improve the state's readiness for major incidents, such as the flood in late 2007 (FEMA, 2009). Among the objectives of the program was to establish reliable two-way communications between government agencies and local businesses. Also, the program has established a partnership with the Washington Business Association and assigned some of their employees to serve as members of the state's Emergency Op-

erations Center (EOC).

Homeland Security and the Financial Sector

Since financial support is essential for all criminal organizations and terror networks to maintain operable, the financial sector plays a large role in terms of ensuring national security. Even though the United States has a highly sophisticated financial system compared to many other countries, there are still ways that terrorists can funnel money to their allies across the nation's borders, or fund networks through transactions disguised as legitimate trade.

In its efforts directly following the attacks of 9/11, newly founded DHS together with the Treasury were mainly concerned with freezing the assets of known terrorist financiers. As of 2004, over $1.5 billion in terrorist assets were frozen or blocked as a result of such operations (Weiss, 2005). However, with the 9/11 Commission Report it became clear that the agency's resources should instead be focused on locating the sources of the assets, and using such leads to find the core of the terrorist organizations (The National Commission on Terrorist Attacks Upon the United States, 2004).

Today, tracking down established terrorist organizations or exposing emerging new cells by tracing and intercepting financial transactions is an essential part of the goal of DHS: to ensure the security of the nation. The Department of Homeland Security encompasses several agencies that investigate terrorist financing. The two major entities are the Federal Bureau of Investigation (FBI) and the U.S. Immigration and Custom Enforcement (ICE).

FBI. Since 2003, The Federal Bureau of Investigation (FBI) has been the lead investigative agency on terrorist financing within the United States (Weiss, 2005). Historically, the bureau has had extensive experience in conducting investigations on white-collar crimes such as fraud and embezzlement, and today they utilize their connections within the private sector to investi-

gate suspicious activity that may expose financing of terrorist networks. Through their Terrorism Financing Operations Section (TFOS), FBI tracks organizations and institutions known for providing financial support to terrorist organizations, and use financial information to expose new or unknown terrorist networks (FBI, 2010).

ICE. The U.S. Immigration and Custom Enforcement (ICE) is the largest investigative agency in the DHS (ICE, 2009). Through their Office of Investigations (OI), ICE monitors immigration, transnational trade and financial transactions to detect and deter criminal organizations from illegally bringing money, goods and manpower across the border to support terrorist networks. With an annual budget of over 1 billion dollars (Weiss, 2005) the agency has the resources necessary to investigate over 20,000 cases each year, and has access to a vast amount of information on organizations and individuals involved in financial crime (Dellicolli, 2006).

Current Legislation and Preventative Measures

There are several legal acts and law enforcement initiatives in place to enable the early detection, investigation, and proper prosecution of financial crimes such as terrorist financing. These do not only help investigative authorities in breaking down criminal networks, but also enable financial institutions to maintain their integrity and keep losses related to fraud, for example, at a minimum.

USA Patriot Act. Enacted by Congress in the aftermath of 9/11, the USA PATRIOT ACT of 2001 introduced new ways law enforcement agencies and other regulatory authorities are allowed to access and share information to better avoid such attacks in the future. Financial institutions are especially affected by Section 314(a) of the act, which allows for better detection and prevention of terrorist financing through extended cooperation and information sharing between financial institutions and law enforcement (United States Congress (2001). Through the

Financial Crimes Enforcement Network (FinCEN), which is a bureau within the Department of the Treasury in charge of collecting and analyzing data from financial institutions (Weiss, 2005), investigating authorities can access the records of over 22,000 financial institutions in search for suspicious transactions and other traces of terrorist financing. FinCEN forwards the detailed requests to banks, MSBs, and depository institutions via a secure website, who then have two weeks to search through their records for the information requested (FinCEN, 2010).

According to FinCEN's most recent feedback survey for involved law enforcement agencies, the program has been successful in providing useful information such as the identification of accounts and transactions for criminal investigations. Since the start of the program in November of 2002, investigating authorities have sent out 333 requests regarding terrorist financing; out of an average of 54% have lead to indictments and/or arrests (FinCEN, 2010).

Bank Secrecy Act and currency transaction reports. The Bank Secrecy Act (BSA) imposes requirements on how financial institutions are to cooperate with law enforcement agencies, such as ICE and the FBI, to prevent terrorist financing (FinCEN, 2010). Originally enacted in 1970 by Congress, the act has been continuously amended to meet the ever-changing nature of financial crimes; one recent example being title III of the USA PATRIOT ACT. Among several anti-money laundering regulations, the BSA dictates that all financial institutions must keep records of deposits, withdrawals and other transfers of cash exceeding $10,000 per day and party. All such transactions must be reported through Currency Transaction Reports (CTRs).

CTRs require bank personnel to record more extensive information than what is otherwise requested from the parties involved in transactions; such as personal information and photocopies of identification and authorized signatures. This is a way for financial institutions to assist law enforcement agencies in creating a national database of organizations and individuals

frequently involved in larger volume cash transaction. Similar to the majority of criminal organizations, terrorist networks operate with large amounts of cash and other hard-to-trace negotiable instruments. By raising red flags when suspicious behavior occur, such as when businesses whose operations are not normally associated with large transactions of cash suddenly start receiving large deposits, the CTRs help law enforcement initiate investigations to separate legitimate trade from organizations possibly involved in funding criminal activity (Dellicolli, 2006). Another benefit of the CTRs is that they can help law enforcement isolate parties that frequently and deliberately keep their transactions below the CTR filing requirement – a common indicator that they have intent to hide or disguise the origin of their funds. For these reasons, ICE frequently uses CTRs in their investigations, and in the year 2005 alone, they accessed the CTR records over 450,000 times (Dellicolli, 2006).

Suspicious activity reports and blocking reports. Since 1996, all financial institutions are expected to file Suspicious Activity Reports (SARs) to FinCEN when they suspect that criminal activity is taking place at their institution (IRS, 2010). These activities can include money laundering, forgery, identity theft, various forms of fraud. Transactions reportable on SARs are subject to two different filing thresholds; face-to-face transactions at MSBs in excess of $2,000; and transactions at other financial institutions of over $5,000. Commonly, SARs are also filed when a party is making conscious attempts to avoid filing a CTR by keeping transactions below the $10,000 threshold, as previously discussed.

While all financial institutions such as banks and Money Services Businesses (MSBs) are required by law to file SARs, all other businesses that cash checks are encouraged to do so as well. By examining reports from local MSBs, law enforcement agencies, such as divisional FBI offices, can detect criminal activity and make out patterns to track individuals and organizations

that commit these crimes. Between 1999 and 2004, FinCEN compiled information from SARs into the SAR Bulletin that was issued to financial institutions and law enforcement agencies on an annual basis. The bulletin contained summaries of actual cases – either solved or under investigation - highlighting various criminal activities deemed important by FinCEN due to their frequent occurrences in SARs, or due to the large dollar amounts involved (FinCEN, 2004). While the bulletin no longer exists, FinCEN continues to inform the private financial sector on issues regarding terrorist financing through various press releases; most recently in the form of an advisory issued in March of 2010. (FinCEN, 2010).

Similar to SARs, blocking reports are filed for transactions involving accounts or individuals from countries, such as North Korea or Cuba, that have been issued sanctions or embargoes by the Treasury's Office of Foreign Assets Control (OFAC) - also referred to as "Specially Designated Nationals" (SDNs)) (FinCEN, 2004). So-called blocked transactions also involve organizations or business entities that have been deemed associated with terrorism and terrorist financing. Financial institutions scan for SDNs when conducting wire transfers, for example, and report any hits to the OFAC telephone hotline (US Treasury, 2010).

Cornerstone. Cornerstone is the name of partnerships created between ICE, local law enforcement agencies, and private financial institutions that work to prevent crime and detect criminal activity on a local scale (ICE, 2009). Through a constant exchange of information between the parties, law enforcement agencies can receive early red flags and warning signs of financial crime from banks, and initiate raids and arrests with the help of ICE. Cornerstone partnerships utilize all tools that financial institutions have to work with in detecting and reporting suspicions of terrorist financing, including the previously discussed SARs, CTRs, and blocking reports. By collecting data from such reports from the FinCEN databases, ICE agents create case

studies and action plans for financial institutions to study and incorporate in their staff training.

Special Agents conduct presentation at private businesses and at government offices to promote awareness of the program, and to encourage individuals to discuss current cases and suspicions of terrorist financing. According to Dellicolli (2006), ICE agents have "given over 2,000 presentations to over 40,000 business leaders, government officials and law enforcement officers, worldwide", leading to more than 200 investigations. The results and developments of Cornerstone partnerships are also presented to financial institutions and local law enforcement agencies through periodic publications called Cornerstone Reports (DHS, 2009). With the help of Cornerstone, ICE seized nearly $300 million in currency and monetary instruments, and made 1,800 arrests for financial crimes in only one year (ICE, 2004).

Trade transparency units. Similar to Cornerstone partnerships but on an international level, Trade Transparency Units (TTUs) are partnerships established between ICE and financial institutions in other countries. The purpose of the TTUs is to increase the security and integrity of international trade by working together with authorities in other countries to investigate discrepancies in trade records and improve upon vulnerabilities in their current trade practices (U.S. Department of State, 2005). For example, a common way for criminal organizations to disguise moving money into the country is by undervaluing shipments of goods or commodities. When the receiving end of the shipment turns around and sells the goods in the United States for a premium, their profit is used to finance the organization. Using their proprietary Data Analysis and Research for Trade Transparency System (DARTTS), ICE agents can detect and prevent such illegal practices by inspecting shipping slips in the forwarding country, for example (Dellicolli, 2006).

While used for detecting all forms of illegal trade: from drugs to human trafficking;

TTUs also give ICE the ability and authority to access bank records and client lists, for example, in foreign banks when investigating the trails and origins of suspected terrorist financing. Together with the U.S. Customs and Border Protection's efforts to apprehend bulk cash smuggled across the nation's borders; TTUs are the nation's primary tool in the defense against funds being smuggled into the country to support terrorist networks.

Since 2004, the TTUs have started over 200 investigations and seized over $30 million (DHS, 2009). The first TTU was established in Columbia, as an effort to fight the many forms of financial crimes that occur between the two nations, such as drug trafficking and contraband smuggling. A product of the new partnership was the Black Market Peso Exchange (BMPE) initiative, which is a tool for authorities in both countries to monitor and track down individuals involved in the illegal trade of the peso currency (Dellicolli, 2006).

Aside from Columbia, countries that currently cooperate with ICE through TTUs are Paraguay, Argentina, Panama, India and the Philippines. ICE is also promoting the idea to initiate partnerships in Eastern and Central European countries, with the future plans of making all international trade documents and data open (U.S. Department of State, 2005).

Recommendations

Through the research conducted for this paper, I have been able to discern two areas of the DHS in which a deeper integration with the private financial industry may have positive effects:

Expansion of Cornerstone Partnerships

Currently, most financial institutions, such as retail banks, only demand that their employees take part of SARs sent out in emails from their divisional FBI agency. However, the SARs mainly discuss individual criminal activities such as fraudulent checks and robberies; they rarely involve more complex financial crimes, and do not present leads or signs of terrorist financing. Making it a legal requirement for all financial institutions to establish mandatory Cornerstone partnerships with their local law enforcement agency, could force management of such institutions to introduce recurring meetings with ICE officers and schedule frequent educational seminars to keep all staff up to date on the recent developments, as presented by the ICE agents. Also, mandated partnerships would help ensure that employees of all levels of the financial institutions take part of the Cornerstone reports created by ICE. Compared to case-by-case based SARs, the Cornerstone has a more systemic way to approach suspicious incidents taking place at the institutions, and helps employees establish connections between otherwise seemingly unique, individual occurrences of criminal activity. By making employees take part of such reports on a recurring basis, together with meetings and seminars by ICE agents; could help raise a higher awareness of current suspicions of terrorist financing; and in turn possibly increase the number of red flags reported back to the authorities by personnel at such institutions.

A possible obstacle for making Cornerstone partnerships mandatory may be that managers of financial institutions feel that the partnerships intrude on their way of conducting their

business, and may discourage them from creatively and enthusiastically engaging in the cooperation. However, increased security in technical systems as well as daily operations lay in the interest of most banks and financial institutions, as customers demand a safe and trustworthy environment to keep their savings and investments. In that sense, the Cornerstone initiative is an easy step for managers to show that they are interested in securing the integrity of their institution.

ICE can mitigate some of their increased costs associated with establishing more Cornerstones partnerships by using intelligence exchanged with financial institutions to become more efficient in finding leads and performing investigations on terrorist financing.

Mandatory TTUs

While all banks that operate in the United States must cooperate with authorities to allow transparency in record keeping and financial transactions, as discussed in the Bank Secrecy Act, for example, TTU partnerships ensure federal agents similar transparency in other countries. However, the number TTU currently in place is not nearly sufficient to allow agencies such as ICE to conduct the investigations needed to trace and prosecute all leads on terrorist financing. As it is the expressed intent by ICE to expand on the number of TTUs, one way this could be accomplished is by incorporating into the regulatory system a demand for TTUs in all countries in which U.S. based financial institutions have branches or subsidiaries..

By forcing banks to lobby for TTU partnerships between the United States and the nations of their foreign entities, the possibility for agencies such ICE to investigate suspicious international cross-border transactions would be greatly improved, and criminal organizations and terrorist networks would be further deterred from funneling monetary funds through American banks. Also, by making banks liable for establishing such relationships with the countries of their foreign branches, costs related to maintaining a safe and secure financial environment becomes

more internalized by the private sector; possibly ensuring an even higher level of responsibility from their part. With the US financial market being one of the most influential in the world, it would perhaps also encourage other nations to introduce similar legislation in their own financial markets.

Although a legislative initiative such as this would most likely be a lengthy and complicated process, and may not generate results quickly; an increase in TTUs abroad, or equivalent partnerships between nations, would greatly simplify future investigations of terrorist financing. Also, TTUs improve the accuracy and quality of all forms of trade, and may save all incorporated parties both money and time by limiting their loss of business to illegal trade.

Conclusion

In this paper, I have presented research on the main areas of terrorist financing, what it means and how it can be prevented. I have presented the aspects of the Department of Homeland Security that are involved in combating such financing, and I have demonstrated ways the private financial sector can do their part by detecting and reporting suspicious activity.

I have shown that by combining the most efficient tools federal agencies have to deter or eliminate terrorist organizations from receiving funding for their criminal activities, with the intelligence and experience financial institutions possess; the Department of Homeland Security can become even more effective in securing the nation from terrorism.

References

Accenture Newsroom. (2004). U.S. Department of Homeland Security awards Accenture-led smart border alliance the contract to develop and implement US-VISIT program. Retrieved from http://newsroom.accenture.com/article_display.cfm?article_id=4112

Bureau of Justice Assistance (2005). Engaging the private sector to promote homeland security: Law enforcement-private security partnerships. Retrieved from www.ncjrs.gov/-pdffiles1/bja/210678.pdf

BusinessWire (2010). Dell to provide business process outsourcing services to help USCIS enhance more than 60 field office operations. Retrieved from http://www.forbes.com/feeds/businesswire/2010/04/14/businesswire138877758_print.html

Dellicolli, Kevin (2006). Statement before the Senate Committee on banking, housing and urban affairs. Retrieved from http://banking.senate.gov/public/index.cfm?FuseAction=Files.-View&FileStore_id=2a41f350-b1fc-405d-93ed-2f3dca23cc02

Department of Homeland Security [DHS] (2009). DHS annual performance report for fiscal years 2008 – 2010. Retrieved from www.dhs.gov/xlibrary/-assets/cfo_apr_fy2008.pdf

DHS (2009). Testimony of deputy assistant secretary Mark Koumans. Retrieved from http://www.dhs.gov/ynews/testimony/testimony_1237218661657.shtm

DHS (2010). Budget-in-Brief, Fiscal Year 2010. Retrieved from http://www.dhs.gov/-xlibrary/assets/budget_bib_fy2010.pdf

DHS (2010). Department components and agencies. Retrieved from http://www.dhs.gov/-xabout/structure/

Eggler, B. (2009). Louis Armstrong International Airport to seek privatization bids. Retrieved from http://blog.nola.com/politics/print.html?entry=./2009/ 09louis_armstrong_-

international.html

FAA (2010). Airport privatization pilot program. Retrieved from http://www.faa.gov/-airports/airport_compliance/privatization/

Faddis, C. (2010). Nuclear plants need real security. Retrieved from http://www.cnn.com/-2010/OPINION/03/15/faddis.nuclear.plant.security/index.html

FATF-GAFI (2003). 40 recommendations. Retrieved from http://www.fatf-gafi.org/document/-28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html

FATF-GAFI (2004). 9 special recommendations on terrorist financing. Retrieved from http://www.fatf-gafi.org/document/9/0,3343,en_32250379_32236920_34032073-_1_1_1_1,00.html

FATF-GAFI (2009). Money laundering and terrorist financing in the securities sector. Retrieved from http://www.fatf-gafi.org/dataoecd/32/31/43948586.pdf

FATF-GAFI (2010). Money laundering FAQ. Retrieved from http://www.fatf-gafi.org/-document/29/0,3343,en_32250379_32235720_33659613_1_1_1_1,00.html

Federal Deposit Insurance Corporation [FDIC] (1996). Part 353 – Suspicious activity reports. Retrieved from http://www.fdic.gov/regulations/laws/rules/2000-7500.html

FDIC (2002). Anti-money laundering measures. Retrieved from http://www.fdic.gov/-news/news/financial/2002/fil0259.html

FEMA (2009). About FEMA. Retrieved from http://www.fema.gov/about/

FEMA (2009). Washington State teams with business. Retrieved from http://www.fema.gov/-privatesector/wash_state.shtm

FEMA (2010). About FEMA Private Sector Division. Retrieved from http://www.fema.gov/-privatesector/about.shtm

Financial Crimes Enforcement Network [FinCEN] (2004). Interpretation of suspicious activity reporting requirements to permit the unitary filing of suspicious activity and blocking reports. Retrieved from http://www.fincen.gov/news_room/nr/pdf/20041214a.pdf

FinCEN (2004). SAR bulletin. Retrieved from http://www.fincen.gov/news_room/-rp/rulings/pdf/sarbul0201-f.pdf

FinCEN (2005). Fact Sheet: Section 312 of the USA PATRIOT Act final regulation and notice of proposed rulemaking. Retrieved from http://www.fincen.gov/news_room/-rp/rulings/html/312factsheet.html

FinCEN (2009). Advisory. Retrieved from http://www.fincen.gov/statues_regs/-guidance/html/fin-2009-a007.html

FinCEN (2010). 314(a) fact sheet. Retrieved from http://www.fincen.gov/314afactsheet.pdf

FinCEN (2010). Advisory. Retrieved from http://www.fincen.gov/statutes_regs/-guidance/pdf/fin-2010-a002.pdf

FinCEN (2010). Am I an MSB? Retrieved from http://www.fincen.gov/financial_institutions/-msb/amimsb.html

FinCEN (2010). Bank Secrecy Act. Retrieved from http://www.fincen.gov/statutes_regs/-bsa/index.html

Gunter, W., & Kidwell, J. (2004). Law enforcement and private security liaison: Partnerships for cooperation. Retrieved from http://www.ifpo.org/articlebank/lawprivateliaison.html

Holt, M, & Andrews, A. (2009). Nuclear power plant security and vulnerabilities. Retrieved from http://www.fas.org/sgp/crs/homesec/RL34331.pdf

Homeland Security and Governmental Affairs (2007). Hurricane Katrina: What can the government learn from the private sector's response? *Hearing before the Committee on Homel-*

and Security and Governmental Affairs, United States Senate. Washington, DC. U.S. Government Printing Office. Retrieved from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_senate_hearings&docid=f:24932.pdf

Internal Revenue Service [IRS]. (2010). Suspicious activity reports. Retrieved from http://www.irs.gov/businesses/small/article/0,,id=154555,00.html

McCormick Tribune Foundation (2006). Understanding the privatization of national security. Retrieved from http://www.mccormickfoundation.org/publications/privatization2006.pdf

Merrion, P. (2010). Midway airport privatization in holding pattern. Retrieved from http://www.-chicagobusiness.com/cgi-bin/printStory.pl?news_id=36929

National Commission on Terrorist Attacks Upon the United States (2004). Complete 9/11 commission report. Retrieved from http://govinfo.library.unt.edu/911/report/index.htm

Sanger. D. (2006). Under pressure, Dubai company drops port deal. Retrieved from http://www.-nytimes.com/2006/03/10/politics/10ports.html

Sechler, B. (2009). FAA accepts Luis Munoz Marin Airport in privatization program. Retrieved from http://www.nasdaq.com/

Service Employees International Union (2009). Wackenhut's nuclear security contract questioned by members of congress, GAO. Retrieved from http://www.securityinfowatch.com/-printer/1275772

Southern Illinoisan (2004). Chicago privatizes skyway toll road in $1.8 billion deal. Retrieved from http://infoweb.newsbank.com

TSA (2010). Business Opportunities. Retrieved from http://www.tsa.gov/join/business

U.S. Government Accountability Office [U.S. GAO] (2003). Report GAO-04-163: Terrorist financing. Retrieved from http://www.gao.gov/new.items/d04501t.pdf

U.S. GAO (2006). Report GAO-06-388: Nuclear power plants. Retrieved from http://www.-gao.gov/new.items/d06388.pdf

U.S. GAO (2009). Report GAO-09-883: Combating terrorism. Retrieved from http://www.-gao.gov/new.items/d09883.pdf

U.S. GAO (2009). Report GAO-10-1: Contingency contradicting. Retrieved from http://www.-gao.gov/new.items/d101.pdf

U.S. Immigration and Customs Enforcement [ICE] (2004). 9/11 commission report: Terrorist financing issues. Retrieved from www.ice.gov/doclib/pi/news/.../092404-GarciaSentBank.pdf

U.S. Immigration and Customs Enforcement [ICE] (2009). The cornerstone report. Retrieved from http://www.ice.gov/pi/cornerstone/reports/csreport_111_page4.htm

U.S. Immigration and Customs Enforcement [ICE] (2009). Topics of interest – trade-based money laundering. Retrieved from http://www.ice.gov/partners/financial/topics.htm

U.S. Congress (2001). H.R. 3162 – USA PATRIOT ACT. Retrieved from http://epic.org/-privacy/terrorism/hr3162.pdf

U.S. Congress (2002). Homeland Security Act of 2002. Retrieved from http://www.dhs.gov/-xlibrary/assets/hr_5005_enr.pdf

U.S. Department of State (2005). Trade transparency units. Retrieved from http://www.state.-gov/p/inl/rls/nrcrpt/2005/vol2/html/42381.htm

U.S. Department of the Treasury (2002). SAR Bulletin. Retrieved from http://www.sec.gov/-about/offices/ocie/aml2007/sarbull0102.pdf

U.S. Department of the Treasury (2008). Duties & functions of the U.S. Department of the Treasury. Retrieved from http://www.treasury.gov/education/duties/

U.S. Department of the Treasury (2010). When should I call the OFAC hotline? Retrieved from http://www.ustreas.gov/offices/enforcement/ofac/faq/answer.shtml#24

UNODC (2010). UNODC on money-laundering and countering the financing of terrorism. Retrieved from http://www.unodc.org/unodc/en/money-laundering/index.html?-ref=menuside

Washington Post (2006). Security fears about infiltration by terrorists. Retrieved from http://www.washingtontimes.com/news/2006/feb/22/20060222-122115-8912r/print/

Weiss, A (2005). Terrorist financing: U.S. agency efforts and inter-agency coordination. Retrieved from http://www.fas.org/sgp/crs/terror/RL33020.pdf