The Homeland Security Review, Vol. 7, No. 2 (Summer 2013).

Information Sharing and Public-Private Partnerships: The Impact on Homeland Security

BY AUSTEN D. GIVENS* AND NATHAN E. BUSCH†

I. Introduction

Alhaji Umaru Mutallab walked into the U.S. Embassy in Abuja, Nigeria on November 19, 2009.[1] He was concerned about his son Umar Farouk Abdulmutallab's increasingly radical Islamic beliefs. Compounding Alhaji's worry, Umar had recently traveled to Yemen and abruptly cut off contact with his family, sending his father a text message that read, "I have found the true Islam. Don't try to contact me anymore."[2] Alhaji planned to go to Yemen to retrieve his son, but the Yemeni government would not grant Alhaji a visa.[3] Frustrated and out of options, Alhaji decided to warn the U.S. government about his son Umar, and to ask for the U.S. government's help in tracking Umar down.[4] While at the embassy, Alhaji met with the U.S. Central Intelligence Agency's (CIA) chief of station—the top CIA official in Nigeria—and expressed his concerns about his son.[5]

The next day at the embassy, U.S. State Department and CIA personnel met to discuss the information that Alhaji had provided to the CIA chief of station. These U.S. government employees then wrote a set of reports about Alhaji's information, which they disseminated within the U.S. Intelligence Community (IC).[6] Despite these concrete steps to document Alhaji Umaru Mutallab's concerns about his son, and

* Austen D. Givens is a PhD student in Public Policy at King's College London, and teaches courses on homeland security and cyber security at Utica College in New York. He can be reached at adgivens@utica.edu.

† Dr. Nathan E. Busch is an associate professor of government at Christopher Newport University (CNU) and co-director of the CNU Center for American Studies, where he is lead coordinator of CNU's annual Symposium on Homeland Security. He is author of *No End In Sight: The Continuing Menace of Nuclear Proliferation* (University of Kentucky Press, 2004), and editor of *Combating Weapons of Mass Destruction: The Future of International Nonproliferation Policy* (University of Georgia Press, 2009). He can be reached at nbusch@cnu.edu.

despite the possibility of Umar's links to Islamic extremists, Umar's name was not placed on a no-fly list or transportation watch list.

Just over a month later on Christmas Day 2009, Alhaji's son, Umar Farouk Abdulmutallab, boarded Northwest Airlines Flight 253 in Amsterdam, the Netherlands, bound for Detroit, Michigan. 289 people were on the plane. Umar carried his own passport, in his own name, which contained an official U.S. Visa—previously issued by the U.S. State Department in 2008.[7] He had paid for his ticket in cash, and he did not check any luggage.[8] Umar had passed through multiple layers of airport security in Amsterdam, all the while concealing a mixture of high explosives in his underwear. He planned to detonate the explosives on Flight 253 by using a syringe to inject a special liquid into them, which would set off a chemical reaction, triggering a violent explosion.[9] And as the plane approached Detroit, Umar injected the special liquid into the explosives inside his underwear. First there was a "pop" sound, like a firecracker.[10] But the explosives did not detonate properly. Instead, Umar's blanket, pants, and underwear caught fire.[11] A passenger on the flight leapt up to extinguish the flames, and then worked with crew members to restrain Umar so that the pilots could safely land the plane.[12]

Although in recent years there have been great advances in public-private sector information sharing for homeland security, the Underwear bomber plot demonstrates that the basic challenge of sharing information that is timely, accurate, and actionable persists. This article identifies and addresses several of the ongoing difficulties affiliated with information sharing between public and private sector partners and the subsequent impact of these difficulties on homeland security. As we will see, today public and private sector partners encounter challenges with inadequate trust between one another, difficulties in effectively filtering and processing a huge amount of incoming information, and problems with low quality of information. Public and private sector partners must deliberately seek to address these difficulties in order to bolster public-private sector information sharing.

The Underwear bomber plot occurred over eight years after the September 11th, 2001 terrorist attacks. Yet the parallels between the information sharing failures of 9/11 and the information sharing failures of the Underwear bomber plot are striking. The 9/11 Commission notes that in the lead-up to the 9/11 attacks, U.S. government agencies did not exchange bits of information in their possession, and these same bits of information, if properly integrated and analyzed, would have pointed toward an imminent terrorist attack upon the United States.[13] In advance of the Abdulmutallab bombing plot, multiple U.S. government agencies also had access to pieces of information which, when

aggregated and analyzed, should have led them to place Abdulmutallab on a no-fly list. Yet that did not happen. Moreover, like the 9/11 attacks, U.S. government officials did not effectively communicate with private sector commercial airlines about the potential threat that certain individuals posed, in the former case, nineteen would-be hijackers, and in the latter case, Abdulmutallab himself.

There is, however, a fundamental difference between the information sharing failures in the Abdulmutallab case and the information sharing failures of 9/11. Unlike in 2001, when effective information sharing was more limited, today government is awash in duplicative, overlapping information sharing programs, tools, and initiatives. To alleviate the information sharing problems that failed to prevent the 9/11 attacks the Information Sharing Environment (ISE) was created to streamline and facilitate information sharing across the federal government. The ISE program has achieved significant success. For example, the ISE Program Manager notes that many of the 70+ fusion centers nationwide are sharing local-level suspicious activity reports with other local, state, and federal agencies.[14] The U.S. Department of Homeland Security established its own office of Intelligence and Analysis, which took its place alongside the other 15 member agencies of the IC.[15] DHS now has plans to set up its own internal fusion center, with the goal of centralizing information from DHS' component agencies.[16] The National Counterterrorism Center (NCTC) was launched after 9/11 to centralize analysis of terrorism-related information from across the federal government.[17] Both public and private sector homeland security analysts are bombarded with information bulletins, alerts, memoranda, and reports each day. While on the surface it might appear that 9/11-era information sharing problems are solved, the Abdulmutallab case demonstrates that serious problems still exist.

In fact, in this article we argue that the efforts to correct the information sharing failures of 9/11 have not alleviated a trust deficit that exists between the public and private sector. Moreover, the changes following September 11th have also inadvertently created new information sharing problems, including information overload for homeland security analysts and a decline in information quality. The challenge for public-private partnerships in homeland security now is to build cross-sector trust, control the flow of information, and manage information quality for decision-makers in government and business.

The article proceeds in four parts. The first part explains why information sharing is necessary for homeland security in general. In the second part, we describe how a lack of trust, information overload, and low-quality information hinder information sharing within

government entities and between the public and private sectors. We then explain how public-private partnerships can help provide solutions to these difficulties by building trust between government and businesses, managing the information deluge, and improving information quality. The article concludes with a set of policy recommendations for government and businesses to address today's information sharing challenges.

II. Why Information Sharing Is Necessary For Homeland Security

Information sharing is important for homeland security because public sector decision-makers can use this data to make more well-informed, and ostensibly better, decisions. Information sharing is much more than just intelligence sharing. Schedules, bureaucratic processes and goals, individual agency and office plans, resource lists, and interpersonal communication all help policymakers to do their jobs more effectively. A lack of information exchange, or low-quality information exchange, can undermine national security by weakening precautions against conventional attack, terrorism, espionage, natural disasters, or other threats. For example, U.S. Immigration and Customs Enforcement needs to share information with U.S. Customs and Border Protection—both of which fall under the umbrella of the U.S. Department of Homeland Security—because their missions are complementary and they each deal with similar threats and challenges. The need for effective information sharing also transcends government departments. For instance, the Central Intelligence Agency (CIA) may need information on satellite orbits from the National Aeronautical and Space Administration (NASA) and National Geospatial Intelligence Agency (NGA). In this way federal agencies collaborate through information exchange, which ultimately helps to achieve homeland security objectives.

Beyond information sharing among federal agencies and departments, homeland security data routinely passes horizontally among businesses and government agencies, as well as vertically among the local, state, and federal levels of government. In New York City, the NYPD Shield program exemplifies public-private sector information as well as vertical information sharing. NYPD Shield enlists local business owners to be the "eyes and ears" of the NYPD in identifying potential terrorist threats. The program encourages business owners and employees to report suspicious activity to the NYPD because these private sector employees are familiar with what may be unusual or out of place in their facilities or neighborhoods.[18]

In exchange for their cooperation in the program, the NYPD gives business owners special access to NYPD intelligence or threat briefings,

business owners can confer with local NYPD precinct counterterrorism coordinators, and they receive alert email messages from the NYPD.[19] Since New York City is under constant threat of terrorist attacks, the NYPD maintains a close working relationship with state level agencies, including the New York State Police and New York State Division of Homeland Security and Emergency Services.[20] And both of these state-level agencies regularly communicate with federal law enforcement agencies like the Federal Bureau of Investigation (FBI). Thus it is entirely possible for a suspicious activity report from a Brooklyn police precinct to go through the NYPD, on to the state level of government, and then to the federal level of government. This type of vertical information sharing now occurs on a regular basis. But since 9/11, it is increasingly clear that vertical information sharing is not enough to achieve homeland security objectives. To protect the nation, government and businesses must exchange information with one another, too.

Government agencies and firms share information during disasters. Recent large-scale incidents in the United States illustrate the indispensable role of this public-private sector information sharing, for it facilitates effective disaster response coordination. As local, state, and federal agencies fanned out across New Orleans after Hurricane Katrina, Wal-Mart efficiently delivered tons of relief supplies to area residents.[21] But Wal-Mart also needed assistance in protecting its New Orleans area stores from looters. As a result, Wal-Mart negotiated with local law enforcement officials, and agreed to provide them with supplies in exchange for protection from looters.[22] In this case information sharing between Wal-Mart and law enforcement officials helped to provide needed goods for first responders, and also helped Wal-Mart to be more effective in distributing relief supplies to disaster survivors.

Home Depot quickly re-opened its Joplin, Missouri store in 2011 after a powerful tornado leveled most of the city. The store served as an important source of construction materials for emergency workers.[23] The Federal Emergency Management Agency (FEMA) and Home Depot shared information with one another about community post-disaster needs, and made arrangements to set up a FEMA information center inside the Joplin Home Depot store. The FEMA information center served to answer area residents' questions about rebuilding.[24] In this way, information exchange between FEMA and Home Depot met both public and private sector interests. FEMA provided information to area disaster survivors, helping to achieve its own organizational objectives. Home Depot benefited from locating the FEMA information center inside its store, because this co-location could draw more area residents to the store itself, potentially boosting sales. These examples

demonstrate that when firms and government agencies share information, it enhances disaster relief efforts. This improved coordination can help to save lives and property in disaster-affected areas.

To be sure, information sharing for homeland security is happening within government and between businesses and government. Many of the fundamental information sharing problems that preceded 9/11 have been reduced or eliminated.[25] But new problems of low trust between the public and private sector, information overload, and low-quality information demonstrate that much important work remains.

III. Current Challenges With Information Sharing For Homeland Security

A. Lack Of Trust Between The Public And Private Sectors

The 9/11 Commission notes that the single biggest impediment to information sharing is human or systemic resistance to information sharing.[26] One of the biggest reasons for this resistance is a lack of trust.[27] Poor information sharing can damage trust. Similarly, damaged trust impedes information sharing; it is a classic example of a vicious circle. Without trust, communication becomes limited. This limited communication can delay important decisions, because both sectors cannot be certain that their efforts will be unified; they risk acting against one another's interests rather than working toward common objectives. Human lives, property, and the environment are ultimately put at risk because of this lack of trust between sectors.

The federal government has taken several steps to address the trust deficits that hampered information sharing prior to the 9/11 attacks. The ISE, which we discussed earlier, was created to build trusting relationships among government and non-government partners.[28] In its 2008 *Information Sharing Strategy*, DHS recognizes that it must cultivate trusting relationships with government agencies at all levels, as well as the private sector.[29] Today scholars outside government have also proposed new methods to improve trust between agencies so as to facilitate information sharing.[30]

But concerns about trust persist between the public and private sectors—and for good reason. Government may be concerned about disclosure of classified information—whether accidental or deliberate—and share lower-quality information with businesses to ameliorate these concerns. Similarly, businesses may be concerned about their own proprietary information being disclosed in public.[31] Trade secrets could leak to the media. Competitors could steal a firm's secrets. Confidential data could be introduced in court for civil or criminal matters. Government agencies could even seize upon discrepancies in company data, using them as a pretext to enforce certain business regulations.

Given these concerns, the private sector may only share low-quality information with government, for doing so eliminates the chances of government disclosing trade secrets, competitors benefiting from leaked information, or firms having their own information used against them in civil or criminal litigation. Moreover, firms avoid being hauled into regulatory compliance hearings based upon information they provided to the government for homeland security purposes. While this reluctance to share information is understandable, it hampers homeland security efforts, because both the public and private sector are forced to operate with less than optimal amounts of data.

B. Information Overload

In light of the information sharing problems described above, the U.S. government has taken steps to boost homeland security information sharing. For example, DHS created the Homeland Security Data Network (HSDN) and Homeland Security Information Network (HSIN)—online portals for exchange of sensitive-but-unclassified and classified information alike.[32] SIPRNet, the Department of Defense's classified information sharing network, is now linked to HSDN, making classified defense information available to state-level fusion center analysts with security clearances.[33] Moreover, DHS produced Lessons Learned Information Sharing (llis.gov), an online repository for best practices in homeland security and emergency management.[34] The IC rolled out Intellipedia—a classified intelligence sharing tool with the look and feel of the online encyclopedia Wikipedia—as well as A-Space, a networking and information exchange website for intelligence analysts.[35] Other tools that pre-date 9/11, such as the FBI's Law Enforcement Online (LEO), are still used by practitioners in the field.[36] Moreover, conventional methods of information exchange—telephone calls, emails, and meetings—are now easier through advancements in smartphones and online video conferencing.

Yet these efforts to improve information sharing, while beneficial in theory, may have actually created new information sharing problems. One study from 2009 suggests that analysts are frustrated—and overwhelmed—by the amount of information sharing that's happening now. For example, one of the study's respondents points out that there is not a clear consensus on what information sharing actually *is*: "[Information sharing means] *every little bit of information about everything that has to do with day-to-day crises to doom-and-gloom…all day, everyday, without filter.*"[37] Other practitioners note that the information being shared is vague, of little value, and often flows in only one direction, i.e. toward the federal government.[38] Moreover, the ever-important feedback loop, in which the information receiver conveys to the information

sender how beneficial the information was, appears to be at best broken, at worst, non-existent.[39]

The Umar Farouk Abdulmutallab case highlights these ongoing problems of information overload in homeland security today. Multiple government entities—the CIA, U.S. State Department, and NCTC—had access to separate pieces of information about Abdulmutallab – a ticket paid for in cash, a warning to the CIA about links to Islamic extremists, and multiple reports entered into government databases.[40] Moreover, Northwest Airlines—a private sector entity—had basic information about Abdulmutallab's ticket purchase, lack of checked baggage, and passport number. With the benefit of hindsight, these data points should have stood out to homeland security analysts, and prompted several U.S. government agencies to take actions that would have prevented Abdulmutallab from boarding flight 253. So what went wrong?

The U.S. Senate Select Committee on Intelligence (SSCI) studied the failed Underwear bombing, and the SSCI's findings show that information overload had a detrimental effect on intelligence analysis, leading to analytical oversights. The SSCI identified 14 distinct points of human, technical, or systemic failure that permitted Abdulmutallab to board the flight and attempt to bring it down.[41] These data points are remarkable in that they echo many of the same types of intelligence failures from 9/11; information was not properly disseminated, there was a failure to "connect the dots," and Abdulmutallab's visa was not revoked.[42] Perhaps most importantly, the SSCI found numerous instances of information overload. First, analysts across the IC were unable to handle multiple analytical priorities at once. At the time of the failed Underwear bombing, the IC was primarily focused on collecting and analyzing information about Al-Qaeda activities in Yemen, and not information about Al-Qaeda threats to the U.S homeland.[43] Second, there appears to have been a backlog of unanalyzed intelligence about Abdulmutallab at the National Security Agency (NSA).[44] In theory, had the NSA analyzed this backlog of intelligence about Abdulmutallab, then it might have provided stronger evidence for homeland security officials to place Abdulmutallab on a no-fly list. Third, the NCTC lacked the resources to process and integrate disparate pieces of intelligence about Abdulmutallab.[45] Each of these findings suggests that there was too much information for IC analysts to process, and insufficient resources to do so effectively.

Is the high volume of homeland security information sharing making people safer or not? Admittedly, it is difficult to prove a negative here; we cannot know how safe we would be if we were *not* taking these steps. But practitioners have suggested that, despite many positive

steps that were taken to improve homeland security information sharing after 9/11, these changes are not achieving the successes that were hoped for.[46] Practitioners' perceptions of effectiveness matter a great deal. Because they are the ones who use this information, they are in the best position to evaluate the state of information sharing. If practitioners do not view these new information resources as helpful, they are less likely to use them.

C. Low-Quality Information

An increasingly widespread practitioner complaint about information sharing for homeland security is that the information itself is vague, dated, unreliable, and not actionable. This hinders analysts, because they are less able to make sense of the information, and it encumbers policymakers, who are presented with low-quality data that is not helpful for them in making decisions. In a 2009 study of homeland security officials, one practitioner framed the problem in blunt terms: "'There's a very fine line between information and s**t, and I think what we see a lot of times is that everybody's swapping s**t.'"[47] This low-quality information problem holds true in many homeland security sub-disciplines, from law enforcement, to emergency management, to critical infrastructure protection, to cyber security.

1. Low-Quality Information In Law Enforcement

In policing there is an ongoing need for information sharing for criminal intelligence purposes; that is, developing information about criminals that can potentially be used later in prosecutions. Moreover, there is a general, everyday need for information to be shared about vehicles, individuals, properties, and so forth. Yet incomplete or duplicative information often makes its way into law enforcement databases, diluting the quality of information that can be shared.

For example, two entries in a database may actually refer to the same person, but because of a misspelled name, future updates to those database entries become split between the two database entries. This same problem can emerge in the use of numbers in databases. To illustrate this, let us assume that John Doe is arrested for loitering, and tells the arresting police officer that his birthdate is November 4, 1974. If the police officer searches a database for John Doe using only Doe's birthdate, and the police officer inadvertently modifies a digit—say he types November 5, 1974 rather than November 4, 1974—then the police officer's search will come up empty, even though John Doe is already in the database under his correct birthdate of November 4, 1974.

The rise in criminal intelligence about persons whose names do not use characters from the Latin alphabet (i.e. a, b, c, d) further complicates this issue. For example, in Arabic, the name Mohammed is consistently spelled:

مُحَمَّد

By contrast, this name can be spelled any number of ways in English: Mohamed, Mohammed, Mohamad, Muhammad, and so on. Because of these differences in spelling, a police officer running a database check on "Mohammed" may turn up nothing at all, because "Mohammed" is actually listed in the database under "Muhammad" or "Mohamed"—a different spelling.[48] These inconsistent spellings can cause confusion both in data entry and data searches, because police officials may input or search for non-Latin character names in an inconsistent way.

The issue of sharing poor quality information now cuts across numerous homeland security-oriented law enforcement agencies. Personally identifiable information (PII) refers to data that can be used to identify a distinct person. Examples of PII include birthdates, addresses, and social security numbers. The FBI is restricted in the types of PII it can share internally, let alone with other law enforcement agencies.[49] This means that the quality and specificity of information that the FBI shares internally and externally is less than ideal. U.S. Customs and Border Protection maintains 17 distinct databases of information on foreign nationals, making database checks cumbersome and information sharing difficult.[50] And in law enforcement agencies at all levels of government, there is still an underlying cultural resistance to sharing information, complicating this issue even more.[51]

Apart from this inter-governmental information sharing, there is frustration between the public and private sectors about the quality of law enforcement information currently being shared. Part of this frustration is rooted in professional prejudices. Some government law enforcement officials view private security officials as less trained, less qualified, and less competent than their public sector law enforcement colleagues.[52] Some private sector security officers feel police lack full understanding of private security officers' roles, are indifferent to private security officers, and have an elitist attitude toward private security officers.[53] While these perceptions are not necessarily shared by all police or all private security officials, they create tense conditions that are not conducive to sharing high quality information. On the contrary, they reinforce attitudes of mistrust, suspicion, and even hostility.

Public-private information sharing in law enforcement is also subject to cumbersome legal and financial restrictions that can undermine effective cooperation. Because classified government information cannot be shared with individuals who do not possess a federally issued security clearance, the number of private sector employees who can receive classified information is limited.[54] Cross-sector information sharing is further inhibited by cost considerations. The average background investigation for a security clearance costs $1,230.00.[55] This fee is usually absorbed by the agency with which a firm is working. For example, if Company ABC is working with the Department of Defense, then the Department of Defense pays for Company ABC's employees to be investigated for a security clearance. Because of the costs involved with these background investigations, there is a natural tendency to limit the number of private sector employees who are issued security clearances; it saves money. While this is beneficial from a budgetary standpoint, it limits the number of private sector employees who can access classified government information, and therefore limits information sharing between the public and private sector.

Businesses are not necessarily quick to share law enforcement-related information with police, either. In the case of private security firms, there may be public relations tensions that inhibit information sharing. For example, if a private security firm detains a criminal, the firm may be reluctant to immediately notify police, because it wishes to claim credit for "catching the bad guy" in the public eye. The private security firm might take pains to get this information out into the open, because it boosts the firm's reputation as a reputable private security provider. If the private security firm were to turn the bad guy over to police immediately, then the police could claim credit for catching the bad guy, stealing the private security firm's public relations thunder. This would ruin an opportunity for the private security firm to market its success, and would sour the relationship between the private security firm and the police.

In the context of critical infrastructure protection, firms can also be reluctant to share sensitive information with law enforcement agencies. Firms within DHS' 16 critical infrastructure sectors can benefit from sharing information about their facilities and operations with police, because that information can be helpful for police during a crisis.[56] At the same time, however, no government agency is leakproof. It is always possible for sensitive information about a private sector facility or equipment to enter the public domain. And this type of disclosure can damage the firm's reputation or competitive advantage in the marketplace. Thus a company might only share superficial,

basic information about its activities with police so as to avoid potentially damaging leaks.

Moreover, if firms seeking to avoid government regulations or industry requirements provide information on their activities to police, these firms can open themselves up to criminal investigations and prosecutions. This puts both businesses and police in an awkward position. Although it makes sense for firms to provide company information to police, they also share this information at their own peril. For police it is awkward because they have a vested interest in building a successful partnership with businesses, and these partnerships are built upon a foundation of trust. But if police discover that a firm is engaged in illegal activity, it cannot ignore that illegal activity—the police must enforce the law and stop the illegal activity. Yet enforcing the law violates the trust that the firm placed in the police. To prevent this sequence of events, firms may only provide "thin" information to police—that is, information that might be helpful for the police, but contains few useful details. This reinforces low-quality information sharing between the private sector and the public sector. Similar concerns about low-quality information sharing are now apparent in the emergency management community, as well.

2. Low-Quality Information in Emergency Management

Information sharing is at the very core of emergency management. Without it, effective coordination among individuals and organizations involved in disaster mitigation, preparedness, response, and recovery is impossible. But the quality of the information shared in the emergency management community is getting worse. For example, e-mailed information bulletins circulate widely among emergency management practitioners. Although these bulletins are often little more than news digests, they do play a role in setting agendas for emergency management organizations by repeatedly documenting certain threats over time, reinforcing pre-conceived notions of threat severity, and prompting organizations to take action.[57]

However, information in these bulletins often adds little value, and the bulletins are not organized in a way that is helpful for decision-makers. One study of multiple homeland security bulletins notes that they are often an amalgam of popular media stories from sources like *The Washington Post*, Bloomberg News, and MSNBC, along with other government produced threat information.[58] Often these stories are displayed in an uncoordinated manner, and do not present a clear hierarchy of threat priorities.[59]

Although the threat information conveyed in these bulletins can be an important piece in developing a strategy to prepare for threats,

bulletins can exaggerate certain threats while diminishing the importance of others, skewing emergency preparation measures and putting lives and property at risk. For example, an emergency management agency in rural Wyoming might receive numerous homeland security bulletins that continue to discuss terrorism, day after day. Terrorists usually attack in densely populated communities, so rural Wyoming is an unlikely place for a terrorist attack. But these bulletins can influence threat perception, and this has an effect on preparation measures. It might lead the agency to purchase things that it does not really need.

Skewed perceptions have contributed to some of the most outrageous post-9/11 emergency preparedness spending. Consider some examples: a rural county in Colorado purchased a $44,000 "mass fatality" trailer that sits unused; one community in Michigan bought 13 arctic blast snow-cone machines to prevent heat-related illnesses during emergencies; and the police department in Hartwell, Georgia (population 4,469) purchased multiple sets of night vision goggles.[60] To be clear, we are not suggesting that low-quality information sharing alone is driving these questionable purchases. However, low-quality information can influence threat perceptions, and these perceptions can lead to decisions to buy expensive and unnecessary equipment.

Electronic information sharing tools have proliferated since 9/11. Yet the effect of these tools in facilitating cooperation between the public and private sectors is unclear. For example, Lessons Learned Information Sharing (llis.gov) is a U.S. Department of Homeland Security website that serves as a repository for best practices related to homeland security and emergency management. The site is constructed as a kind of bulletin board; anyone with a user account can post documents from exercises, meeting notes, and similar types of material for the learning benefit of others. For example, in the wake of Hurricane Katrina, many communities were left with reduced access to clean drinking water because of flooding and contamination. Water had to be imported from one community to another to meet crucial needs. This process prompted a number of local governments in the Gulf to post information about their emergency water sharing activities on llis.gov. The National Rural Water Association (NRWA), a private sector organization, harvested these lessons for information. As a result, the NRWA developed written guidelines for water sharing networks and mutual-aid agreements between states and localities.[61] These guidelines are available for state and local water authorities to use in order to better prepare for emergencies. Thus the private sector (the NRWA) used lessons learned from the public sector (Gulf local governments) to benefit the public sector (other state and local governments).

This case can be held up as a success story for high-quality information sharing in emergency management.

However, other evidence about information sharing tools paints a slightly different picture. A 2009 study of llis.gov users found that although the site seemed to increase awareness of homeland security threats, there was no significant correlation between frequency of information sharing and perceived ability to prevent homeland security emergencies. Nor was there a significant correlation between use of llis.gov and perceived organizational preparedness.[62] These findings suggest a gap between the actual sharing that takes place on sites like llis.gov and the effect of that sharing on homeland security activities. They imply that although information is being shared on sites like llis.gov, the quality of that information may not be of much use. One respondent framed the issue plainly: "'I hope somebody someplace has more information that they're utilizing to protect the country because I'm not seeing a lot of stuff that's of great value.'"[63]

3. Low-Quality Information in Critical Infrastructure Protection

Some 85% of all critical infrastructure in the United States is owned or managed by the private sector.[64] Given this reality, government has little choice but to partner with businesses to protect critical infrastructure. It is logical to assume that because of this dependency, government and businesses would exchange information that is timely, relevant, and actionable on a frequent basis. While this is happening to a limited extent, important challenges remain unresolved related to information quality.

As stated earlier, certain government information is classified because releasing it to the public would damage U.S. national security. When the government classifies something, it attaches legal protections to that information, charging the holder of the information to safeguard it or face stiff legal penalties for disclosing it. In order to legally exchange classified information, both the sender and recipient of the information must have security clearances at or above the classification level of the information itself. Moreover, the recipient must have a need to know the information.[65] This compartmentalizes information, limiting any one person's knowledge of classified information beyond their immediate area of professional responsibility. These measures—security clearances and the "need to know"—have been in place for many years. But classified information also complicates the way information gets shared between the public and private sectors.

Many owners or operators of critical infrastructure companies and corporations do not have security clearances. As a result, when the

government sends important information to these private sector employers, it must send an unclassified version of the information, rather than a classified version of the information. Often this unclassified version of the information omits certain details to protect information sources and intelligence-gathering methods. But these omissions limit the utility of the information. Without a source, a recipient cannot make independent judgments about how credible or non-credible a piece of information is. There are other issues that show how low quality information sharing in critical infrastructure protection concerns more than just handling classified information.

Sharing information that is timely, relevant and actionable costs time and money. Government officials must sift through databases and files to locate specific information that can benefit critical infrastructure owners and operators. If we consider information sharing to be a transaction, then the transaction cost of sharing high quality information is greater than the transaction cost of sharing low-quality information, because high quality information is always in short supply. If government officials act in a predictable manner (and we assume that they do) then they will gravitate toward lower cost information transactions.

Conditions are similar for the private sector. For example, businesses can easily generate information about sales revenue. This data is commonplace in any firm. But it is harder for a business to inventory each of its security cameras, conduct vulnerability assessments, or produce detailed facility maps. These tasks are less common. They take time—time that is spent away from revenue-generating activities. And they cost money; labor and supplies to do these things are not free. But a detailed inventory of security cameras, vulnerability assessments, and facility maps are likely more useful for government than sales data. Thus there is a higher transaction cost associated with gathering data on security measures than gathering data on sales revenue. For both the public and private sectors, then, there is a high transaction cost in sharing high quality information, and this means that government and businesses will naturally gravitate toward lower transaction costs, and therefore lower-quality information sharing.

4. Low-Quality Information in Cyber security

Cyber threats are exploding in number and scope. As in other areas of homeland security, the public and private sectors share information about these threats. And although substantial progress has been made in this area, low-quality information continues to circulate across the public-private sector divide in cyber security.

Information sharing agreements in cyber security are highly complex.[66] They extend horizontally across government, and vertically between local, state, and federal governments. Moreover, these agreements extend between the public and private sectors.[67] And while the complexity of an information sharing network does not necessarily equate with low-quality information sharing, threat information can fragment in a complex information sharing network. Fragmented information is incomplete information, and incomplete information is less useful for decision-makers. It is reasonable to assume that the tangled net of public and private sector entities sharing cyber security information can inadvertently generate fragmented, low-quality information.

Information sharing websites go a long way toward centralizing cyber security knowledge across government and the private sector. But at the same time, it is not clear that this centralized information is very useful for decision-makers.[68] The websites themselves are not immune to attack, either. In 2009 a hacker broke into the Homeland Security Information Network (HSIN), a password-protected website for sharing homeland security-related data.[69] During this incident, the hacker accessed the phone numbers and email addresses of state and federal employees, but he did not retrieve sensitive information like social security numbers.[70] This shows that information sharing websites may not be very useful, because they likely contain fragmented, low-quality information. And somewhat ironically, the websites used to share cyber security information are themselves vulnerable to cyber threats.

The public and private sector are not meeting one another's expectations for sharing cyber security information, and this partly explains why low-quality information sharing occurs in this area. A 2010 Government Accountability Office (GAO) report points toward a number of central problems that vex businesses and government working in cyber security. For example, the private sector expects government information on threats to be "usable, timely, and actionable," but this is still not happening, even with efforts to improve information sharing through tools like HSIN or professional organizations focused on cyber security issues.[71] Government believes that the depth and specificity of information that businesses share about cyber security is limited; this seems to stem from firms' reluctance to share sensitive and proprietary information with government.[72]

In sum, a lack of trust between the public and private sector impedes cross-sector information sharing for homeland security. There is an unmanageable tidal wave of homeland security information that hammers businesses and government daily. And the quality of that information is questionable. These issues point toward a series of new

challenges for public-private partnerships in homeland security: building cross-sector trust over time, managing the flow of homeland security information, and improving the quality of information being shared. Fortunately public-private partnerships are well-equipped to begin addressing these challenges.

IV. Public-Private Partnership Solutions For Information Sharing In Homeland Security

A. Public-Private Partnerships Can Help Build Trust

The trust deficit between the public and private sector encumbers information sharing. It invites both sectors to view one another with mutual suspicion. This harms homeland security, because it limits the chances of cross-sector information sharing being helpful for either sector. So how can public-private partnerships increase cross-sector trust?

Trust forms through repeated contact between business and government representatives. And this trust leads to professional relationships. This person-to-person relationship building helps to create trust between organizations. Groups like Infragard and the CIPAC help facilitate this process. As Paul Byron Pattak, CEO of the Infragard National Capital Members Region, explains:

> The first thing you have to do is create an environment where people are comfortable coming and meeting others. So before any [information sharing] happens, the relationships have to be established. And as we all know, we don't trust people immediately when we meet them. We need to get to know them a little bit better, we need to spend some time with them, maybe have lunch or dinner … so trust is built over time. But once you have it, there is so much you can do with the relationship … Because we join [Infragard] individually as members, we're really good at helping forge those relationships. And people come to Infragard and get the opportunity to meet people that you are unlikely to meet in other contexts.[73]

Pattak's remarks underline the way in which personal relationships can translate into inter-organizational trust. This inter-organizational trust enhances effectiveness in sharing information. With greater trust, the public sector will be more likely to share sensitive or classified information with the private sector, not only because private sector officials hold the requisite clearances to safeguard classified information (a formal indicator of trust) but also because of individual relationships between public and private sector representatives (an informal indicator of trust).

An additional way public-private partnerships can increase cross-sector trust is by constructing service level agreements (SLAs) in contracts and honoring them. This is a business-focused approach to set expectations between public-private partners. An SLA sets specific, measurable metrics for vendor performance, whether that vendor is delivering a product or a service. These metrics often come with incentives for excellent performance, or penalties for poor performance. For example, an SLA might stipulate the time for delivery of a desktop computer, from order submission to installation, at 48 hours. Using this example, if a desktop computer is ordered, delivered, and installed in less than 48 hours, the vendor might receive a small bonus payment. If the desktop computer is not delivered in 48 hours, by contrast, the vendor might compensate government by paying a penalty for failing to meet the SLA.

SLAs manage public and private sector expectations in contracts, building trust over time. Both parties know that good work is rewarded, while shoddy work is not. A certain "gray area" of work is eliminated through this arrangement, too. That is, without SLAs, if a product or service is not delivered correctly or on time, there is no recourse or compensation for government—just a "gray area" of frustration and violated expectations. Without SLAs, firms have no incentive to work more efficiently, other than meeting the minimum requirements of contracts with government. But with SLAs, government knows that it can be compensated for the contract not being fulfilled according to its expectations. From the government's perspective, SLAs eliminate this "gray area" of unfulfilled expectations. From the private sector's perspective, SLAs offer incentives to do work better and more efficiently, which can increase the firm's bottom line substantially. SLAs manage public and private sector expectations, and they diminish the chance of expectations being violated by either government or businesses. And with fewer violations of expectations, trust increases over time.

B. Public-Private Partnerships Can Help to Manage the Information Deluge

There is a natural limit to the amount of information a given homeland security analyst can process. It does not really matter that the most advanced technology is being applied to information sharing problems in homeland security; the true problem here is that while computers' ability to process information grows constantly, a human being's ability to process information remains unchanged. In the midst of the present information sharing tidal wave, public and private sector homeland security analysts are encouraged to review as many

sources of information as possible, because (the thinking goes) this leads to higher quality analyses. This places homeland security analysts in an impossible position, where they have to sort through an unmanageably high level of information and continue to produce high quality analyses.[74] Yet public-private partnerships offer a number of important solutions to help manage the flow of homeland security information.

Technological innovations, coupled with enhanced operator skills to use new technologies, are perhaps the most obvious solutions to managing the homeland security information deluge. Firms, collaborating with government, can develop software to filter and prioritize information for individual analysts. This helps to ensure that analysts review and study information that is most relevant to them. By managing the flow of information in this way, public-private partnerships help analysts. Analysts can then do more with less, because the information they review has been reduced to manageable levels. When the flood of information slows, analysts can focus more upon analysis itself, rather than filtering through information so that they can begin analysis. This ultimately benefits decision-makers that are consumers of intelligence products.

Programmatic innovation, too, can help to manage the high volume of information. For example, the FBI's Infragard program is a public-private partnership focused on critical infrastructure protection.[75] Infragard is heavily populated by law enforcement personnel, especially FBI employees. Infragard meetings typically include significant informal interaction between police and private sector representatives. And these low-level interactions serve an important agenda-setting function which helps to manage the flow of information.[76] During informal conversations and formal presentations at Infragard meetings, certain topics come up regularly: terrorism, surveillance of nuclear power plants, synthetic drugs, and so forth. These conversations help to set organizational agendas, because they reinforce the importance of certain homeland security concerns over others, and they demonstrate that those concerns are shared by numerous public and private sector organizations. This agenda-setting effect helps to manage the information flood, because it prompts analysts to focus more on higher priority issues that are discussed than lower priority issues that are not discussed.

Business process analysis is a favorite tool of the private sector, because it helps to identify and eliminate inefficiencies, leading to cost savings for firms. Process improvements can help to manage the homeland security information flood. Private sector consultants can help review government homeland security information sharing processes,

and identify areas of weakness or waste within them. By implementing process changes, government's information sharing efforts become more effective, and can help to reduce the information deluge to reasonable levels. Consultants benefit by being paid for their expertise. Thus public-private partnerships can help to manage the information sharing flood in an effective, mutually beneficial way.

C. Public-Private Partnerships Can Improve Information Quality

Alliances between businesses and government can improve the quality of homeland security information. This can happen in ways that are practically identical to those benefits conferred in managing the information flow: via technology, programming, and process analysis.

The same software used to filter the volume of information seen by homeland security analysts can also be used to enhance the quality of the information. For example, a new tool developed by IBM addresses poor data quality in police databases.[77] This tool—a software application—searches for entries in databases that appear to be duplicative and flags them for further investigation. This helps the police to identify fragmented or low-quality data and to improve the data so that it is more useful in practice. Eliminating duplicate or fragmented database entries improves data consistency, and data consistency helps analysts.

Programming innovations also help to improve information quality. DHS maintains a Critical Infrastructure Partnership Advisory Council (CIPAC) composed of public and private sector leaders. The CIPAC focuses on sharing threat information to enhance critical infrastructure protection.[78] Moreover, the CIPAC is further sub-divided into sector-specific working groups. These groups address issues germane to each of the 16 critical infrastructure sectors that DHS identifies.[79] Because of the substantial level of cross-sector communication and collaboration involved in the CIPAC, the group provides an agenda-setting function that manages the volume of information being shared, as well as the quality of the information being shared. By filtering out low-priority topics in CIPAC discussions, public and private sector leaders are better able to set information sharing agendas within their own organizations, and they can make more informed decisions about the amount and type of information they share with other organizations. Because of this, analysts are fed higher quality information. And this means that analyses are better than they would be otherwise.

Business process analysis can improve the quality of information being shared. A business process analysis of multiple intelligence agencies, for example, might find that they are all producing redundant

reports about the same topic, and that they are all sharing those redundant reports with other agencies. Private sector consultants can spot and change this behavior. This not only saves taxpayer dollars by eliminating duplication of effort, but it also helps to reduce the amount of information analysts must sort through. This increases the quality of information being shared, and it makes the information sharing process more effective for both government and businesses.

V. Recommendations For The Future Of Public-Private Partnerships In Homeland Security Information Sharing

Low cross-sector trust, the persistent flood of homeland security information, and the abundance of low-quality information all challenge public-private partnerships in homeland security. But public-private partnerships offer a number of avenues to improve homeland security information sharing over the long haul, too. By building trust over time, managing the information deluge, and improving the quality of information, public-private partnerships can be a catalyst for better information sharing in homeland security. To bolster homeland security information sharing using public-private partnerships, four specific policy recommendations follow below. While these recommendations cannot address every challenge in homeland security information sharing, they are concrete steps for government agencies and businesses to begin improving their information sharing practices.

A. Learn to measure trust

Most data on cross-sector trust tends to be qualitative and descriptive. Quantitative data on precisely how much public and private sector entities do or do not trust one another could be useful for scholars in assessing trust levels over time, and identifying effective ways to improve cross-sector trust. For example, using surveys containing Likert scales, which can assign numerical values to trust levels, public and private sector officials can more accurately gauge how the entities in a given partnership view each other.[80] Where partners desire to improve their partnership, private sector polling firms could provide valuable assistance in administering these surveys. Insights from these surveys can be used to improve public-private partnerships in general.

This survey data could also open the door to future "action research." Action research involves scholars actively working with practitioners in order to test theories or bring about a desired outcome, rather than serving as passive, disinterested observers.[81] Scholars can help homeland security practitioners improve their operations by offering

a fresh, outside perspective and enabling practitioners to see their work practices in a new light. In action research that focuses upon homeland security information sharing, scholars could serve as active facilitators in public-private sector trust-building forums and collaborative projects.[82] Conducting action research in this way, and publishing the results of this research, could be valuable for homeland security scholars and practitioners alike.

B. Software algorithms can help manage the information overload

The private sector can help government intelligence analysts to deal with information overload by developing innovative software algorithms to assist in processing and sorting through information. In much the same way that a particular Google search term can retrieve precisely the information that a computer user is searching for, well-designed intelligence analysis software can help analysts separate useful information from less-useful information. These algorithms can be integrated into existing IC databases, making it easier to connect disparate pieces of information, look up names with multiple possible spellings, or discern patterns that point toward suspicious activity.

Additionally, these same algorithms can help to integrate separate IC databases, making it possible for analysts to conduct a single search that covers numerous databases at once. These kinds of software algorithms can help to ensure that information gathered by one IC member agency can be accessed by all IC member agencies, helping analysts to "connect the dots." While tools like software algorithms cannot be a cure-all for the problem of information overload, they *can* make it easier for intelligence analysts to make sense of the information overload, and ultimately help homeland security policymakers make more well-informed decisions.

C. Determine how much information is too much information.

The general consensus among researchers is that homeland security analysts are drowning in data. In business management literature there is a concept called "span of control" that refers to the number of persons one individual can effectively supervise.[83] There is a similar "span of control" limit for the amount of information one individual can effectively process and analyze in an hour, a day, or a week.[84] Using data on the amount of information that homeland security analysts can effectively process, homeland security managers can develop specific targets that designate how much information a given analyst can receive and analyze at any given point in time.

Furthermore, as discussed above, software algorithms can help to manage this information deluge. But beyond managing the information flood, software algorithms offer a second, related benefit: these algorithms can also bolster individual analysts' effectiveness. When software algorithms steer analysts toward useful, high-quality information, that same high-quality information influences their analyses. Using high-quality raw data can lead to sharper, more insightful intelligence analyses. These improved analyses signal an increase in analysts' efficiency and effectiveness. Well-designed software algorithms help to keep analysts from drowning in data, and also help them to be better analysts.

D. Improve analysis through peer review.

Some information sharing tools such as Intellipedia permit IC analysts to peer review information, enhancing the credibility of a particular piece of analysis and its author.[85] Amazon.com and EBay.com, two of the world's largest online shopping websites, use similar ratings systems for buyers to evaluate sellers. Pandora.com, an Internet radio website, permits listeners to rate each song they hear. With this information, Pandora.com uniquely tailors each listener's experience according to her own musical preferences; a listener can reject certain genres or artists while embracing others. Could homeland security information circulated via email or other information sharing networks employ a similar rating system? And could the rating system be designed so that high-priority, high-quality analyses "bubble up," while redundant or vague analyses get filtered out? Scholars and practitioners can benefit from exploring this idea further.

Information sharing will continue to be vital in homeland security for the foreseeable future. Public-private partnerships are essential to making this information sharing effective. In building cross-sector trust, managing the information flood, and honing the quality of information, public-private partnerships hold great promise for the future of homeland security.

ENDNOTES

[1] U.S. Immigration and Customs Enforcement, "Underwear Bomber Umar Farouk Abdulmutallab sentenced to life" [Press Release], February 16, 2012, accessed October 5, 2012, http://www.ice.gov/news/releases/1202/120216detroit.htm.
[2] Barbara Van Woerkem, Peter Kenyon, Ofeibea Quist-Arcton, Dina Temple-Raston, Priscilla Villareal, "Timeline: From Student to Radical," npr.org, n.d., accessed October 5, 2012, http://www.npr.org/templates/story/story.php?storyId=123768455.
[3] Sarah Childress, Jay Solomon, and Stephen Fidler, "Suspect's Privileged Existence Took a Radical Turn," *The Wall Street Journal*, December 29, 2009,

accessed October 5, 2012, http://online.wsj.com/article/SB126187511080506063.html.
[4] Woerkem et al., "Timeline."
[5] Ibid.
[6] Senate Select Committee on Intelligence, "Attempted Terrorist Attack on Northwest Airlines Flight 253," May 24, 2010, accessed October 5, 2012, http://www.intelligence.senate.gov/pdfs/111199.pdf, 2; Mark Hosenball, "What the CIA Did and Didn't Know About Alleged Underpants Bomber," *The Daily Beast*, December 30, 2009, accessed October 5, 2012, http://www.thedailybeast.com/newsweek/blogs/declassified/2009/12/30/what-the-cia-did-and-didn-t-know-about-alleged-underpants-bomber.html.
[7] Sarah Netter, "Jasper Schuringa Yanked Flaming Syringe Out of Abdulmutallab's Pants," abcnews.com, December 28, 2009, accessed October 5, 2012, http://abcnews.go.com/GMA/northwest-flight-253-hero-yanked-flaming-syringe-abdulmutallab-pants/story?id=9432099#.UFH_d5gVoro.
[8] Peter Baker and Scott Shane, "Obama Seeks to Reassure U.S. After Bombing Attempt," *The New York Times*, December 28, 2009, accessed October 5, 2012, http://www.nytimes.com/2009/12/29/us/29terror.html?pagewanted=all.
[9] U.S. Immigration and Customs Enforcement, "Underwear Bomber Umar Farouk Abdulmutallab."
[10] "Passenger says he helped thwart terror attack," cnn.com, December 26, 2009, accessed October 5, 2012, http://articles.cnn.com/2009-12-26/justice/airliner.attack.schuringa_1_umar-farouk-abdulmutallab-plane-northwest-airlines-flight?_s=PM:CRIME.
[11] Tom Leonard, "Hero tackled alleged Northwest plane bomber as flames came from him on flight to Detroit," *The Telegraph*, December 26, 2009, accessed October 5, 2012, http://www.telegraph.co.uk/news/worldnews/northamerica/usa/6890990/Hero-tackled-alleged-Northwest-plane-bomber-as-flames-came-from-him-on-flight-to-Detroit.html.
[12] Ibid.
[13] Barbara A. Grewe, "Legal Barriers to Information Sharing: The Erection of a Wall Between Intelligence and Law Enforcement Organizations," National Commission on Terrorist Attacks Upon the United States: Staff Monograph, August 20, 2004, accessed October 9, 2012, http://www.fas.org/irp/eprint/wall.pdf; National Commission on Terrorist Attacks Upon the United States, "How To Do It: A Different Way Of Organizing The Government," 2004, accessed October 9, 2012, http://govinfo.library.unt.edu/911/report/911Report_Ch13.htm; U.S. Department of Homeland Security, *Implementing 9/11 Commission Recommendations: Progress Report 2011*, 2011, accessed October 9, 2012, http://www.dhs.gov/xlibrary/assets/implementing-9-11-commission-report-progress-2011.pdf, 11– 12; CBS/AP, "Costly post-9/11 info sharing program slammed," cbsnews.com, October 3, 2012, accessed October 9, 2012, http://www.cbsnews.com/8301-201_162-57524994/costly-post-9-11-info-sharing-program-slammed/.
[14] Jolie Lee, "Agencies get better at 'whole of government' info sharing," federalnewsradio.com, August 30, 2012, accessed October 5, 2012, http://www.federalnewsradio.com/490/3014484/Agencies-get-better-at-whole-of-government-info-sharing.
[15] U.S. Intelligence Community, "Our Strength Lies in Who We Are," intelligence.gov, n.d., accessed October 9, 2012, http://www.intelligence.gov/about-the-intelligence-community/member-agencies/.
[16] Kashmir Hill, "The Department of Homeland Security Wants All The Information It Has On You Accessible From One Place," forbes.com, November 29, 2011, accessed October 5, 2012, http://www.forbes.com/sites/kashmirhill/2011/11/29/department-of-homeland-security-wants-all-the-information-it-has-on-you-accessible-from-one-place/.
[17] National Counterterrorism Center, "About the National Counterterrorism Center," n.d., accessed October 5, 2012, http://www.nctc.gov/about_us/about_nctc.html.
[18] New York Police Department, "NYPD Shield: About," 2006, accessed October 5,

2012, http://www.nypdshield.org/public/about.aspx.
[19] Ibid.
[20] The Washington Post, "Top Secret America: New York," 2012, retrieved October 5, 2012, http://projects.washingtonpost.com/top-secret-america/states/new-york/.
[21] Michael Barbaro and Justin Gillis, "Wal-Mart at Forefront of Hurricane Relief," *The Washington Post*, September 6, 2005, accessed October 5, 2012, http://www.washingtonpost.com/wp-dyn/content/article/2005/09/05/AR2005090501598.html; Steven Horwitz, "Wal-Mart to the Rescue: Private Enterprise's Response to Hurricane Katrina," June 2008, accessed March 6, 2013, http://myslu.stlawu.edu/~shorwitz/Papers/Wal-Mart_to_the_Rescue.pdf.
[22] Ami J. Abou-bakr, *Managing Disasters through Public-Private Partnerships* (Washington, DC: Georgetown University Press, 2013), 24.
[23] Craig Allen, "As Joplin, Missouri Rebuilds, a Home Depot Store Reopens," homedepot.com, January 11, 2012, accessed October 5, 2012, http://ext.homedepot.com/community/blog/tag/joplin/.
[24] Roger McKinney, "RESOURCE: FEMA specialists on hand at Home Depot," *The Joplin Globe*, July 1, 2011, accessed March 6, 2013, http://www.joplinglobe.com/tornadoresources/x652255506/FEMA-specialists-on-hand-at-Home-Depot.
[25] U.S. Department of Homeland Security, *Implementing 9/11 Commission Recommendations: Progress Report 2011*, 2011, accessed March 6, 2013, http://www.dhs.gov/xlibrary/assets/implementing-9-11-commission-report-progress-2011.pdf, 3–6.
[26] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, 2004, accessed March 6, 2013, http://www.9-11commission.gov/report/911Report.pdf, 433.
[27] U.S. Department of Homeland Security, *Department of Homeland Security Information Sharing Strategy*, April 18, 2008, accessed March 6, 2013, http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf, 6; Peter J. Denning, "Hastily Formed Networks," *Communications of the ACM* 49, no. 4 (2006): 18–19; Naim Kapucu, "Non-Profit Response to Catastrophic Disasters," *Disaster Prevention and Management* 16, no. 4 (2007): 551–561; Eugene Bardach, *Getting Agencies to Work Together: The Practice and Theory of Managerial Craftsmanship* (Washington, DC: Brookings Institution Press, 1998), 252–253; William L. Waugh, Jr., "Terrorism, Homeland Security, and the National Emergency Management Network," *Public Organization Review* 3, no. 4 (2003): 373–385.
[28] The White House, *National Strategy for Information Sharing,* October 2007, accessed March 6, 2013, http://www.fas.org/sgp/library/infoshare.pdf, 10.
[29] U.S. Department of Homeland Security, *Department of Homeland Security Information Sharing Strategy*, 2.
[30] Joseph W. Pfeifer, "Network Fusion: Information and Intelligence Sharing for a Networked World," *Homeland Security Affairs* 8 (October 2012): 11.
[31] Nathan E. Busch and Austen D. Givens, "Public-Private Partnerships in Homeland Security: Opportunities and Challenges," *Homeland Security Affairs* 8 (October 2012): 13.
[32] Joseph Straw, "Intelligence Sharing improves," *Security Management*, n.d., accessed October 5, 2012, http://www.securitymanagement.com/article/intelligence-sharing-improves.
[33] U.S. Department of Homeland Security, "DHS Announces New Information-Sharing Tool to Help Fusion Centers Combat Terrorism" [Press Release], September 14, 2009, accessed October 9, 2012, http://www.dhs.gov/news/2009/09/14/new-information-sharing-tool-fusion-centers-announced.
[34] Federal Emergency Management Agency, Lessons Learned Information Sharing (llis.gov), n.d., accessed October 9, 2012, https://www.llis.dhs.gov/index.do.
[35] Central Intelligence Agency, "Intellipedia Celebrates Third Anniversary with a Successful Challenge," April 29, 2009, accessed October 9, 2012, https://www.cia.gov/news-information/featured-story-archive/intellipedia-celebrates-third-anniversary.html; Joab Jackson, "A-Space melds social media and intelligence gathering," gcn.com, November 20, 2009, accessed October 9, 2012, http://gcn.

com/articles/2009/11/30/a-space-dia-intell-sharing-wiki.aspx.
[36] Federal Bureau of Investigation, Law Enforcement Online (leo.gov), n.d., accessed October 9, 2012, http://www.leo.gov/.
[37] Hamilton Bean, "Exploring the Relationship between Homeland Security Information Sharing & Local Emergency Preparedness," *Homeland Security Affairs* 5, no. 2 (2009): 9, italics in the original.
[38] Ibid., 8.
[39] Henry H. Willis, Genevieve Lester, and Gregory F. Treverton, "Information Sharing for Infrastructure Risk Management: Barriers and Solutions," *Intelligence and National Security* 24, no. 3 (June 2009): 362–363.
[40] Senate Select Committee on Intelligence, "Attempted Terrorist Attack on Northwest Airlines Flight 253," 2.
[41] Ibid.
[42] Ibid.
[43] Ibid., 6,7,9.
[44] Ibid., 8.
[45] Ibid., 7.
[46] Bean, "Exploring the Relationship between Homeland Security Information Sharing."
[47] Ibid., 9, asterisks ours.
[48] Converting names from one alphabet to another alphabet is called transliteration. The issue of transliteration in national security databases is receiving increasing attention. See David Holmes, Samsun Kashfi, and Syed Uzair Aqeel, "Transliterated Arabic Name Search," Proceedings of the Third IASTED International Conference: Communications, Internet, and Information Technology, November 2004, accessed October 9, 2012, http://uzair.nairang.org/wp-content/uploads/2006/10/433-175.pdf; Mark Arehart, "Indexing Methods for Faster and More Effective Person Name Search," Proceedings of the 2010 Language Resources Evaluation Conference, 2010, accessed October 9, 2012, http://www.lrec-conf.org/proceedings/lrec2010/pdf/166_Paper.pdf.
[49] Peter L. Gomez, "Enhancing FBI Terrorism and Homeland Security Information Sharing With State, Local, And Tribal Agencies" (master's thesis, Naval Postgraduate School, September 2010, 2.
[50] U.S. Department of Homeland Security Office of the Inspector General, *Information Sharing on Foreign Nationals: Border Security (Redacted)*, February 2012, OIG-12-39, 2.
[51] Willis, Lester, and Treverton, "Information Sharing for Infrastructure Risk Management," 348.
[52] International Association of Chiefs of Police, *National Policy Summit: Building Private/Public Policing Partnerships to Prevent and Respond to Terrorism and Public Disorder—Vital Issues and Policy Recommendations*, 2004, accessed October 9, 2012, https://www.theiacp.org/LinkClick.aspx?fileticket=UVc2ImxcWpQ%3D&tabid=938, 7.
[53] Ibid.
[54] Richard A. Best Jr., "Intelligence Information: Need-to-Know vs. Need-to-Share," Congressional Research Service, June 6, 2011, retrieved September 21, 2012, http://www.fas.org/sgp/crs/intel/R41848.pdf, 3.
[55] William Henderson, "How Much Does It Really Cost to Get a Security Clearance?", clearancejobs.com, August 7, 2011, accessed October 9, 2012, http://www.clearancejobs.com/cleared-news/381/how-much-does-it-really-cost-to-get-a-security-clearance.
[56] Presidential Policy Directive (PPD) 21 reduced the number of federally recognized critical infrastructure sectors from 18 to 16. See The White House, "Presidential Policy Directive—Critical Infrastructure Protection and Resilience," February 12, 2013, accessed March 7, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil; U.S. Department of Homeland Security, "Critical Infrastructure Sectors," n.d., accessed March 6, 2013, http://www.dhs.gov/critical-infrastructure-sectors.
[57] Hamilton Bean and Lisa Keränen, "The Role of Homeland Security Information Bulletins Within Emergency Management Organizations: A Case Study of

Enactment," *Journal of Homeland Security and Emergency Management* 4, no. 2 (2007): 9.
[58] Ibid.
[59] Ibid.
[60] David Olinger and Jennifer Brown, "Colorado's homeland security spending has been all over the map," *The Denver Post*, September 4, 2011, accessed October 9, 2012, http://www.denverpost.com/911/ci_18805920; "Montcalm County gets homeland security snow cone machine," wzzm13.com, December 5, 2011, accessed October 9, 2012, http://www.wzzm13.com/news/article/188877/14/Montcalm-County-gets-homeland-security-snow-cone-machine.
[61] Katherine J. Worboys, "Recent Research from *Lessons Learned Information Sharing*: The Importance of Partnerships in the Rural Water Response to Hurricane Katrina," *Journal of Environmental Health* 69, no. 2 (September 2006): 31–33.
[62] Bean, "Exploring the Relationship between Homeland Security Information Sharing," 7.
[63] Ibid., 12.
[64] U.S. Department of Homeland Security, "Critical Infrastructure Sector Partnerships," n.d., accessed October 9, 2012, http://www.dhs.gov/critical-infrastructure-sector-partnerships.
[65] Richard A. Best Jr., "Intelligence Information: Need-to-Know vs. Need-to-Share," Congressional Research Service, Report No. R41848, June 6, 2011, retrieved September 21, 2012, http://www.fas.org/sgp/crs/intel/R41848.pdf, 1–13.
[66] Rachel Nyswander Thomas, "Securing Cyberspace through Public Private Partnership: A Comparative Analysis of Partnership Models" (master's thesis, Georgetown University, 2012).
[67] Ibid.
[68] Bean, "Exploring the Relationship between Homeland Security Information Sharing."
[69] Ben Bain, "Information-sharing platform hacked," *Federal Computer Week*, May 13, 2009, accessed October 9, 2012, http://fcw.com/articles/2009/05/13/web-dhs-hsin-intrusion-hack.aspx.
[70] Ibid.
[71] U.S. Government Accountability Office, "Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed," July 2010, GAO-10-628, 13.
[72] Ibid., 22.
[73] "Public-Private Sector Information Sharing-Paul Byron Pattak," Symposium on Homeland Security, 26.16– 27.10, posted by Christopher Newport University Center for American Studies, July 20, 2012, http://www.symposiumonhomelandsecurity.com/Panel3.html.
[74] Nathan Alexander Sales, "Mending Walls: Information Sharing After the USA PATRIOT Act," *Texas Law Review* 88, no. 7 (June 2010): 1804.
[75] Federal Bureau of Investigation, infragard.net, 2012, accessed October 9, 2012, http://www.infragard.net/.
[76] This is similar to the agenda-setting function of homeland security bulletins. See Bean and Keränen, "The Role of Homeland Security Information Bulletins," 9–10.
[77] Darryl Plecas, Amanda V. McCormick, Jason Levine, Patrick Neal, and Irwin M. Cohen, "Evidence-based information sharing solution between law enforcement agencies," *Policing: An International Journal of Police Strategies and Management* 34, no. 1 (2011): 120–134.
[78] U.S. Department of Homeland Security, "Critical Infrastructure Partnership Advisory Council," n.d., accessed October 9, 2012, http://www.dhs.gov/critical-infrastructure-partnership-advisory-council.
[79] U.S. Department of Homeland Security, "Critical Infrastructure Sectors," n.d., accessed April 19, 2013, http://www.dhs.gov/critical-infrastructure-sectors.
[80] For an example of how Likert scales have been used to measure trust, see John K. Butler Jr., "Toward understanding and measuring conditions of trust: Evolution of a conditions of trust inventory," *Journal of Management* 17, no. 3 (1991): 643–663.

[81] Jean McNiff and Jack Whitehead, *Action Research in Organisations* (London: Routledge), 2001, 3–4; Jack Whitehead and Jean McNiff, *Action Research: Living Theory* (Thousand Oaks, CA: SAGE Publications, Inc.), 2006, 13.
[82] For a recent example of how action research can be applied to homeland security, see Stig Johnsen and Mona Veen, "Risk assessment and resilience of critical communication infrastructure in railways," *Cognition, Technology & Work* 15, no. 1 (March 2013): 95–107.
[83] For a classic treatment of this concept, see Michael Keren and David Lehari, "The Optimum Span of Control in a Pure Hierarchy," *Management Science* 25, no. 11 (1979): 1162–1172.
[84] Marten van Someren, Niels Netten, Vanessa Evers, Henriette Cramer, Robert de Hoog, and Guido Bruinsma, "A trainable information distribution system to support crisis management," *Proceedings of the Second International ISCRAM conference* (Brussels, Belgium), April 2005.
[85] Frank Ahrens, "A Wikipedia of Secrets," *The Washington Post*, November 5, 2006, accessed September 28, 2012, http://www.washingtonpost.com/wp-dyn/content/article/2006/11/03/AR2006110302015.html; Nancy M. Dixon and Laura A. McNamara, "Our Experience With Intellipedia: An Ethnographic Study at the Defense Intelligence Agency," Defense Intelligence Agency Laboratory Project, February 5, 2008, accessed September 28, 2012, http://www.au.af.mil/au/awc/awcgate/sandia/dixon_mcnamara_intellipedia.pdf.