Public-Private Partnerships in Homeland Security: Opportunities and Challenges

Nathan E. Busch and Austen D. Givens

ABSTRACT

Public-private partnerships are a major issue of discussion in businesses and government agencies concerned with homeland security. However, this issue has received a much less thorough treatment in scholarly literature on homeland security. This article begins to fill a gap in homeland security scholarship by identifying the essential role that public-private partnerships are now taking in homeland security and by examining opportunities and challenges for this transformative shift in the field. The article begins by contextualizing our argument within recent scholarship, and tracing the development of public-private partnerships in homeland security. The article then examines the growing role of public-private sector partnerships in homeland security. The article concludes by discussing ongoing challenges that will need to be considered and addressed for public-private partnerships to be successful over the long term.

INTRODUCTION

> *"…I want to just say this about the private sector. In my mind, the government is incapable of responding to its maximum ability without private sector support…"*[1]
> –Hon. Tom Ridge, Former Secretary, U.S. Department of Homeland Security

April 20, 2010 had been an otherwise typical day. At 9:49 p.m., however, the first of several blasts shattered the night air over the Gulf of Mexico, ultimately killing eleven workers and crippling the Deepwater Horizon oil rig.[2] The explosion and subsequent oil spill eventually became the largest environmental catastrophe in US history.[3] Over the following months, hundreds of government and private sector actors convened around the Gulf of Mexico, summoning an unprecedented amount of equipment and technical expertise to stop the oil flow from the Gulf's floor. British Petroleum (BP), the National Oceanic and Atmospheric Administration, the US Coast Guard, state governments, local governments, and hundreds of businesses and public sector agencies collaborated in response to the disaster.[4] British Petroleum and local officials launched initiatives enlisting local fishermen to assist in waterborne cleanup efforts.[5] The federal government used privately manufactured oil dispersants in recovery operations.[6] Throughout this process, the public and private sector worked closely together to restore a sense of normalcy in the Gulf.

The Deepwater Horizon incident provides a large-scale illustration of an actively growing trend in emergency management and homeland security.[7] Public-private partnerships are a major issue of discussion in businesses and government agencies. However, this issue has received a much less thorough treatment in scholarly literature on homeland security. This is surprising, as public-private partnerships are perhaps the most dynamic and important subjects for homeland security practitioners today.

Public-private partnerships have been defined as collaboration between a public sector (government) entity and a private sector (for-profit) entity to achieve a specific goal or set of objectives.[8] This collaboration results in government-business relationships that include service contracts, supply chains, ad hoc partnerships, channel partnerships, information dissemination partnerships, and civic switchboard partnerships.[9] These partnerships have been discussed in narrow ways in the scholarly literature in related disciplines (such as public administration broadly understood) and some of the various subfields of homeland security (such as

emergency management or critical infrastructure protection).[10] For example, Yossi Sheffi suggests public-private partnerships are important for supply chain security under threat of international terrorism, a theme that David J. Closs and Edmund F. McGarrell repeat.[11] Others underscore that private sector participation is integral in critical infrastructure protection and homeland security.[12] Discussion of the private sector's role within other subfields, such as intelligence, cybersecurity, transportation security, public health, and hazard mitigation shows increasing understanding of businesses' impact on homeland security.[13]

Overall, however, the scholarly literature has not yet caught up to the practitioner understanding of public-private partnerships' prominence in homeland security.[14] This article begins to fill a gap in homeland security scholarship by identifying the essential role that public-private partnerships are now taking in homeland security, and by examining the implications of this transformative shift in the field. As we will see, public-private partnerships hold great promise, but also face significant obstacles that will need to be overcome. The article begins by tracing the development of public-private partnerships in homeland security. It then examines multiple subfields of homeland security and highlights the growing role of public-private sector partnerships in homeland security. The article concludes by discussing ongoing challenges that will need to be considered and addressed for public-private partnerships to be successful over the long term.

THE EMERGENCE OF PUBLIC-PRIVATE PARTNERSHIPS IN HOMELAND SECURITY

Government and businesses' roles in homeland security can be traced back to America's founding. For example, in the *Federalist Papers*, James Madison was careful to underscore the importance of the federal government in "times of war and danger," while not diminishing the importance of the states in periods of "peace and security."[15] In 1803, following a devastating fire in Portsmouth, New Hampshire, Congress authorized the suspension of federal bond payments for merchants affected by the disaster.[16] For the first time, the US government provided emergency relief for a community. Thus began an escalation of federal-level involvement that continues today, requiring close working relationships among the federal, state, and local levels of government, non-governmental organizations, and the private sector.

Public-private partnerships evolved in the nineteenth century, as various disasters prompted a re-calibration of government's role in emergencies. The Great Chicago Fire of 1871 burned a four square mile area in the southwestern part of the city, leaving one third of the city's population homeless.[17] While difficult to fathom today, the federal government's role was limited in recovery efforts. No appreciable amount of financial assistance flowed from Washington, DC to Chicago in the fire's aftermath.[18] Instead, the majority of recovery financing came from a combination of local and state governments, as well as charities and businesses.[19] The fire facilitated a shift in governmental involvement in emergency management. Subsequent twentieth-century disasters, including the 1906 San Francisco Earthquake and the 1927 Great Mississippi Flood, ratcheted up government support for response and recovery efforts.[20] Increasing amounts of funding changed hands between the public and private sectors to support post-disaster reconstruction.

From World War II through the end of the Cold War, public-private partnerships remained an essential element in national defense. Citizens were trained by the federal government to watch for enemy aircraft, assist in preparation for nuclear attacks, and direct air raid drills in public spaces.[21] At the same time, US manufacturing capacity adapted to emerging needs. Firms recycled and repurposed commercial products (e.g. rubber, steel, wood) to support the materiel needs of the armed forces. The private sector modified production to fill new demands. The Ford Motor Company, for example, built an entire complex to construct military aircraft.[22] Government and private sector

functions in national security evolved to meet wartime priorities.

Public-private sector partnerships continued to develop in the late twentieth and early twenty-first century. The Federal Emergency Management Agency (FEMA) was created during the Carter administration to consolidate disaster management functions previously scattered across the federal government.[23] Over time, businesses began taking a more expansive role in defense and security, from building out information technology (IT) infrastructure, to production of specialized equipment in law enforcement, to contracting out job functions in government offices.[24]

The September 11, 2001 terrorist attacks, Hurricane Katrina, and the Deepwater Horizon oil spill all highlight the prominence of public-private partnerships in what is today called homeland security. In all three of these disasters, the private sector worked closely with local, state, federal, and non-profit entities to respond to community needs. For example, following the 9/11 attacks, Verizon assumed a pivotal role in quickly rebuilding network infrastructure to re-open the New York Stock Exchange (NYSE).[25] In the aftermath of Hurricane Katrina, FEMA, in cooperation with the State of Louisiana, distributed $2.3 billion in public assistance funding to residents affected by the storm.[26] But Wal-Mart was instrumental in providing relief supplies – blankets, plastic tarpaulins, batteries, flashlights, water, and non-perishable food – to Gulf residents immediately following Katrina's impact.[27] Similarly, the Deepwater Horizon disaster required close coordination among government, non-profit, and private sector entities.[28] The American Red Cross sheltered and cared for displaced Gulf residents, while the private sector hired local fishermen to assist in cleanup efforts and worked with government agencies to stop the oil leak.[29] It is clear from these examples that businesses, alongside numerous government and non-governmental entities, now play an increasingly integrated role in homeland security.

In the following sections, we examine different initiatives and facets of homeland security, highlighting the role of public-private partnerships in each. Given the current expansive scope of public-private partnerships in homeland security as a whole, we limit our discussion to select federal-level public-private partnerships, which have enjoyed varying levels of success. However, it is important to note that homeland security includes efforts at the state and local levels, including fusion centers, non-profits, civic groups, professional associations, and individual citizens. As an "umbrella" concept, homeland security also touches on various subfields apart from those we discuss below, including immigration services, public health, and intelligence.[30] A comprehensive treatment of public-private partnerships in every aspect of homeland security is beyond the scope of this article. Nevertheless, the following discussion identifies some of the most significant trends in homeland security today.

CRITICAL INFRASTRUCTURE PROTECTION

With approximately 85 percent of the nation's critical infrastructure under private sector control, alliances between government and business are essential for homeland security.[31] The US Department of Homeland Security (DHS) creates coordination bodies to facilitate information exchange, planning, and situational awareness between the public and private sectors. The Office of Infrastructure Protection (OIP) within DHS works on threat and vulnerability analyses, national and local-level coordination with businesses and government agencies, and risk mitigation.[32] The OIP is responsible for coordinating information exchange and collaboration among six sectors: chemical; commercial facilities; critical manufacturing; dams; emergency services; and nuclear reactors, materials, and waste.[33] Given that private sector companies operate most of the facilities in these six sectors, public-private sector partnerships are indispensable to the OIP mission. The Critical Infrastructure Partnership Advisory Council (CIPAC), a strategic body, complements the OIP.

The CIPAC is the basic organizational framework in which government and private sector representatives exchange information and coordinate critical infrastructure

protection activities at the federal level. The CIPAC membership roster reads as a veritable "who's who" of government agencies and industry leaders nationwide. Firms in the CIPAC include such companies as BASF Corporation, the Trump Organization, Verizon, the Boeing Company, Google, and the US Oil and Gas Association. Government entities in the CIPAC include the United States Environmental Protection Agency, Department of Commerce, and Department of Justice.[34]

The CIPAC demonstrates substantial cooperation between public and private entities at the federal level related to critical infrastructure protection in homeland security. The existence of multiple coordination groups, as well as the presence of leading US businesses within them, underscores that public-private partnerships are integral to achieving homeland security objectives in critical infrastructure protection.

Despite the clear need that the CIPAC is designed to address, however, there are legitimate criticisms that can be leveled against this group. For example, some firms may sense that they are expected to share a significant amount of information with government, but do not get timely information back from government. One could also claim the CIPAC is overly government-centric, and does not give due consideration to business concerns. Moreover, firms may feel pressured to participate in order to avoid regulations that will force them to alter their business strategies.[35] Without diminishing the relevance of these concerns, the CIPAC nonetheless provides an important example of how public-private partnerships are enhancing critical infrastructure protection.

CYBERSECURITY

Information technology (IT) firms are essential in achieving national cybersecurity objectives. Well-known companies routinely partner with government to share information and collaboratively address IT challenges with homeland security implications. For example, the National Cyber Security Alliance (NCSA) is an organization that raises awareness about cybersecurity issues and empowers computer users to protect themselves against electronic threats.[36] Public-private partnerships are critical to the NCSA mission.[37] The NCSA board includes representatives from numerous national firms, including AT&T Services, Inc., Cisco Systems, Lockheed Martin, Microsoft, Google, Facebook, Bank of America, SAIC, and Visa.[38] Demonstrating linkages between the NCSA and federal government, the White House and DHS promoted the most visible NCSA initiative, known as National Cyber Security Awareness Month (NCSAM), in 2010.[39] The NCSA is an excellent example of public-private partnerships at work in the cybersecurity arena.

A recent hacking incident further highlights the interconnectedness of the public and private sectors in cybersecurity. In June 2011, Google publicly disclosed that individuals in China illegally accessed the personal email accounts of several senior US government officials.[40] This was allegedly done through use of "phishing," a method of fraudulently obtaining a user's information through fabricated emails asking for usernames, passwords, and related data. Google notified the FBI about the incident. The White House National Security Council (NSC), as well as DHS, followed up with Google to assess the incident's impact.[41] Understanding this attack's sources and methods provides greater knowledge of cybersecurity threats to public and private sector organizations. As this incident demonstrates, public-private sector partnerships, as well as information sharing, are critical to effective cybersecurity.

PORT SECURITY

America's ports are vital hubs of economic activity. In 2010 alone, nearly 263,000 metric tons of products passed through the port of Houston-Galveston, Texas.[42] During the same period, approximately 30 million passengers flew in and out of LaGuardia airport in New York City.[43] With such a high volume of goods and persons moving through US ports of entry, port security is an urgent priority. Against this backdrop, the Customs

Trade Partnership Against Terrorism (C-TPAT) is a government-business sector initiative that was created to enhance worldwide supply chain security.[44] Over 6,000 firms are certified through the C-TPAT program, meaning they enjoy close working relationships with United States Customs and Border Protection (CBP), are able to obtain government risk assessments of their supply chain, and can attend special government-sponsored supply chain security training sessions.[45] Programs like the C-TPAT are useful to homeland security in providing a broad administrative framework for regular public-private sector coordination.

On-the-ground security initiatives also impact this critical area of economic activity. The Transportation Worker Identification Credential (TWIC) program pre-screens workers with unescorted access to sensitive areas of America's ports to ensure they do not pose a security threat.[46] This arrangement enhances supply chain security, and helps achieve port security objectives. As of 2009, over 500,000 workers were enrolled in the TWIC program.[47]

Technologies in use at America's ports underline the importance of public-private sector partnerships. Consider the SAIC Vehicle and Cargo Inspection System (VACIS). The VACIS is a device that emits low-level radiation, providing a rapid view of cargo containers' contents – not unlike an X-ray machine.[48] The VACIS permits government and private sector officials to quickly evaluate if a given container poses a threat. Similarly, new luggage and passenger screening machines produced by L-3 and GE Security bolster protection in US airports.[49] While the latter continue to be the subject of vigorous public debate, it is worth noting that the so-called "full body scanners" are a private sector response to a governmental need – a clear example of public-private partnerships at work in homeland security.

Another public-private partnership in US airports is the Screening Partnership Program (SPP). Under this initiative, screening companies that meet certain qualifications carry out TSA-like duties at US airports. Additionally, individual airport executives may petition TSA for private sector employees to work as screeners in their facilities.[50] While the program's scope is limited – only sixteen airports are participating – the SPP is proving a helpful alternative to TSA screening.[51] Mark VanLoh, Director of Aviation for Kansas City, Missouri, noted in Congressional testimony that the SPP enhances flexibility in personnel use, allows for greater employee cross-training, and is more effective in dealing with non-performing workers.[52] Like the use of new, privately manufactured screening technologies in airports, the SPP illustrates the increasing presence of public-private partnerships in port security.

EMERGENCY MANAGEMENT

Emergency managers are increasingly engaged in all aspects of homeland security, including the previously discussed areas of critical infrastructure protection, cybersecurity, and port security.[53] But there is still a distinct area within emergency management that stands apart from these subfields: immediate, near-term response and recovery activities.[54] In such activities, FEMA has widely embraced the essential role of public-private partnerships.[55] Hurricane Katrina and the BP Deepwater Horizon oil spill illustrate why FEMA has embraced these partnerships.

Hurricane Katrina provides emergency management scholars and practitioners with a powerful lesson in what not to do. While popular blame for inadequate response initially fell upon FEMA, today researchers acknowledge systemic failures at all levels of government.[56] Despite these shortcomings, the private sector helped to address various government deficiencies in response and recovery efforts.[57] As the world's largest employer, Wal-Mart is proficient in logistics; that is, efficiently moving and distributing large quantities of goods over a wide geographic area. In anticipation of the storm's impact in 2005, Wal-Mart deployed trucks full of relief supplies to the Gulf region.[58] Clothing, diapers, toothbrushes, bottled water, ice, and non-perishable food items began rolling off Wal-Mart's fleet of trucks as the storm passed.[59] Government leaders took notice. A local official even suggested that FEMA use Wal-Mart's response as a model for its own efforts.[60] In

the midst of a significant disaster, Wal-Mart filled governmental gaps in disaster recovery capabilities.

Like Katrina, the 2010 Deepwater Horizon oil rig explosion and spill affected a vast geographic area in the Gulf of Mexico. The initial response involved hundreds of local, state, and federal government actors, as well as representatives from the non-profit and private sectors. British Petroleum, which was a responsible party for the spill, worked with the federal government and veterans of the Exxon Valdez oil spill to assess its impact and facilitate cleanup efforts.[61] The public sector lacked the necessary combination of equipment and technical expertise to shut off the flow of oil from the Gulf floor.[62] Thus BP, which drilled the leaking undersea oil well in the first place, cooperated with the public sector in carrying out the work of halting the spill. Public-private sector partnerships were integral to the overall response and recovery effort.

FEMA has made public-private partnerships a high priority, and leads a major national initiative to forge closer ties with the business community. The agency's regional offices, which cover all fifty states and US territories, house a private sector liaison officer charged with building alliances with firms.[63] FEMA Administrator Craig Fugate underscored the importance of the private sector for emergency management in recent public remarks:

> The private sector, from Fortune 500 companies to your local grocery store, is an essential member of the team.... The faster we can help stores and businesses get back on their feet [after a] disaster, the more effective the rest of the team can be in focusing our resources on helping disaster survivors in areas that don't yet have access to those goods and services. Growing strong working relationships between emergency managers and the private sector is a good business decision for everyone – it helps us better serve survivors, rebuild our communities and boost local economies.[64]

These comments illustrate the degree of buy-in within FEMA oriented toward building relationships with businesses. Public-private partnerships are beneficial in enhancing firms' preparedness for disaster, as well as connecting them with government partners in advance of a large-scale emergency. From FEMA's leadership team to personnel in regional offices, public-private sector partnerships carry tremendous importance. This emphasis has real-world impacts in disaster response.

BENEFITS OF PUBLIC-PRIVATE PARTNERSHIPS FOR HOMELAND SECURITY

Public-private partnerships can enhance hiring, resource utilization, specialization, cross-sector trust, and technological innovation. They are often able to cut across traditional bureaucratic divides within government. And they can enhance public protection in ways not possible for government or businesses acting independently. In this section, we will discuss each of these advantages, which suggest public-private partnerships will make ongoing contributions in homeland security.

HIRING

The private sector helps the public sector fill personnel needs more effectively than the government acting independently. Background checks for security clearances – a widespread requirement for prospective employees in the homeland security arena – are notoriously sluggish, sometimes taking years to complete.[65] This can create a significant time lag effect between an applicant being offered a position, and actually assuming that position. Compounding the issue, separate human resources-oriented activities are also necessary to bring a new employee into the homeland security workforce. These background investigation and human resources processes frequently overlap. Businesses operating within the homeland security space are often able to bring in new employees faster, and more efficiently, than the public sector.[66] This, in turn, creates value for the public sector. This arrangement serves firms' business interests, as well as governmental personnel needs.

Today, firms like SAIC, Booz Allen Hamilton, Northrop Grumman, and General Dynamics assign employees to work

shoulder-to-shoulder with government counterparts in public sector homeland security offices.[67] As a result, the homeland security workforce benefits from the hiring speed of the private sector. These private sector employees perform traditionally government functions, from intelligence analysis, to emergency planning, to protecting critical infrastructure. Thus, businesses can augment the total homeland security workforce faster than government acting alone. This provides a swift, cost-effective solution to the need for more personnel in homeland security positions.

RESOURCE UTILIZATION

Firms have a fixed amount of human and physical capital with which to achieve business objectives. Resource utilization refers to these assets being directed toward a specific aim, and in so doing, forgoing other opportunities. By orienting resources toward homeland security applications, businesses, government, and the public can benefit. Firms' sales increase. Government gains from privately produced products and services, and public safety is enhanced. Private companies forge an advantageous triangular relationship among these stakeholders by using their resources for homeland security purposes.

A case from aviation security illustrates how focused resource utilization can benefit businesses, government, and the general public. In 2008, the Transportation Security Administration (TSA) announced that it would permit airline passengers to keep laptops in bags at security checkpoints, provided the bags adhere to a certain x-ray transparency standard.[68] TSA subsequently released a Request for Information (RFI) about bag requirements: they should have no metal components, such as zippers, buttons, or snaps that could interfere with the ability of an x-ray to "see" the laptop's components. To this end, Aerovation – a luggage producer – responded by designing a "checkpoint friendly" laptop bag.[69] In public-private partnerships such as this, a firm re-allocates research and development resources in order to meet government homeland security objectives, while at the same time serving its business interests. In theory, this would increase operational efficiency and reduce wait times for airline passengers in security queues. For this innovation to be effective, however, TSA personnel would need to receive training to recognize these "checkpoint friendly" bags and allow passengers to keep their laptops in the bags. This training may not have sufficiently occurred yet. But through these and similar efforts to maximize resource utilization, public-private partnerships can work to achieve homeland security objectives.

SPECIALIZATION

By participating in homeland security activities, private sector actors develop specializations in functional areas, enhancing public sector performance.[70] This process, in turn, can permit government agencies to focus more upon mission-essential activities.[71] For example, in 2009, TSA announced the award of an IT services contract to CSC, a firm based in Falls Church, Virginia.[72] The $493 million, five-year deal includes provisions for designing, maintaining, and upgrading TSA's IT infrastructure over time.[73] Serving one agency's IT needs in such a comprehensive way means that CSC develops increasing familiarity with TSA systems, software, hardware, and requirements. This knowledge creates efficiencies over time. On the one hand, CSC is able to anticipate TSA's needs in a more effective fashion. On the other hand, TSA is freed to devote personnel and resources to other critical activities. Increasing specialization by CSC increases aggregate effectiveness, serving both private sector and public sector interests in a mutually beneficial manner.

BUILDING TRUST, INCREASING EFFECTIVENESS

Communication between the public and private sector can decrease officials' skepticism and mistrust of one another. Over time, repeated interaction and collaboration may actually build trust across the government-business divide. Whether developing plans for the future, or

responding to an emergency, trust is invaluable in fostering effective, mutually beneficial outcomes.[74] So public-private partnerships have what might be called a "softer" benefit – the construction of relationships themselves. It is challenging to quantify the value of a public-private sector relationship in the same way one might appraise a house or a car. But having excellent working relationships in place during routine operations, as well as crises, is invaluable.[75]

TECHNOLOGICAL INNOVATION

Public-private partnerships can also serve as catalysts for new technological innovations.[76] Two growing DHS initiatives stand out in their promotion of private sector innovation for homeland security-related challenges: the System Efficacy through Commercialization, Utilization, Relevance and Evaluation (SECURE) program, and its sister program, FutureTECH.[77] The SECURE program provides a pathway for private sector research and development (R&D) to occur without DHS financing the process itself. This departs from the traditional model of government-funded R&D, in that DHS provides clear requirements and design specifications to prospective vendors via public announcement. Firms, in turn, design technologies using their own resources, and attempt to sell them to the government at a competitive price.[78] This achieves public sector budgetary savings, permits firms to focus their R&D activities in a more effective way, and strives to deploy solutions in the short-term.

The FutureTECH program aims to enhance existing technologies to meet anticipated needs, taking a longer view of the innovation process. DHS identifies specific focus areas in which firms can continue to update and improve homeland security tools. These areas include detection of homemade explosives and waterborne improvised explosive devices.[79] By entering into a Cooperative Research and Development Agreement (CRADA) with DHS, firms can benefit from public sector subject matter experts who help to shape the design of a given product to meet precise requirements. In this sense, CRADA require close coordination between a DHS Science and Technology (S&T) officer and business representatives.[80] Both SECURE and FutureTECH can advance innovation for homeland security by focusing private sector R&D activities to meet public sector needs. Despite the great promise of public-private partnerships in homeland security, they also have a number of shortcomings. The article next addresses some of the ways in which public-private partnerships can fail, and outlines areas of governance in which public-private partnerships cannot function.

POTENTIAL SHORTCOMINGS OF PUBLIC-PRIVATE PARTNERSHIPS

Public-private partnerships can provide tremendous advantages for both government and businesses and can help the United States to meet its national security needs. There are, however, instances in which public-private partnerships are inappropriate due to the unique mandates of government. There have also been cases in which public-private partnerships fail to meet expectations or businesses do not comply with government recommendations. These issues demonstrate that while public-private partnerships are an important development in homeland security, they are imperfect, and there are certain roles that must be retained exclusively by the public sector.

THE LIMITS OF PUBLIC-PRIVATE PARTNERSHIPS

There are certain functions that must remain squarely within the public sector domain. The decision to hire and fire government employees is clearly a public sector responsibility – and must remain an authority of the public sector. To be clear, private sector-contractors can *assist* public sector entities in human resources-related processes, providing operational assistance, information, and expertise. But the actual *decision* to grow or shrink the workforce affects government in a deeply rooted way, and requires a government employee's signature. To do otherwise would risk undermining the political process, and would

create severe conflicts of interest in the very contracts that are approved for the private sector. This would present an unacceptable and unethical quandary for government.

Procuring resources, managing crises, and securing contracts are clear public sector responsibilities that should not be placed in private sector hands. For accountability reasons, businesses cannot control public sector budgets. Firms can provide advice on budgeting decisions for government, but they cannot actually approve them. In order to avoid conflicts of interest, signatures on procurement orders must remain those of government employees. The public sector also relies on contracts for provision of goods and services, and government employees must sign those contracts. Outsourcing this function effectively places control of public dollars in private hands, undermining society's trust in government's stewardship of tax revenue. Similarly, crises often call for public safety-related decisions about the movement of people and resources. The democratic state's first duty is to protect its citizens, and it naturally follows that these types of choices – sending another police officer, opening and closing evacuation shelters – must ultimately be directed by government employees.

UNMET EXPECTATIONS AND COST OVERRUNS

Without proper management, contractual public-private partnerships can fail for many reasons, including unmet expectations and cost overruns. One component of the DHS Secure Border Initiative, widely known as the "Virtual Fence," provides an excellent example of how this can happen. This initiative was to consist of a series of surveillance radars, cameras, and sensors to monitor the United States-Mexico border.[81] But the region's harsh terrain caused the equipment to malfunction, and the different technologies that made up the Virtual Fence were challenging to integrate.[82] These issues would be problematic enough on their own, but the project also ran into cost overruns. Estimates for 2005 showed it would cost $7 billion for the fence to cover the *entire* 2,000-mile US southern border.[83] But a pilot test of Virtual Fence technology cost $1 billion to cover *fifty-three miles of the border* – just 2 percent of the total project.[84] In January 2011, DHS canceled the Virtual Fence project, noting that it "'did not meet current standards for viability and cost effectiveness.'"[85] The Virtual Fence project demonstrates how contractual partnerships between government and business can fall apart. Unmet expectations, poor execution, and spiraling costs doomed the initiative. This underscores the importance of effective and transparent management of contracts in public-private partnerships.

APPEARANCE VERSUS REALITY OF COOPERATION

In 2008, teams of government scientists identified a cyber vulnerability in the US Bulk Power System (BPS), drafted a list of remedies to address the vulnerability, distributed the list to electrical companies, and provided a timeline for implementation. Despite these proactive steps, and despite the apparent mutual interest in addressing these vulnerabilities, in reality there was minimal private sector compliance with these recommendations.[86] This example shows differences between public and private sector approaches to cybersecurity. It also suggests that, despite the appearance of public-private sector cooperation on cybersecurity initiatives, actual cooperation may be less common than one imagines.[87]

Differing approaches to critical infrastructure protection can also be a source of discord between the public and private sectors. Marc de Bruijne and Michel van Eeten point out that while government and business both agree on the importance of critical infrastructure protection, this consensus can be remarkably shallow.[88] Another scholar notes that any business executive who suddenly announced he was increasing security spending by 25 percent for the good of the nation would almost certainly be fired.[89] Government appeals to morals, patriotism, or civic responsibility quickly lose their luster when they begin to eat into a firm's bottom line.[90] Businesses may publicly promote their commitment to security, but behind closed doors, there is an

upper limit to firms' security expenses. Beyond that limit, genuine (rather than rhetorical) investment in security can be difficult to come by.

These examples provide a cautionary tale for the public and private sectors. Public-private partnerships provide great value for both government and businesses. But there are fundamental limits to what public-private partnerships can do, and they sometimes fail to deliver as expected. In the following section, we discuss ongoing challenges for public-private sector partnerships for homeland security.

ONGOING CHALLENGES FOR PUBLIC-PRIVATE PARTNERSHIPS IN HOMELAND SECURITY

As the examples in the previous sections demonstrate, public-private sector partnerships are transforming the entire discipline of homeland security, but there are potential pitfalls from such partnerships as well. This trend toward public-private partnerships can therefore provide tremendous benefits, but it can also create organizational pathologies, long-term challenges, and many uncertainties. Several of the challenges discussed below are already emerging, while others may arise as public-private partnerships continue to evolve in homeland security. Scholars and practitioners will need to be mindful of these issues as the discipline of homeland security matures.

EVOLVING GOVERNANCE AND RESPONSIBILITY

In public-private partnerships, traditional hierarchy yields to collaborative engagement. In addition to more traditional skills in overseeing and directing, managers will increasingly need to connect and coordinate the shared activities, resources, and capabilities of a host of new organizations and individuals. This arrangement suggests a shift in management and organizational accountability, raising salient legal and ethical questions.

Management and Accountability

Over time, public-private partnerships will undoubtedly affect the skill sets required for public sector managers. As noted, supervisors will be more valued for their ability to foster collaboration among personnel and organizations than for hierarchical management skills. This transition toward a more coordinated public sector management is known as "networked governance."[91] Like most organizations broadly concerned with public safety, homeland security agencies have historically self-organized in a paramilitary-style, top-down structure. Networked governance suggests a flattening of this organizational structure over time.

In this sense, the need for collaborative management will ultimately drive changes in hiring and promotion practices. The spoils will go to those who can effectively communicate and coordinate the actions of many disparate actors – not to those who can simply command. The coordination-oriented manager's skills, values, and outlook then trickle down into the rest of the organization, eventually changing it from within. This adjustment from a hierarchical to a more horizontal organization would require excellent planning and execution by both public and private sector leaders to ensure continuing effectiveness. These potential organizational changes also connect with questions of accountability.

Who is calling the shots now? With more firms entering the homeland security space, delicate management questions become salient: is it ever appropriate for a private sector employee to direct a government civil servant to perform specific work functions? Under what circumstances might this hold true? Two members of Congress recently voiced reservations about this idea, underlining that it is government, not business, that must be ultimately be "in charge" of homeland security.[92] Is this always the case? What protections can government devise to ensure that it continues to direct homeland security operations, even with a substantial private sector presence? None of these questions are easy to answer. As the field of homeland security moves forward, these issues will continue to present difficult

challenges for governmental and private sector specialists.

Legal and Ethical Challenges

Government can expand its presence and influence via public-private partnerships in homeland security. This carries legal implications worth considering. Jon D. Michaels refers to a phenomenon he calls "deputizing," in which the private sector, along with citizens and other organizations, serve as a force multiplier for homeland security purposes. He holds that this arrangement can place homeland security activities on ambiguous legal and regulatory ground.[93] For example, private security officers now outnumber police officers three to one in the United States.[94] Retaining private security firms can be financially advantageous for government. Guarding federal buildings or large-scale events increases long-term fixed costs for law enforcement agencies. Retaining firms to temporarily perform these duties saves time and money. It permits law enforcement agencies to reallocate resources to other priorities. Despite these benefits, this type of public-private partnership also raises serious constitutional questions.

There is a vigorous debate related to the legal powers of private security officers.[95] Private security firms may or may not act as government agents. Depending upon context, they may conduct limited searches of persons. It is not yet clear if these searches are uniformly constrained by the US Constitution's fourth and fifth amendments.[96] Similarly, there are concerns about the chain of command within private security companies. To whom do private security officers ultimately report, and to whom are they ultimately accountable – a government authority or a business? And how does this distinction affect the way they carry out their duties? These issues blur the legal boundaries between business and government. The implications here are significant. Use of private firms for law enforcement-like functions raises legal and organizational questions that must be balanced against financial advantages.[97]

Despite these challenges, proponents of public-private partnerships can point to a number of strategic advantages. Government can exert its influence through businesses in a beneficial way. Putting aside discussion of private security firms, consider that privately produced technologies scan citizens for explosives and contraband in airports. Scholars in emergency management, public administration, operations management, and urban affairs highlight the benefits of private sector participation in disaster response.[98]

Skeptics, however, can be apprehensive about the degree to which the state intrudes on private lives via public-private partnerships: surveillance cameras can capture one's every move in public; cell phone intercepts erase the notion of private information exchange; and invasive airport security screening is often interpreted as eroding individual liberties and initiating a slow shift toward more widespread draconian security measures. These are valid sources of concern and require clear responses from government and businesses.

The shifting of organizational and technological responsibilities to the private sector also prompts related questions about liability. If private sector technologies do not deliver, what does this mean from a legal perspective? For example, let us assume a sophisticated network of chemical sensors fails to detect a toxic agent in the Washington, DC-area Metro system. Who gets the blame? Absent indemnification agreements, can government sue the firm? Is it more appropriate for citizens' litigation to be directed toward government or the business itself? Joint action means sharing accountability for successes and failures in homeland security. Security, however, is the state's first duty. It is government, not business, that must ultimately make critical decisions and take decisive actions in homeland security. How to reconcile these positions? Does public-private sector collaboration mean mutual or individual culpability for mistakes? These lines of inquiry require further investigation. Additional liability questions arise when the public sector lacks the knowledge to make informed judgments and decisions.

The Deepwater Horizon oil rig explosion and spill show what can happen when government regulation breaks down. No public sector agency had a complete view of

the problem, nor the expertise and equipment needed to solve it. Might the privatization of airport security functions create a similar dilemma? For instance, what happens if an explosive device slips through a security checkpoint, ultimately downing a commercial airliner? Will government be able to adequately explain to the public why the lapse occurred, and how to remedy it? Contractual consequences under this scenario prove worrisome, as well. If government homeland security capacity is "hollowed out" via outsourcing to private firms, then homeland security can be held hostage to the private sector.[99] Public sector agencies must guard against this possibility through diversifying contracts, incentivizing competition among private sector actors, and maintaining a minimum baseline of expertise in core competencies.

Increasing Need for Transparency

Public-private partnerships also raise concerns related to transparency, which refers to two distinct, yet related concepts. The first is governmental transparency, specifically agency reporting to Congress. The second is agency and business reporting to the general public. Both areas of transparency pose significant challenges. Legislative oversight is problematic for DHS. As of July 2012, over 100 committees or subcommittees address matters related to departmental operations.[100] Businesses in the homeland security space compound this challenge. For example, are private sector representatives held to the same standards of ethics and accountability as their public sector counterparts? If Congressional oversight of DHS is fractured, how effective is oversight of firms' activities? Robust monitoring of public and private sector homeland security actions is essential. Lawmakers will need to ensure that oversight evolves in parallel with the trend toward public-private partnerships in homeland security.

A second challenge relates to decreasing transparency in the privatization of national security functions.[101] Among the many volumes on the evolution of homeland and international security since 9/11, Dana Priest and William M. Arkin provide the most expansive treatment of this topic.[102] They raise several salient observations about the expansion of post-9/11 government contracts. Under the Bush administration, they argue that Congress was able to substantially grow government for national security reasons via private contracting.[103] At the same time, they note that Congress tried to create the appearance government was not growing – presumably for political reasons.[104] There is also a span of control issue; top government officials admit the number of national security programs involving businesses has become unmanageable.[105] Cozy relationships between government and business representatives are uncomfortable for Priest and Arkin. These are best exemplified in the lavish conferences in which public and private sector officials mingle over expensive drinks, dinner, and entertainment.[106] The purpose of these conferences is to build business relationships between the public and private sectors.[107] To Priest and Arkin, though, they appear to erode the sense of accountability and due diligence needed in government contracting. They argue that these trends are ultimately damaging to national security.

To a limited extent, we agree with Priest and Arkin's thesis. It is true that ineffective program management is fiscally irresponsible and is conducive to misdirection and error. It is also important for the public to know that program oversight is in place and that outcomes are being measured in a meaningful way. But the suggestion that there is something sinister here is unfounded. Priest and Arkin gloss over the efficiencies that public-private partnerships can create. As we have argued in this article, public-private partnerships can improve hiring, resource utilization, specialization of labor, and technological innovation. In public-private partnerships, firms seek profits, and government scales in a way that would be impossible if acting independently. In this sense, public-private partnerships enhance efficiencies in ways that government cannot produce on its own. This is not foul play; it is a case of rational action by both the public and private sectors.

In light of these challenges, the public and private sectors would be well served by showing why government-business

partnerships are necessary, and how their existence benefits homeland security. A positive example of such efforts would be the work of Thomas Cellucci, former chief commercialization officer at DHS, who publishes extensively on the benefits of public-private partnerships for government, businesses, and taxpayers.[108] For example, he makes the case for public-private partnerships, particularly in the context of the DHS SECURE program:

> The products that are developed through [the SECURE program] (even the ones that were not purchased by DHS) can be offered to other private sector entities, such as airport security, school and university security, and security for professional sports and concerts, many of whom support the defense of critical infrastructure and key resources nation-wide. There is then an increase in public safety and security, all while the private sector, public sector and taxpayer benefit from the partnership.[109]

In clear language, Cellucci demonstrates the benefits of public-private partnerships for businesses, government, and the public. Similar government reporting and explanation will help allay concerns over the necessity of public-private partnerships.

INCENTIVIZING PRIVATE SECTOR PARTICIPATION

Public-private partnerships are easy when both government and business immediately benefit. In a service contract, for example, government is able to procure a needed good or service, and a company's bottom line increases. But what happens when government needs the private sector – such as in obtaining data on critical infrastructure vulnerabilities – but the private sector lacks incentives to cooperate with government? Working with public sector officials, while helpful for homeland security purposes, eats into firms' overhead expenses. Collecting data on a business' vulnerabilities requires time, labor, and material costs that are not profit-oriented. There is a financial disincentive for businesses to assist government in this case. This problem can be compounded if a company's competitor decides not to cooperate with government in the same way. The competitor can potentially provide services at a lower cost than the company that decides to "play ball."[110]

Public-private partnerships can also create proprietary and legal risks for companies. What assurances, for example, do firms have that government will protect proprietary or sensitive information? The WikiLeaks scandal underlines that classified national security information can quickly enter the public domain, damaging the national interest.[111] It is reasonable to suggest that firms' confidential information could be subject to similar disclosures while in government custody. Such leaks can rapidly erode a business' competitive edge. Other firms offering similar products or services gain valuable business intelligence from these data. Private sector actors may find their trust in government undercut by information leaks. *In extremis*, private sector cooperation with government on critical infrastructure protection could lead to a business' outright failure through breaches of confidentiality.[112]

Regulatory questions become salient in exchange of sensitive information. Can businesses be targeted for punitive measures if they unwittingly turn over damaging information about their activities? There is a potential moral dilemma in businesses providing the government information on facilities and operations. Countless firms are subject to government regulation. In cooperating with government for homeland security purposes, firms potentially risk shining a light on unsavory or illegal business practices. Government and businesses may need to develop clear guidelines on exchanging potentially damaging information for homeland security purposes.[113]

How to promote private sector engagement under these challenging circumstances? Orszag argues tax breaks make bad policy; they can provide benefits to firms that would have invested in security measures anyway, increasing the firms' budgetary costs but not actually providing extra security.[114] Moreover, he argues that tax credits do not distinguish between high-risk and low-risk sectors – for example, chemical plants versus shopping malls – when they logically should.[115] Similarly, James A. Lewis points out that voluntary cooperation from firms in the cybersecurity arena is

inconsistent with other sectors of homeland security that require strict government regulation, including banking, commerce, and transportation.[116] Both of these examples show the difficulty of balancing regulatory tools and market forces to engage businesses in homeland security efforts. Scholars, public sector practitioners, and private sector representatives therefore aid homeland security by seeking new ways to encourage businesses' participation. Developing a menu of policy options to increase firms' involvement in homeland security will be an important priority for the years ahead.

POLITICS, BUDGETS, AND LONG-TERM PLANNING

Politics, budgets, and long-term planning are interconnected in the homeland security context. The electoral process can impact homeland security in significant ways. Representatives' thinking about homeland security leads to adjustments in budgets and policies. While hawkish elected officials may choose to funnel more resources toward homeland security, others might elect to trim budgets and focus more narrowly on specific strategic priorities. These shifts can alter, or even undermine, long-term planning in homeland security. The ongoing global financial crisis also impacts government and businesses' approaches to homeland security. In this dynamic environment, the public and private sectors must effectively plan for future threats and challenges in homeland security.

Politics affect public-private partnerships. For example, Connecticut Senator Joseph Lieberman recently expressed concern that private employees, rather than government officials, are making critical decisions at DHS.[117] After TSA halted an initiative in 2011 to expand businesses' roles in airport security, Florida Congressman John Mica vowed to investigate the decision, noting "Nearly every positive security innovation since the beginning of TSA has come from the contractor screening program."[118] When politics challenges businesses in this way, firms can become increasingly reluctant to enter the homeland security space. Winning government contracts comes at significant overhead cost; research and development, labor, and negotiation expenses come out of firms' bottom lines. It makes little sense for firms to invest in homeland security if elected officials (vis-à-vis bureaucrats, with whom those firms routinely interact) can abruptly restrict or halt business. When companies hesitate to enter the homeland security arena, this reduces the size of the private sector homeland security market. With less competition in the game, firms that stay at the table can charge higher fees for government contracts. The public sector is left with a diminishing pool of choices for outsourcing, becoming increasingly beholden to a small number of businesses for products and services. Of course, with stifled competition, any cost increases are passed on to taxpayers. Political forces can profoundly change government-business partnerships in homeland security.

Global financial markets influence agency budgets. Recently, the worldwide economic recession reduced the number of private contractors performing traditionally governmental functions. A 2009 DHS initiative began to examine the appropriate balance of government workers and contractors within the department.[119] By April 2011, DHS cut 3,200 contractor positions, converting them into 2,400 government jobs.[120] The DHS 2012 fiscal budget includes provisions to convert another 1,881 positions from the private sector to the public sector.[121] Current trends away from private contracting are not limited to DHS. In January 2011, then-Secretary of Defense Robert Gates announced an initiative to drastically thin the ranks of contractors within the Department of Defense, as well:

> [As] I have said before, this department has become far too reliant on contractors to perform functions that should either be done by full-time employees or, in some cases, to staff activities that could – and should – be discontinued.... Overall, we will cut the size of the staff support contractor cadre by 10 percent per year for three years and realize nearly $6 billion in total savings.[122]

Reduced budgets affect public-private partnerships in homeland security, and will

continue to change amidst efforts to revive the world's economies.

Businesses now face an uncertain future. Some firms find themselves in "survival mode," trimming staff because of operating costs. In 2011, icons of American industry with links to homeland security, including GM (official vehicles), Caterpillar (construction and debris removal equipment), Sprint Nextel (communications), and Home Depot (disaster recovery supplies) cut thousands of positions.[123] When firms trim budgets, they have fewer resources (human and physical capital) to produce products and deliver services. This means the range of possible business relationships for homeland security narrows. Complicating matters, when government budgets shrink, firms can find it difficult to plan for the future; revenue streams become dynamic, and this year's homeland security cash cow may not be there next year. These circumstances create a vicious circle effect for businesses. Government budget cuts eliminate business for the private sector, forcing firms to scale down. This trimming could restrict the ability of companies to operate in the homeland security space. For both the public and private sectors, then, there is an aggregate shrinking effect in homeland security capacity. This creates hardships for both sectors. Government may not be able to guarantee a consistent level of public protection, while businesses may find it difficult to sustain operations and grow effectively. Both sectors are burdened by the global financial crisis.

In light of these trends, government and businesses must effectively plan for the future of homeland security. Converting private sector jobs to public sector positions requires focused government effort. Competencies, skills, and knowledge must smoothly transfer from business to government hands. Yet there is little financial incentive for businesses to cooperate in this process. Doing so contradicts their self-interests. After all, firms in the homeland security space make money from government contracts. For its part, government may find it has lost the capacity to perform in certain areas of homeland security. This may be due to over-reliance on the private sector – the "hollowing out" of government mentioned above. Further complicating this picture, there is a continual flow of homeland security officials between the public and private sectors. Firms' employees may join government to gain excellent benefits, promotion potential, and predictable work schedules. Public sector employees can gravitate toward the private sector for substantially higher salaries and fewer bureaucratic constraints. Downplaying or ignoring these trends hinders effective long-term planning in homeland security. Business and government officials should carefully consider these factors in their respective plans for the future.

CONCLUSIONS

This article shows that public-private partnerships are now integral to homeland security as a whole – not just its subfields. Government and business cooperation can provide distinct advantages in hiring, resource utilization, specialization, and technological innovation. These partnerships also have significant implications for management practices, legal and ethical challenges, transparency, building private sector participation, politics, budgeting, and long-term planning. Future studies will need to examine other critical issues that become relevant as public-private partnerships continue.

For example, what is the effect of decreasing the number of private contractors working in homeland security? This may increase cost savings, but also degrade operational efficiencies. In an era of shrinking budgets and rising demands on security officials, it may be that reducing the privatization of homeland security also diminishes effectiveness. This may be fiscally healthy, in other words, but damaging from a security standpoint. Scholars can benefit from critically examining the effects of private sector personnel reductions on homeland security.

As public-private partnerships continue to grow, there is also a compelling need for scholarly investigation of effective management and successful outcomes in public-private partnerships. Moreover, academics can make valuable contributions

in studying actions, initiatives, and special projects that add value to public-private partnerships in homeland security. Researchers can work with industry leaders to enhance tools to share best practices. For example, an existing DHS website designed for sharing best practices – Lessons Learned Information Sharing – could provide an excellent starting point for this cross-sector collaboration.[124] Scholars are in an ideal position to make analytical connections and provide a theoretical framework for successful management of public-private partnerships.

From a theoretical perspective, public-private partnerships also raise important questions. Our understanding of homeland security is increasingly linked with concepts, rather than agencies. Flexibility, adaptability, and resilience have become hallmarks of homeland security programs at all levels of government. Incorporating these concepts into agencies' plans and operations helps to produce favorable outcomes. But do public-private partnerships sufficiently align with these concepts? Some might argue this is clearly true – contracting represents a "flexible" way to expand homeland security staffing. However, others could demonstrate that this is hardly the case; contracting can increase government dependency on the private sector, reducing organizational flexibility. These questions merit additional examination.

There is an enduring need to maintain capabilities in homeland security. From 9/11, to Hurricane Katrina, to the 2011 Joplin, Missouri tornado, natural and man-made disasters continue to loom large in the national conscience. The private sector will continue to play a major role in addressing similar threats in the future. Public sector agencies benefit from working with businesses to strengthen US resilience. There will be an ongoing need for scholars to provide insights as these trends continue to develop.

ABOUT THE AUTHORS

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.*

Austen D. Givens *teaches graduate courses on terrorism and emergency management at Utica College in Utica, NY. He previously served as director of emergency management at Christopher Newport University (CNU) in Virginia. Austen is a fellow with Virginia Commonwealth University's (VCU) National Homeland Security Project, holds a master's degree in Homeland Security and Emergency Preparedness from VCU, and studied international relations in the Woodrow Wilson Department of Politics at the University of Virginia. He has worked with the Department of Homeland Security, the Office of the Secretary of Defense at the Pentagon, and the Virginia Fusion Center. He can be reached at adgivens@utica.edu.*

ACKNOWLEDGMENTS:

The authors wish to thank Joe Giordano, Shanna Van Slyke, and Greg Walsh for their helpful comments on earlier versions of this article.

---

[1] Homeland Security Television, *Public-Private Partnerships for Homeland Security*, (Washington, DC: August 3, 2011) online video, http://www.youtube.com/watch?v=ka6dgMxLrJI.

[2] British Petroleum, *Deepwater Horizon: Accident Investigation Report*, September 8, 2010, 29; National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, *Deep Water: The Gulf Oil Disaster and The Future of Offshore Drilling – Report to the President*, January 2011, http://www.oilspillcommission.gov/sites/default/files/documents/DEEPWATER_ReporttothePresident_FINAL.pdf.

[3] National Commission on the BP Deepwater Horizon Oil Spill, *Deep Water*, 173.

[4] Ibid., 1-398.

[5] Ibid., 140.

[6] Ibid., 145.

[7] Throughout this article, the term "homeland security" refers to "actions taken at every level (federal, state, local, private, and individual citizen) to deter, defend against, or mitigate attacks within the United States, or to respond to other major domestic emergencies." See Dave McIntyre, "What Is Homeland Security? A Short Story," n.d., accessed April 12, 2012, http://www.homelandsecurity.org/bulletin/ActionPlan_WhatIsHLS.htm.

The International Association of Emergency Managers (IAEM) defines emergency management as "the managerial function charged with creating the framework within which communities reduce vulnerability to hazards and cope with disasters." Our use of the term "homeland security" also includes emergency management.

See International Association of Emergency Managers, *Principles of Emergency Management Supplement*, (September 11, 2007), 4, http://www.iaem.com/publications/documents/PrinciplesofEmergencyManagement.pdf.

[8] Robert A. Beauregard, "Public-Private Partnerships as Historical Chameleons," in *Partnerships in Urban Governance: European and American Experience*, ed. Jon Pierre (London: MacMillan Press, 1997), 52–70; Pauline V. Rosenau, ed., *Public-Private Policy Partnerships* (Cambridge, MA: MIT Press, 2000); Peter V. Schaeffer & Scott Loveridge, "Toward an Understanding of Types of Public-Private Cooperation," *Public Performance & Management Review* 26, no.2 (2002): 169–189; Bonnie L. Regan, *Enhancing Emergency Preparedness and Response: Partnering with the Private Business Sector* (master's thesis, Naval Postgraduate School, December 2009), 14–15.

[9] Stephen Goldsmith and William D. Eggers, *Governing By Network: The New Shape of the Public Sector*, (Washington, DC: Brookings Institution, 2004), 69–70.

[10] Goldsmith and Eggers, *Governing By Network*; Beauregard, "Public-Private Partnerships as Historical Chameleons," 52–70; Regan, *Enhancing Emergency Preparedness and Response,* 14–15; Yossi Sheffi, "Supply Chain Management Under the Threat of International Terrorism," *International Journal of Logistics Management* 12, no. 2 (2001): 1–11; David J. Closs and Edmund F. McGarrell, "Enhancing Security Throughout the Supply Chain," Special Report Series (IBM Center for the Business of Government, 2004)

[11] Sheffi, "Supply Chain Management Under the Threat of International Terrorism," 1–11; Closs and McGarrell, "Enhancing Security Throughout the Supply Chain," 1–56.

[12] Stephen E. Flynn and Daniel B. Prieto, "Neglected Defense: Mobilizing the Private Sector to Support Homeland Security," Council Special Report No. 13 (Council on Foreign Relations, March 2006); Phillip Auerswald, Lewis Branscomb, Todd La Porte, and Erwann Michel-Kerjan, eds., *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability* (New York, NY: Cambridge University Press, 2006); Myriam Cavelty and Manuel Suter, "Public-Private Partnerships Are No Silver Bullet: An Expanded Governance Model for Critical Infrastructure Protection," *International Journal of Critical Infrastructure Protection* 2, no. 4 (2009): 179–187.

[13] Ashton B. Carter, "The Architecture of Government in the Face of Terrorism," *International Security* 26, no. 3 (2001–2002): 5–23; Charles A. Stone and Anne Zissu, "Registered Traveler Program: The Financial Value of Registering the Good Guys," *Review of Policy Research* 24, no. 5 (2007): 443–462; Crystal Franco, Eric Toner, Richard Waldhorn, Thomas Inglesby, and Tara O'Toole, "The National Disaster Medical System: Past, Present, and Suggestions for the Future," *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 5, no. 4 (2007): 319–325; Mary C. Comerio, "Public Policy for Reducing Earthquake Risks: A US Perspective," *Building Research and Information* 32, no. 5 (2005): 403–413.

[14] Government documents, vis-à-vis the homeland security literature, place great emphasis upon the role of the private sector in homeland security operations. This reflects a greater understanding of public-private partnerships' importance for homeland security in the practitioner domain than in the scholarly domain, where knowledge is more limited. See The White House, *National Security Strategy* (Washington, DC: May 2010); U.S. Department of Homeland Security, *National Response Framework* (Washington, DC: 2008), 18–20; ----, *National Incident Management System* (Washington, DC: 2008), 15-16; ----, *National Infrastructure Protection Plan* (Washington, DC: 2009); ----, *National Cyber Incident Response Plan* [Interim Version] (Washington, DC: September 2010); ----, *National Disaster Recovery Framework* (Washington, DC: September 2011).

[15] James Madison, No. 45: "The Alleged Danger from the Powers of the Union to State Governments considered for the Independent Journal," in *The Federalist Papers* (Yale Law School: The Avalon Project, 2008), http://avalon.law.yale.edu/18th_century/fed45.asp.

[16] Suburban Emergency Management Project, "History of Federal Domestic Disaster Aid Before the Civil War," July 24, 2006, http://www.semp.us/publications/biot_reader.php?BiotID=379.

[17] Elizabeth Witham and Steve Bowen, *Financing Recovery from Catastrophic Events: Final Report* (Washington, DC: Homeland Security Institute March 30, 2007), http://www.homelandsecurity.org/hsireports/Financing_Recovery_HSI_final_report.pdf, 22.

[18] Ibid., 24.

[19] Ibid., 21–26.

[20] Ibid., 27–38.

[21] Homeland Security National Preparedness Task Force, "Civil Defense and Homeland Security: A Short History of National Preparedness Efforts," (Washington, DC: FEMA, September 2006), http://training.fema.gov/EMIWeb/edu/docs/DHS%20Civil%20Defense-HS%20-%20Short%20History.pdf.

[22] Jenny Nolan, "Willow Run and the Arsenal of Democracy," *The Detroit News*, January 28, 1997, http://apps.detnews.com/apps/history/index.php?id=73&category=locations.

[23] Federal Emergency Management Agency, "FEMA History," August 11, 2010, http://www.fema.gov/about/history.shtm.

[24] For example, see Apptis, Inc., "About Us," accessed March 4, 2012, http://www.apptis.com/about/default.aspx; Taser, "About Taser," accessed March 12, 2012, http://www.taser.com/about-taser; Raytheon, "Raytheon Homeland Security," accessed March 12, 2012, http://www.raytheon.com/capabilities/homeland/.

[25] Verizon, "World Trade Center – A Year Later," accessed January 27, 2012, http://newscenter.verizon.com/kit/wtc2/.

[26] Federal Emergency Management Agency, "Louisiana Katrina/Rita Recovery," n.d., accessed June 8, 2012, http://www.fema.gov/pdf/hazard/hurricane/2005katrina/la_progress_report_0810.pdf, 1.

[27] Michael Barbaro and Justin Gillis, "Wal-Mart at Forefront of Hurricane Relief," *The Washington Post*, September 6, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/09/05/AR2005090501598.html.

[28] Austen Givens, "Deepwater Horizon Oil Spill Is An Ominous Sign for Critical Infrastructure's Future," *Emergency Management*, May 27, 2011, http://www.emergencymgmt.com/disaster/Deepwater-Horizon-Oil-Spill-Critical-Infrastructure-052711.html?page=1&.

[29]American Red Cross, "Gulf Coast Beach Safety," June 21, 2010, http://www.redcross.org/portal/site/en/menuitem.1a019a978f421296e81ec89e43181aa0/?vgnextoid=886d19439f749210VgnVCM10000089f0870aRCRD; Restorethegulf.gov, "Technical Assistance: Guide to Private/Non-profit programs," accessed June 6, 2012, http://www.restorethegulf.gov/node/4621#redcross; Robbie Brown, "Fishermen Sign On to Clean Up Oil," *New York Times*, April 30, 2010, http://www.nytimes.com/2010/05/01/us/01marsh.html.

[30] Dale Jones and Austen Givens, "Public Administration: The Central Discipline in Homeland Security," in *The Future of Public Administration, Public Management, and Public Service Around the World: The Minnowbrook Perspective*, eds. Rosemary O'Leary, David Van Slyke, and Soonhee Kim (Washington, DC: Georgetown University Press, 2011), 67–78.

[31] "Critical Infrastructure Sector Partnerships" (Washington, DC: U.S. Department of Homeland Security, 2011), http://www.dhs.gov/files/partnerships/editorial_0206.shtm.

[32] Ibid.

[33] "More About the Office of Infrastructure Protection" (Washington, DC: U.S. Department of Homeland Security, 2010), http://www.dhs.gov/xabout/structure/gc_1189775491423.shtm.

[34] "Council Members, Critical Infrastructure Partnership Advisory Council" (Washington, DC: U.S. Department of Homeland Security, 2012), http://www.dhs.gov/files/committees/editorial_0848.shtm.

[35] The authors thank an anonymous reviewer for this suggestion.

[36] "About the National Cyber Security Alliance," National Cyber Security Alliance, n.d., accessed January 26, 2012, http://www.staysafeonline.org/about-us/about-national-cyber-security-alliance.

[37] Ibid.

[38] National Cyber Security Alliance, "Board Members," n.d., accessed April 4, 2012, http://www.staysafeonline.org/about-us/board-members.

[39] "National Cyber Security Awareness Month 2010 Results in Brief" (National Cyber Security Alliance, January 14, 2011), http://www.staysafeonline.org/sites/default/files/resource_documents/NCSAM%202010%20Short%20Report011411.docx.

[40] Cecilia Kang and Ellen Nakashima, "Google Says Hackers Based in China Accessed U.S. Officials' Gmail Accounts," *Washington Post*, June 1, 2011, http://www.washingtonpost.com/business/technology/google-says-hackers-based-in-china-accessed-us-officials-gmail-accounts/2011/06/01/AGwgRmGH_story.html.

[41] Ibid.

[42] "U.S. Waterborne Foreign Trade 2010: RANKING OF U.S. CUSTOMS DISTRICTS BY VOLUME OF CARGO" (American Association of Port Authorities, November 23, 2011), http://aapa.files.cms-plus.com/Statistics/U.S.%20WATERBORNE%20FOREIGN%20TRADE%202010%20RANKING%20OF%20U.S.%20CUSTOMS%20DISTRICTS%20BY%20TRADE%20VOLUME.pdf.

[43] "LaGuardia Airport Facts and Information" (Port Authority of New York and New Jersey, 2012), http://www.panynj.gov/airports/lga-facts-info.html.

[44] "C-TPAT Overview" (U.S. Customs and Border Protection, December 13, 2007), http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/what_ctpat/ctpat_overview.xml.

[45] Adboulaye Diop and David Hartman, "Customs-Trade Partnership Against Terrorism Cost-Benefit Survey" (U.S. Customs and Border Protection, August 2007), 3, http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/what_ctpat/ctpat_cost_survey.ctt/ctpat_cost_survey.pdf; C-TPAT Overview.

[46] "Federal Port Security Credential Now Available Nationwide" (Transportation Security Administration, September 17, 2008), http://www.tsa.gov/press/releases/2008/0917.shtm.

[47] Testimony of Maurine Fanguy, Program Director, Transportation Security Administration, Before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Border, Maritime, and Global Counterterrorism, Transportation Security Administration, September 27, 2008, http://www.tsa.gov/press/speeches/091708_fanguy_twic_depolyment_complete.shtm.

[48] "Borders and Transportation Security" (SAIC, 2012), http://www.saic.com/natsec/homeland-security/border-security.html.

[49] Joseph Straw, "New Views on Airport Screening," *Security Management* (2012), http://www.securitymanagement.com/article/new-views-airport-screening-004586?page=0%2C1.

[50] House Committee on Homeland Security, Subcommittee on Transportation Security, *Screening Partnership: Why Is A Job Creating, Public-Private Partnership Meeting Resistance at TSA?*, 112th Cong., 1st sess., February 16, 2012.

[51] Transportation Security Administration, "Screening Partnership Program," n.d., accessed June 8, 2012, http://www.tsa.gov/what_we_do/optout/index.shtm

[52] House Committee on Homeland Security, *Screening Partnership*, 12.

[53] William L. Waugh and Gregory Streib, "Collaboration and Leadership for Effective Emergency Management," *Public Administration Review* 66, no. S1 (2006): 131–140. Comprehensive emergency management means all of a community's hazards are considered in mitigation, preparedness, response, and recovery activities.

[54] Naim Kapucu, "Interorganizational Coordination in Dynamic Context: Networks in Emergency Response Management," *Connections* 26, no. 2 (2005): 33–48.

[55] Elaine Pittman, "What Big-Box Retailers Can Teach Government About Disaster Recovery," *Government Technology*, November 28, 2011, http://www.govtech.com/policy-management/Big-Box-Retailers-Teach-Disaster-Recovery.html.

[56] Eric Bonabeau and W. David Stephenson, "Expecting the Unexpected: The Need for a Networked Terrorism and Disaster Response Strategy," *Homeland Security Affairs* 3, no. 1 (February 2007), http://www.hsaj.org/?article=3.1.3.

[57] Barbaro and Gillis, "Wal-Mart at Forefront of Hurricane Relief."

[58] Ibid.

[59] Ibid.

[60] Ibid.

[61] Harold F. Upton, *The Deepwater Horizon Oil Spill and the Gulf of Mexico Fishing Industry* (Washington, DC: Congressional Research Service, 2011), 8-9, http://www.fas.org/sgp/crs/misc/R41640.pdf.

[62] Givens, "Deepwater Horizon Oil Spill."

[63] "About Industry Liaison Program" (Federal Emergency Management Agency, 2010), http://www.fema.gov/privatesector/industry/about.shtm.

[64] Federal Emergency Management Agency, "FEMA Administrator: Business Community is Critical Partner in Disaster Response and Recovery," November 4, 2011, http://www.fema.gov/news/newsrelease.fema?id=59308. Fugate is FEMA's top official.

[65] For example, see Edward T. Pound, "Security Clearance Challenges Defy Easy Fixes," *Government Executive*, August 14, 2007, http://www.govexec.com/welcome/?zone=welcome&rf=http%3A%2F%2Fwww.govexec.com%2Fdailyfed%2F0807%2F081407nj1.htm; "Personnel Clearances: Key Factors for Reforming the Security Clearance Process," Statement of Brenda S. Farrell, U.S. Government Accountability Office, May 22, 2008, http://www.gao.gov/assets/130/120165.pdf; Letter to U.S. Senators Daniel Akaka and George Voinovich from Brenda Farrell, Director of Defense Capabilities and Management, U.S. Government Accountability Office, July 14, 2008, http://www.gao.gov/new.items/d08965r.pdf; "Security Clearance Reform: Upgrading the Gateway to the National Security Community," Subcommittee on Intelligence Community Management, Permanent Select Committee on Intelligence, ASIS International, September 25, 2008, http://www.asisonline.org/councils/documents/govt_secclearance.pdf; "Personnel Security Clearances: An Outcome-Focused Strategy Is Needed to Guide Implementation of the Reformed Clearance Process" (Washington, DC: U.S. Government Accountability Office, May 2009), http://www.gao.gov/new.items/d09488.pdf; Letter (with attachment) to Steven Aftergood, Federation of American Scientists from Dionne Hardy, FOIA Officer, U.S. Office of Management and Budget, May 20, 2011, http://www.fas.org/irp/dni/irtpa-2011.pdf.

[66] George Boyne, "Public and Private Management: What's the Difference?," *Journal of Management Studies* 39, no. 1 (2002): 97–122; Mary K. Feeney and Hal G. Rainey, "Personnel Flexibility and Red Tape in Public and Nonprofit Organizations: Distinctions Due to Institutional and Political Accountability," *Journal of Public Administration Research & Theory* 20 (2010): 801–826.

[67] See "Homeland Security," Booz Allen Hamilton, accessed October 3, 2011, http://www.boozallen.com/consultants/civilian-government/homeland-security-consulting; "Homeland Security," SAIC, accessed October 3, 2011, http://www.saic.com/natsec/homeland-security/; "Homeland Security," Northrop Grumman, accessed October 3, 2011, http://www.is.northropgrumman.com/by_solution/homeland_security/index.html; "Homeland Security," General Dynamics C4 Systems, accessed October 3, 2011, http://www.gdc4s.com/content/detail.cfm?item=a96ae1cb-eb74-47d6-bffc-bc7ada51469a.

[68] "'Checkpoint Friendly' Laptop Bag Procedures," Transportation Security Administration, August 15, 2008, http://www.tsa.gov/press/happenings/simplifying_laptop_bag_procedures.shtm.

[69] "Aerovation Products," Aerovation, n.d., accessed January 26, 2012, http://aerovation.com/; "Laptop Bags: Industry Process and Guidelines," Transportation Security Administration, July 29, 2008, http://www.tsa.gov/press/happenings/innovative_laptop_bag_designs.shtm.

[70] Goldsmith and Eggers, *Governing by Network*, 25–39.

[71] Ibid.

[72] "TSA Awards Contract for Information Technology Infrastructure," Transportation Security Administration, September 28, 2009, http://www.federaltimes.com/article/20110131/DEPARTMENTS03/101310303/1050/PERSONNEL04.

[73] Ibid.

[74] Danny Peterson and Richard Besserman, "Analysis of Informal Networking in Emergency Management," *Journal of Homeland Security and Emergency Management* 7, no. 1 (2010): 1–14; Kathleen M. Kowalski-Trakofler, Charles Vaught, Michael R. Brinch Jr., Jacqueline H. Jansky, "A Study of First Moments In Underground Mine Emergency Response," *Journal of Homeland Security and Emergency Management* 7, no. 1 (2010): 1–28.

[75] The authors thank an anonymous reviewer for this suggestion.

[76] Goldsmith and Eggers, *Governing by Network*.

[77] Thomas A. Cellucci, ed., *Innovative Public-Private Partnerships: Pathway to Effectively Solving Problems* (U.S. Department of Homeland Security Science and Technology Directorate, July 2010), 17–20, http://www.dhs.gov/xlibrary/assets/st_innovative_public_private_partnerships_0710_version_2.pdf

[78] Ibid.

[79] "FutureTECH," U.S. Department of Homeland Security, accessed January 27, 2012, http://www.dhs.gov/files/programs/gc_1242058794349.shtm.

[80] Thomas A. Cellucci, *FutureTECH: Concept of Operations (*U.S. Department of Homeland Security, n.d., accessed January 27, 2012), http://www.dhs.gov/xlibrary/assets/st_commercialization_office_futuretech_conops.pdf.

[81] Julia Preston, "Homeland Security Cancels 'Virtual' Fence After $1 billion Is Spent," *New York Times*, January 14, 2011, http://www.nytimes.com/2011/01/15/us/politics/15fence.html.

[82] Daniel B. Wood, "Janet Napolitano Halts Funding for Virtual Border Fence," *The Christian Science Monitor*, March 17, 2012, http://www.csmonitor.com/USA/2010/0317/Janet-Napolitano-halts-funding-for-virtual-border-fence; Robert N. Charette, "Napolitano Cancels the US $1 billion SBINet Virtual Fence Project," *IEEE Spectrum* (March 2011) http://spectrum.ieee.org/telecom/security/napolitano-cancels-the-us-1-billion-sbinet-virtual-fence-project.

[83] Preston, "Homeland Security Cancels 'Virtual' Fence."

[84] Ibid.

[85] Ibid.

[86] Hon. John D. Dingell, "Protecting the Electrical Grid from Cybersecurity Threats," testimony before the Subcommittee on Energy and Air Quality, of the Committee on Energy and Commerce, U.S. House of Representatives, 110th Cong., 2nd Sess., September 11, 2008, 128.

[87] U.S. Chamber of Commerce, Business Software Alliance, TechAmerica, Internet Security Alliance (ISA), Center for Democracy and Technology, *Improving Our Nation's Cybersecurity through the Public-Private Partnership: A White Paper* (Center for Democracy and Technology, March 2011), https://www.cdt.org/files/pdfs/20110308_cbyersec_paper.pdf. This co-authored white paper supports the assertion that public-private partnerships can be strengthened in multiple dimensions.

[88] Mark de Bruijine and Michel van Eeten, "Systems That Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment," *Journal of Contingencies and Crisis Management* 15, no. 1 (2007): 18.

[89] Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security In an Uncertain World* (New York, NY: Copernicus Books, 2003), 41. See also de Bruijne and van Eeten, "Systems That Should Have Failed."

[90] de Bruijne and van Eeten, "Systems That Should Have Failed," 18.

[91] Goldsmith and Eggers, *Governing by Network*.

[92] Gregg Carlstrom, "Senator: DHS Budget Begins 'Turnaround' Away from Contracting," *Federal Times*, February 24, 2010, http://www.federaltimes.com/article/20100224/CONGRESS03/2240304/1055/AGENCY; Stephen Losey, "TSA halts expansion of privatized airport screening," *Federal Times*, January 31, 2011, http://www.federaltimes.com/article/20110131/DEPARTMENTS03/101310303/1050/PERSONNEL04.

[93] Jon D. Michaels, "Deputizing Homeland Security," *Texas Law Review* 88, no. 7 (2010): 1435–1473.

[94] Kai Jaeger and Edward P. Stringham, "Private Policing Options for the Poor" (National Center for Policy Analysis, December 15, 2011), http://www.ncpa.org/pub/ba763.

[95] For example, see Cooper J. Strickland, "Regulation Without Agency: A Practical Response to Private Policing in United States v. Day," *North Carolina Law Review* 89 (2011): 1338–1363.

[96] Ibid., 1340.

[97] For one of the first of many studies on this subject, see P.W. Singer, *Corporate Warriors: The Rise of the Privatized Military Industry* (Ithaca, NY: Cornell University Press, 2003).

[98] Ross Prizzia, "Coordinating Disaster Prevention and Management in Hawaii," *Disaster Prevention and Management* 15, no. 2 (2006): 275–285; Naim Kapucu, "Public-Nonprofit Partnerships For Collective Action in Dynamic Contexts of Emergencies," *Public Administration* 84, no. 1 (2006): 205–220; Camilla Stivers, "'So Poor and So Black': Hurricane Katrina, Public Administration, and the Issue of Race," *Public Administration Review* 67, no. 1 (Special Issue, December 2007): 48–56; Geoffrey T. Stewart, Ramesh Kolluru, and Mark Smith, "Leveraging Public-Private Partnerships to Improve Resilience in Times of Disaster," *International Journal of Physical Distribution and Logistics Management* 39, no. 5 (2009): 343–364; Susan A. McManus and Kiki Caruson, "Emergency Management: Gauging the Extensiveness and Quality of Public and Private-Sector Collaboration at the Local Level," *Urban Affairs Review* 47, no. 2 (2011): 280–299.

[99] For a classic treatment of this phenomenon, see R.A.W. Rhodes, "The Hollowing Out of the State: The Changing Nature of the Public Service in Britain," *The Political Quarterly* 65, no. 2 (1994): 138–151.

[100] House Judiciary Committee Hearing on Oversight of the Homeland Security Department, 112th Cong., 2nd Sess., July 19, 2012, accessed September 13, 2012, http://www.micevhill.com/attachments/immigration_documents/hosted_documents/112th_congress/TranscriptOfHouseJudiciaryCommitteeHearingOnOversightOfTheHomelandSecurityDepartment.pdf; *House Judiciary Committee Hearing on Homeland Security Oversight* (Washington, DC: C-SPAN, July 19, 2012), online video, http://www.c-spanvideo.org/program/307135-1#.

[101] To date, the most comprehensive and illuminating work on this topic is Dana Priest and William M. Arkin, *Top Secret America: The Rise of the New American Security State* (New York: Little, Brown and Company, 2011).

[102] Ibid.

[103] Ibid., 180.

[104] Ibid.

[105] Ibid., 187–188.

[106] Ibid., 194–201.

[107] Ibid.

[108] For example, see Thomas A. Cellucci, *Partnership Program Benefits Taxpayers as well as Public and Private Sectors* (Washington, DC: U.S. Department of Homeland Security Science and Technology Directorate, 2008).

[109] Thomas A. Cellucci and James W. Grove, *Leveraging Public-Private Partnership Models and the Free Market System to Increase Speed-of-Execution of High-Impact Solutions Throughout State and Local Governments* (U.S. Department of Homeland Security, August 2011), 10.

[110] For a similar point, see Stephen Flynn, "The Brittle Superpower," in Auerswald et al., *Seeds of Disaster*, 30–31.

[111] Scott Shane and Andrew Lehren, "Leaked Cables Offer Raw Look at U.S. Diplomacy," *New York Times*, November 28, 2010, http://www.nytimes.com/2010/11/29/world/29cables.html?pagewanted=all.

[112] See Auerswald et al., *Seeds of Disaster*, for a thorough examination of public-private sector cooperation for critical infrastructure protection.

[113] Ellen Nakashima, "Cybersecurity Bill Promotes Exchange of Data; Critics Say Measure Could Harm Privacy Rights," *Washington Post*, November 11, 2011, http://www.washingtonpost.com/world/national-security/cybersecurity-bill-promotes-exchange-of-data-white-house-civil-liberty-groups-fear-measure-could-harm-privacy-rights/2011/11/30/gIQAD3EPEO_story.html. Recent legislation seeks to limit firms' liability for sharing data with government. This is an example of an incentive for firms to exchange information with the public sector.

[114] Peter R. Orszag, "Homeland Security: The Problems With Providing Tax Incentives to Private Firms," Testimony Before the House Committee on Small Business Subcommittee on Rural Enterprise, Agriculture, and Technology, 108th Cong., 2nd Sess., July 21, 2004.

[115] Ibid.

[116] Ibid. See also James A. Lewis, "Aux Armes, Citoyens: Cyber Security and Regulation in the United States," *Telecommunications Policy* 29 (2005): 821–830.

[117] Carlstrom, "Senator: DHS Budget Begins 'Turnaround'."

[118] Losey, "TSA halts expansion of privatized airport screening.

[119] "Mature and Strengthen the Homeland Security Enterprise," U.S. Department of Homeland Security, March 14, 2011, http://www.dhs.gov/xabout/gc_1240838201772.shtm.

[120] "Over Reliance on Contractors," Department of Homeland Security Appropriations Bill, 2012, Committee Reports (112th Congress), Senate Report 112-074, September 7, 2011, http://thomas.loc.gov/cgi-bin/cpquery/?&sid=cp112YCOmu&r_n=sr074.112&dbname=cp112&&sel=TOC_56275&. The 2012 Department of Homeland Security Appropriations Bill notes that DHS includes 110,000 private employees, vis-à-vis 221,000 federal employees. This effectively means that approximately one third of DHS is privatized.

[121] Ibid.

[122] Robert Gates, "A Statement on Department Budget and Efficiencies," U.S. Department of Defense, January 6, 2011, http://www.defense.gov/speeches/speech.aspx?speechid=1527.

[123] "Big U.S. Companies Announce Massive Job Cuts," MSNBC, January 26, 2009, http://www.msnbc.msn.com/id/28854051/ns/business-stocks_and_economy/t/big-us-companies-announce-massive-job-cuts/.

[124] U.S. Department of Homeland Security, "Lessons Learned Information Sharing," n.d., accessed June 8, 2012, https://www.llis.dhs.gov/index.do.