

# Perspectives on Preparedness

August 2002  
No. 6



BELFER CENTER FOR SCIENCE AND  
INTERNATIONAL AFFAIRS  
TAUBMAN CENTER FOR STATE AND  
LOCAL GOVERNMENT



U.S. DEPARTMENT OF JUSTICE  
OFFICE OF JUSTICE PROGRAMS  
OFFICE FOR DOMESTIC PREPAREDNESS

## Executive Session on Domestic Preparedness

The Executive Session on Domestic Preparedness (ESDP) is a standing task force of leading practitioners and academic specialists concerned with terrorism and emergency management. Sponsored by the John F. Kennedy School of Government, Harvard University, and the U.S. Department of Justice, the ESDP brings together experts with operational experience in diverse professional fields that are essential to domestic preparedness -- emergency management, law enforcement, fire protection, public health, emergency medicine, national security and defense, and elected office.

The *Perspectives on Preparedness* series aims to provide useful information to the concerned professional communities about how the nation can enhance its ability to respond to the threat of terrorism with weapons of mass destruction. The ESDP also produces discussion papers and case studies. Visit the ESDP website at:

[WWW.ESDP.ORG](http://WWW.ESDP.ORG)

## BEYOND BUSINESS CONTINUITY: THE ROLE OF THE PRIVATE SECTOR IN PREPAREDNESS PLANNING

*JULIETTE N. KAYYEM AND PATRICIA E. CHANG*

When a hijacked jet—American Airlines Flight 77—crashed into the Pentagon on September 11, executives of Science Applications International Corporation<sup>1</sup> had 14,000 workers in offices around the Washington area, but received no guidance from government authorities as to whether it would be safe to release them. That same day, Washington Hospital Center canceled all elective surgery, cleared out beds and operating rooms, and prepared to receive victims, but failed to receive word from local officials that there would be few injured victims to treat.<sup>2</sup>

Earlier that morning in New York, after American Airlines Flight 11 and United Airlines Flight 175 hit the north and south towers of the World Trade Center, nearly everyone who could evacuate did so promptly. Their escape was facilitated by revisions made in the evacuation plan by the Port Authority after a terrorist bomb exploded in the World Trade Center in 1993. In addition, the structurally sound buildings, which were equipped with stairwells larger than building codes require, stood long enough to give potential survivors a chance to escape.<sup>3</sup> These factors helped save hundreds, and possibly thousands of lives on September 11.<sup>4</sup>

These accounts illustrate the range of private sector responses on September 11 and also demonstrate the vital role the private sector plays in ensuring the safety and well being of its employees. Some entities in the private sector, which had not previously worked on contingency planning or had depended on inadequate contingency plans, were forced to improvise hasty patchwork measures on September 11. On the other hand, those private sector entities that already had adequate disaster plans in place prior to September 11 were able to recover much more quickly and maintain a critical level of functionality.

Perhaps one of the most important lessons learned by the private sector was how foresight, prompt intervention, and emergency planning can save lives and greatly aid business recovery and continuity at the same time. Conversely, a sobering look at September 11 shows that a lack of preparation for disasters may complicate consequence management, halt business activity, and endanger lives. One lesson is clear: emergency planning needs to take place before a crisis occurs, and the private sector is an essential actor in that process.

**Juliette Kayyem** is Executive Director of the Executive Session on Domestic Preparedness (ESDP) at the John F. Kennedy School of Government.  
**Patricia E. Chang** is a Research Assistant with the ESDP.

When the nation's domestic preparedness program began in the 1990s, the focus was primarily to ensure that the federal, state, and local governments were well equipped to deal with any potential terrorist attack. A similarly limited view has also been adopted by the private sector. Since September 11, the issue of business continuity—the idea that planning is needed for businesses to operate and deliver uninterrupted services to customers during natural and man-made disruptions—has been the focus of much discussion within the business community.

While business continuity is essential, there is an even greater need for an integrated public and private domestic preparedness strategy, one that views the private sector not merely as a profit making entity, but as an entity responsible (as the government is) for protecting life and ensuring security.

The first part of this paper argues the private sector's current lack of integration into domestic preparedness programs is dangerous and explains the need for public-private emergency planning. The second part provides models and recommendations that would facilitate private sector involvement in public safety and security planning.

### **Lack Of Attention Given To The Private Sector Role**

Since September 11, the government has focused much time, energy, attention, and money towards fighting the “war against terrorism.” Some of the changes include increased federal attention to counterterrorism measures; the creation of new entities to fight terrorism, including the Office of Homeland Security; and sweeping changes in legislation to empower law enforcement and intelligence communities with new tools, such as expanded wiretapping and surveillance capabilities.<sup>5</sup> These changes operate with budgetary funding. A total of \$37.7 billion has been allocated for the homeland security program, which provides support for first responders, defense against bioterrorism, security for America's borders, and investment in technology that facilitates information and intelligence sharing.<sup>6</sup> The federal government, however, has focused

primarily on coordinating ways in which federal, state, and local government agencies will respond to a mass-casualty event; it has paid too little attention to integrating the private sector into nationwide counterterrorism efforts.

By neglecting the private sector in its emergency planning, the government limits the number of potential needs that its homeland defense initiatives can address. Historically, the private sector has not been a part of disaster planning. The responsibility has been given primarily to first responders at the state and local level, to FEMA for “consequence management,” and to the Department of Justice for “crisis management” at the federal level.<sup>7</sup> Assigning an emergency management role in crises to the public but not to the private sector, has contributed to an oversight of private sector involvement in domestic preparedness.

Bob Peck, president of the Greater Washington Board of Trade, illustrates this point:

“On September 11, I looked out of my window; the federal government did a chaotic job of evacuation; there was gridlock on the streets and we [Washington Board of Trade] started getting all these phone calls from businesses wanting to know if they should evacuate and how to secure their buildings...There were also rumors that the Metro was closed down, that were not true ...They [government officials] are used to planning their part of the deal [after a terrorist attack]. They [government officials] will tell the public to clear the area, so that they may do their job. But the private sector is not integrated.”<sup>8</sup>

In other words, there is a disconnect between the government and the private sector during and after a crisis situation.

Paralleling this disconnect is the way that businesses have reacted in the aftermath of September 11. Many businesses, while concerned with revamping their disaster-preparedness plans, have merely been focused on recovering and maintaining their own operations and systems after the attacks. The disorder created in New York City's financial

district, for example, was especially difficult to resolve. Approximately 20% of the downtown Manhattan office market—or 15.5 million square feet of office space—was destroyed in the September 11 attack. An additional 12 million square feet of office space was damaged as a result of falling debris, building collapse, and fires.<sup>9</sup> Corporations near Ground zero (such as Merrill Lynch, American Express, Morgan Stanley, Dean Witter, and Lehman Brothers) worked frantically in the first few hours after the attack to locate their dispersed employees. These corporations also attempted to return to business by relocating to their satellite office spaces, pulling up backup files, and trying to stem the loss of revenues.<sup>10</sup>

Some companies that were affected by the September 11 attacks did an extensive revision of their employee safety strategies, facilities strategies, communication strategies, information technology strategies, and insurance coverage in the weeks following the attacks.<sup>11</sup> Such changes in emergency response and incident management procedures include:

1. **Communications:** Communications plans should be in place in order to reassure, give instructions, and share information. Good communication is needed to prevent rumors and misinformation. New technology has made it possible for telecommunications to be an alternative for conducting business, bypassing the necessity of face-to-face interaction.<sup>12</sup>
2. **Leadership.** Management needs to review its emergency planning and practice executing decisions before a crisis occurs. Learning how to effectively handle a disaster is a management responsibility; consequently, leadership should familiarize itself with how to declare a disaster and how to appropriate necessary resources in response.
3. **Transportation.** Many employees were stranded or unable to work after 9-11. Businesses relying on

transportation for critical functions were paralyzed: overnight shipping was postponed, paychecks went undelivered.<sup>13</sup> Commuting to recovery sites was, in some cases difficult or impossible.

4. **Geographic Location.** Many companies affected by September 11 have chosen to diversify their geographic locations. According to TenantWise.com, an online real estate broker, only 17% of the 137,919 employees displaced by the attacks have returned.<sup>14</sup> Some Wall Street firms - Lehman Brothers Holdings Inc., Cantor Fitzgerald, and Fiduciary Trust - have relocated to midtown Manhattan.<sup>15</sup> In all, firms based in downtown New York have moved 30% of their employees outside the city, many of them permanently.<sup>16</sup>
5. **Personnel Back-Up.** Few companies have thought about succession planning, and those that have, focused primarily on the potential replacement of top executives.<sup>17</sup> Cantor Fitzgerald experienced one of the worst losses, with 700 employees killed as a result of the terrorist attacks.<sup>18</sup>
6. **Database Back-Up.** Companies have learned that some redundancy in operations and processing is helpful. With the destruction of desktops, laptops, LAN's, and other technology and data support systems on September 11, managers realized that paper files still remain an important means of information storage and maintenance for work in progress.<sup>19</sup>
7. **Key Dependencies.** Companies should understand dependencies on key vendors. The reliance on extended enterprise such as suppliers and service providers became a problem especially when the shipment of supplies was delayed and manufacturing cycles were disrupted. Understanding dependencies will help to minimize the risk of a supply chain or service breakdown.<sup>20</sup>

8. **Security.** Both physical and logical security efforts should be reviewed, and the right amount of preparedness should be chosen. This includes, but is not limited to, the physical security of buildings as well as the security of IT systems.<sup>21</sup>
9. **Insurance.** Companies should review insurance coverage to capture the required information for preparing a claim. The ability of carriers and reinsurers to assume resulting liabilities should be verified in advance.<sup>22</sup>

These efforts to alter business continuity plans were mostly, if not completely focused internally, neglecting how the government might guide or assist in contingency planning. Instead of collaborating with the government to assess risks, determine protection needs, select and implement cost-effective policies and controls, and initiate program tests, businesses made their security and emergency preparedness decisions individually. In other words, businesses concentrated solely on improving their own particular response when addressing safety concerns, mirroring how the government focuses on its own agenda for homeland security.

Peck characterizes the private sector response as follows: "The private sector people dealt like the government people, for instance, [by] putting more security in their lobbies...But more needs to be done on the front of preparedness...and with coordinating with the government."<sup>23</sup> George Vradenburg, the Strategic Advisor to AOL/Time Warner and a co-chair of the Potomac Regional Preparedness and Recovery Task Force agrees: "What is needed is a clear shared vision in regional private-public partnerships and a coherence to how government works with businesses and task forces."<sup>24</sup> As the events of September 11 have shown, the risks are too great and the costs are too high for a lack of preparation and coordination between the public and private sectors to persist.

## Limited Progress

To a certain extent, some recognition has been given to this lack of preparation and coordination. The terrorist attacks have ratcheted up the stakes, giving new impetus for the government and private industry to plan safe communities. For example, federal, state, and local government agencies have made some progress working with private sector entities in the areas of aviation security and cyber-security. Even before September 11, a Presidential Decision Directive, (PDD) 63 or Critical Infrastructure Protection, issued in May 1998 was intended to "improve federal agency security programs, establish a partnership between the government and the private sector, and improve the nation's ability to detect and respond to serious computer-based attacks."<sup>25</sup> The Aviation Security Act of 2001, noted that, "The existing fragmentation of responsibility for that safety and security among government agencies and between government and nongovernmental entities is inefficient and unacceptable in light of the hijackings and crashes on September 11, 2001."<sup>26</sup> It also placed more responsibility on the federal government for overseeing private security functions and security personnel at United States airports.<sup>27</sup>

There has also been more vocal attention given to private sector security. For instance, public officials are more frequently issuing statements that stress the importance of consistent communication from the government to the private sector. "A lot of businesses...are getting different messages from different levels of government..." regarding emergency procedures. "We have to go seek out private sector entities to make sure we're helping them prepare for [an economic] recovery. There has to be a meshing of public and private sector operations," states one local official.<sup>28</sup>

This sentiment is echoed in a recent White House Report, "Securing the Homeland, Strengthening the Nation." The report tasks OHS Director Tom Ridge with creating a national strategy for homeland security that will be based "on the principle of partnership with state and local governments, the private sector, and citizens."<sup>29</sup> In a briefing with

members of the National Association of Manufacturers (NAM), the nation's largest industrial trade association, Governor Ridge said:

“But, in fact, for it [national counter-terrorism strategy] to be a successful national strategy, the federal government, the state and local governments, have to be involved; the public sector certainly has to be involved. But very much at the heart of a successful strategy will be the involvement of the private sector. And to date, that involvement has been substantial and specific, and in the months and the years ahead we will continue to build on really the foundation that the private sector has laid, the public sector has been working on over the past couple of months as well.”<sup>30</sup>

Accordingly, federal, state, and local officials have noted that rethinking the role of the private sector in disaster planning is essential for many reasons. But much more needs to be done rather than simply expressed, now that the nation has recognized the need.

## Reasons For Government To Invest

There are many reasons why the government should be invested in engaging the private sector in its strategy for homeland security. First, more than 80% of information systems are owned by the private sector.<sup>31</sup> Approximately 90% of critical infrastructure is owned by the private sector, including banking, finance, transportation, and intelligence systems, utilities and water supplies, and communication networks.<sup>32</sup> Some of the most valuable institutions, and therefore the most desirable targets, are owned by the private sector.

Second, September 11 made evident the fact that the private sector has a crucial role to play in emergency planning and response. Many essential services used in an emergency—communications, power, water, food, and medical services—are owned or operated by private businesses.<sup>33</sup> Should a WMD or biological attack occur, private doctors, hospitals, and emergency technicians would

treat most of the victims. Likewise in a crisis situation, pharmaceutical companies would supply stockpiles of the critical medicines and vaccines; manufacturers would supply the necessary protective equipment and gear; banks and financial institutions would provide monetary support to the disaster site; privately owned communications systems would provide equipment and repairing services; and privately owned universities, schools, hospitals, or other buildings might contribute space for triage and other support activities.<sup>34</sup>

Third, most Americans spend a majority of their time away from home, inside of private institutions that have their own regulatory procedures. These institutions have significant influence over people's actions. Employers of the private sector are often responsible for planning emergency communications and evacuation efforts, including school closures, the provision of shelter, blood drives, vaccination programs, and other functions.<sup>35</sup> The decisions made by these private institutions affect the conduct and welfare of employees as well as the surrounding community. The government should factor this reality into its emergency and crisis planning.

Fourth, incorporating the voice of the private sector into the national homeland security strategy would also help stave off inefficiency in the war against terrorism. Without the input of the private sector, counterterrorism efforts may be fragmented and critical information may remain stove-piped. A fragmented strategy may consequently cause confusion, duplicative efforts, and an ineffective alignment of resources with strategic goals.<sup>36</sup> On the other hand, once the roles and responsibilities of the government and private sector are clarified and delineated, the burden of counterterrorism is shared—to the benefit of both.

Fifth, the United States Constitution and our legal regulatory system view the private sector, for the most part, as an entity that is not easily controlled. The Fifth Amendment to the Constitution states explicitly that there shall be no government taking of private property, without just compensation. President Truman's attempts to control the steel mills during the undeclared Korean War were invalidated by the

Supreme Court in 1952;<sup>37</sup> without congressional authorization, the Court said, the President could not simply take control of industry, regardless of the need during a war. Thus, in the event of an emergency, the government may not have the legal authority to force private entities to act in certain ways—for example, to provide transportation or safe havens for the population.<sup>38</sup> A domestic preparedness strategy that integrates the private sector will help ensure, first, that there is a working cooperation between government and business so that expectations and demands can be discussed, and second, that any legal impediments can be determined before an event, and legislation may be sought to remedy any deficiencies.

Finally, joining private and public efforts to homeland security may also help the government sustain an appropriate level of responsiveness and readiness for future disasters. Involvement of both the private and the public sectors in emergency planning will assist in sustainability, and in the maintenance of focus and political support for emergency preparedness planning, even when the attention given to terrorist threats has waned. Understanding and appreciating the value of preparedness by both the private and public sectors will ensure the longevity, if not the success, of emergency planning.

### Reasons Why The Private Sector Should Invest

The private sector should be invested and engaged in domestic preparedness programs for reasons stemming from obligation to self-interest. First, the clearest reason for private sector involvement in emergency preparedness is to ensure employee safety. After September 11, senior executives and boards recognized a “heightened sense of responsibility” for the safety of their people and consequently addressed the “human factor” of business.<sup>39</sup> Many businesses realized that their greatest asset was their people, and that the greatest loss to the company was not the loss of revenues, but the loss of human life.

Second, the failure to provide for planning may have unintended consequences for the private sector. For instance, the events of September

11 should change the way businesses think about their people and the way they provide for their needs, in particular for their mental health needs. Greg Farris, executive director of business continuity planning at Morgan Stanley, noted that people were so deeply influenced by the World Trade Center attacks that they required assistance from crisis counselors in, “getting back to normal and being productive again.”<sup>40</sup> A well-developed and robust emergency response plan, under the guidance of an incident commander, however, may provide for the safety of employees as well as provide for necessary mental health resources.

Third, as discussed earlier, the private sector needs to be invested in emergency preparedness because business continuity plans are a corporate necessity. Corporations that engage in business continuity planning (BCP) recognize that the risks leading to business process failure, asset loss, regulatory liability, customer service failure, or reputation damage may be mitigated.<sup>41</sup> Adequate BCP may also ensure the safety of one’s staff, preserve valuable information, minimize service interruptions, and help resume normal services.<sup>42</sup> Yet focusing solely on business continuity is a far too limited approach. With government assistance and guidance, businesses may be better assured that their safety efforts and continuity plans are as comprehensive and realistic as possible.

Fourth, having public-private preparedness plans in place may help maintain consumer and shareholder confidence. For example, the knowledge that the government and the private sector are working on safety precautions, has helped reassure some air flight passengers hesitant to fly after September 11. Confidence in the safety of a region may help recover losses (as in the case with aviation security), as well as help attract new jobs and economic growth to that area.<sup>43</sup>

Finally, the private sector should be engaged in preparedness planning with the government because there are needs that the private sector alone cannot meet by itself when disaster strikes. One such need is government guidance that provides accurate and timely

information during an emergency, guidance which allows the private sector to craft an appropriate response and execute its role in emergency preparedness. Other private sector needs include the protection of vital records and the maintenance of open communication lines.

Lastly, the government plays a part in stimulating economic recovery after disasters, e.g., President Bush's renewal of his pledge of at least \$20 billion in monetary assistance to New York.<sup>44</sup> (All in all, September 11 created a \$54 billion loss in the Lower Manhattan economy, displacing more than 100, 000 jobs.)<sup>45</sup> Integrating the private sector during emergency planning can help ensure that all vital services, including those outside the government, will continue.<sup>46</sup>

### Barriers To Private Sector Investment

Despite the many compelling reasons for private sector integration, numerous private-public collaborations have not yet occurred. This is partly because of historical precedent—there has been a traditional lack of government attention given to private sector involvement. The stronger and more troublesome reason is that there are significant barriers and obstacles hindering security investment. Investing in security may in fact, be to many companies' disadvantage. "Security is not an income generator, it's a cost generator...People want to spend as little as possible," states Kevin Surette, a security consultant in Litchfield, Maine.<sup>47</sup> "Security is not going to add to your bottom line. It's a necessary evil," adds Joe Grillo, a chief operating officer at HID Corp.<sup>48</sup> Consequently, even if standards for preparedness are the responsibility of the government and are federally mandated and developed, the costs for implementing or evaluating these practices still falls mainly on the private sector. Security is often viewed as a huge cost, instead of an investment with a sizable return in the form of preventing losses.

Exacerbating this problem, are substantial legal concerns—concerns that organizations could face antitrust violations for sharing information with industry partners, that their information could be subjected to Freedom of Information Act disclosures, or that they could face liability

concerns. These, along with cost concerns, currently limit private sector involvement.<sup>49</sup> Thus, whereas more rhetorical attention is being paid to the lack of private sector involvement in preparedness, substantial initiatives to address this problem are either lacking or are still burgeoning.

### How To Engage The Private Sector: Models

The work that remains to be done is daunting, but nevertheless achievable. In a practical sense, private and public partnerships will need to foster effective communication to and from the private sector and the government. "We need those in positions of authority to communicate clearly and calmly. Unless public officials and private sector leaders coordinate in advance, mixed messages will complicate the job of surviving, recovering, and putting communities back together. That's why advance planning is so critical,"<sup>50</sup> states Mike McCurry, founder of Grassroots Enterprise and co-chair of the Potomac Task Force.

Advance planning entails developing public and private dialogues on issues of common concern, understanding differing motivations and perspectives, cooperatively defining roles and responsibilities, and addressing burden sharing issues.<sup>51</sup> As private and public entities learn to work together, they will be better able to discover the gaps in domestic preparedness, identify and share some of their best security, safety, and recovery practices, and work to standardize their emergency planning with government guidance.

Perhaps the most difficult question to answer is how the private sector should be integrated into domestic preparedness programs. One model of how public and private sectors have worked together effectively on a transnational problem emerged during the Y2K millennium crisis. During the 1990s, it was feared that computer systems, software applications, and embedded microprocessors would crash or malfunction on January 1, 2000. Because they were programmed with date fields using just two digits for the year, people feared they would simply return to 1900 at the start of the new millennium.<sup>52</sup>

According to the Office of Management and Budget, the federal government spent an estimated \$8.34 billion to remedy the Y2K problem; the Commerce Department estimated that U.S. government and businesses combined spent roughly \$100 billion.<sup>53</sup> With roughly 180 billion lines of software code to be rewritten, and millions of embedded chips that needed to be replaced or destroyed, the magnitude of the technological and managerial challenge was brought to international attention as a *bona fide* emergency.<sup>54</sup> The attention resulted in massive mobilization with a leadership role for the federal government and partnerships with the private sector and international governments.

The federal approach to the Y2K situation may be organized into the following five categories:

1. Congressional oversight of agencies to hold them accountable for demonstrating progress to heighten public awareness of the problem.
2. Central leadership and coordination to ensure that federal systems were ready for the date change, to coordinate efforts primarily with the states, and to promote private sector and foreign government action.
3. Partnerships within the inter-governmental system and with the private entities, divided into key economic sectors to address such issues as contingency planning.
4. Communications to share information on the status of systems, products, and services, and to share recommended solutions.
5. Human capital and budget initiatives to help ensure that the government could recruit and retain the technical expertise needed to convert systems and communicate with the other partners and to fund conversion operations.<sup>55</sup>

A homeland security plan may demand a level of leadership, oversight, and partnership similar to the Y2K model.<sup>56</sup> However, Homeland Security Director Ridge realizes its distinct challenges: "You may say homeland security is a Y2K problem that doesn't end January 1<sup>st</sup> of any given year," he has said, alluding to the fact that unlike the relative success of initiatives and partnerships formed to face the Y2K situation, initiatives and partnerships addressing counter-terrorism need to be sustained over time.<sup>57</sup>

Since September 11, two of the most visible prototypes that have addressed the needs of private industry in crisis situations are: the Potomac Conference Regional Task Force on Preparedness and Recovery, working in collaboration with the Washington Council of Governments' (WASHCOG) Task Force on Homeland Security and Emergency Preparedness; and the New York City Partnership (hereinafter the NYCP).<sup>58</sup> The Potomac Conference Regional Task Force on Preparedness and Recovery (hereinafter the Potomac Conference Task Force) was launched in Washington on November 29, 2001, to promote regional collaboration and to spur businesses, non-profits, and public officials in all levels of government to prepare for future crises. More specifically, its goal is to work with public sector leadership to "develop and implement a comprehensive, integrated plan for prevention, response, and recovery from any potential crisis in the Greater Washington region."<sup>59</sup> The Potomac Conference Task Force, comprised of 160 individuals from businesses, non-profits, and the government, was divided into four break-out groups that would address: (1) Emergency Preparedness; (2) Business and Non-Profit Continuity; (3) Economic Recovery; and (4) Communications.<sup>60</sup>

Similarly, the NYCP is comprised of 200 "partners"—leaders from the business, real estate, and investment communities. The NYCP is a non-profit organization that works on legislation, regulation, and public issues impacting businesses and the economy.<sup>61</sup> Since September 11, it has engaged in studies and actions devoted to rebuilding the Lower Manhattan business community. The NYCP, however, is still in the preliminary stages of

addressing public-private collaboration and is currently working on designating a safety and security task force dedicated to this issue.<sup>62</sup> Promoting partnerships such as the Potomac Conference Task Force the NYCP may maximize resources and foster useful regional relationships.

### How To Engage The Private Sector: Recommendations And Tools

While the government relies on the private sector for greater support in protecting critical infrastructure and the homeland, many in the private sector are looking to the government to encourage safer networking and information-sharing in nonlegislative and nonregulatory ways. The government should take active steps in fostering a private-public approach to homeland security, and to encourage private sector participation in domestic preparedness. There are three steps involved in the process: researching the problem, providing risk and threat assessments to the private sector, and finally implementing policy tools that encourage private sector integration into homeland security.

The first step is to understand the problem fully before making recommendations and taking action. A public-private commission comprised of people who have worked on critical infrastructure protection, health officials from the private and public areas, businesses leaders, and government officials should be tasked with examining the lack of private sector integration in homeland security. Any recommendations made by this public-private commission should be framed in terms of establishing and maintaining private sector involvement in domestic preparedness programs.

Second, after understanding the problem and focusing on what needs must be met, the government should offer assistance with risk and threat assessments. Risk assessments are “decision-making support tools that are used to establish requirements and prioritize program investments.”<sup>63</sup> Risk assessments form a “deliberate, analytical approach that results in a prioritized list of risks;” this list may be used to select countermeasures to create

a certain level of preparedness for an area.<sup>64</sup> Threat assessments are tools that “identify and evaluate each threat on the basis of factors such as capability and intent to attack an asset, the likelihood and severity of the consequences of a successful attack.”<sup>65</sup>

Without the benefits of a threat and risk assessment, many companies rely on worst-case chemical, biological, radiological, or nuclear scenarios to generate countermeasures for prevention. This means that the company, working from a worst-case scenario, focuses on vulnerabilities (which are unlimited) rather than credible threats (which are limited).<sup>66</sup> Compared to worst-case scenarios, targeted threat and risk assessments give better guidance as to how to address threats and allocate resources, taking into account how much preparedness is necessary.<sup>67</sup>

Since September 11, many in the private sector have taken security matters into their own hands. This is evident from the rise of security spending and technological security devices: private security guards, metal detectors, digital cameras, electronic photo ID cards used to track employees, facial recognition systems, and fingerprint readers.<sup>68</sup> Other companies have chosen to irradiate mail and check ventilation systems in anticipation of an anthrax or bioterror event.<sup>69</sup> Still others have decided to strengthen the structure of their buildings,<sup>70</sup> or even to relocate.

Risk and threat assessments, however, will help decide what level of preparedness and action is appropriate, while factoring the context of the business operation together with the likelihood of an attack. Thus, a small company in Iowa will not necessarily possess the same safety concerns or the same safety requirements as a large investment bank in downtown New York. A company’s level of preparedness needs will differ by location, density, industry, and a range of other factors.

Lead federal agencies should develop a best-practices model for the private sector that enables them to conduct more accurate risk, vulnerability, and survivability assessments.<sup>71</sup> Such a model would allow industry to address its security needs according to a set of

performance standards, as opposed to a set of government specifications. The Defense Department's internal assessment program may serve as a guide in developing best practices.<sup>72</sup> In addition, the Department of Justice Office for Domestic Preparedness and the FBI have worked together to provide state and local governments with a risk and threat assessment tool.<sup>73</sup> This tool includes a step-by-step methodology for assessing threats, risks, and requirements which could likely be put to use by the private sector.

Third, the federal government possesses a variety of policy instruments (such as regulations, tax incentives, and regional coordination and partnerships) that could be used to encourage or mandate that private sector entities take actions addressing security concerns. The methods for engaging the private sector may rest on frameworks ranging from the regulatory to the rewarding, to the simple removal of barriers to security investment.

The *regulatory* framework operates under the assumption that the government must take more proactive measures in setting standards for infrastructure and programs vital to preparedness. In the most stringent regulatory framework, federal agencies would support standards adopted by the private sector, and these standards would be placed under federal oversight. A less stringent regulatory framework would present alternatives to federal preemption and operate on a more voluntary basis. The following are five models proposed by a Government Accounting Office Report.<sup>74</sup> These models represent the spectrum of shared regulatory authority:

1. Fixed federal standards that preempt all state regulatory action in the subject area covered;
2. Federal minimum standards that preempt less stringent state laws but permit states to establish standards that are more stringent than the federal;
3. Inclusion of federal regulatory provisions not established through preemption in grants or other forms of

assistance that states may choose to accept;

4. Cooperative programs in which voluntary national standards are formulated by federal and state officials working together; and
5. Widespread state adoption of voluntary standards formulated by quasi-official entities.

Enforcing these standards is a separate issue, which can be addressed in a regulatory framework. Depending on how stringent the chosen regulatory framework may be,<sup>75</sup> entities that enforce these security standards (or recommendations) may respond in kind. A variety of entities may be "enforcers." For example, companies might undergo regular federal audits, engage in voluntary reporting to committees with federal oversight, or report to trade organizations, which would oversee the enforcement of these standards. If standards/recommendations are not properly implemented, these entities may respond in a punitive fashion.

The methods used in a *rewarding* framework consist of incentives that encourage the private sector to increase its security precautions. Incentives would include measures such as tax incentives and designation on an honor roll. Tax incentives may consist of special exclusions, exemptions, deductions, credits, deferrals, or tax rates in the federal tax laws.<sup>76</sup> Tax incentives do not generally permit the same degree of federal oversight and targeting as grants.<sup>77</sup> Similarly, a biannual "honor roll," a list used for comparing companies and noting exemplary performance, is suggested to highlight the top 100 companies that have adopted these security standards—to stimulate and encourage voluntary participation.<sup>78</sup> The honor roll would essentially create a competitive atmosphere in industry, in which the adoption of comprehensive security systems is rewarded with recognition. More importantly, it would likely be utilized by "potential customers, investors, and insurers," in their decisions choosing between potential providers.<sup>79</sup>

The methods used in the *removing barriers* framework simply entail doing that which is expedient to encourage private sector involvement in security. This includes providing Freedom of Information Act (FOIA) exemptions<sup>80</sup> to specific companies. FOIA exemptions exempt certain business records from disclosure. Many companies fear that any information that they share about their vulnerability or risk of intrusion will become public knowledge and will therefore damage public and shareholder confidence. Companies hesitate to disclose that information, even if it is vital to the interest of national defense. Competitors may also use FOIA requests to gain information about a company's practices or systems—information that may include trade secrets.<sup>81</sup>

The damage done when confidential information is made public may be detrimental to businesses; “an inadvertent release of confidential business information, such as trade secrets or proprietary information, could damage reputations, lower consumer confidence, hurt competitiveness, and decrease market shares of firms.”<sup>82</sup> Targeted FOIA exemptions, however, would encourage some businesses (which would be pre-identified by the government's commission) to share critical information in the interests of protecting the nation, and to cooperate in making threat assessments of infrastructure without compromising business concerns.

The government should also provide narrow antitrust exemptions, such as the legislation passed by the 105<sup>th</sup> Congress, the Information and Readiness Disclosure Act,<sup>83</sup> which exempted any information sharing for the purposes of Y2K preparedness from antitrust laws. Antitrust laws are meant to prevent businesses from colluding and price-fixing, but they also inhibit companies from sharing information on infrastructure vulnerability or from working on the means to protect it.<sup>84</sup> When homeland security is threatened, however, any cooperation to protect critical infrastructure should be exempted from antitrust laws to protect cooperative companies from unjust lawsuits.

One pending legislative bill that promotes both FOIA and antitrust exemptions is the S. 1456, the Critical Infrastructure Information Security Act of 2001. The bill has several purposes—to “facilitate the security of the critical infrastructure of the United States; to encourage the secure disclosure and protected exchange of critical infrastructure information; to enhance the analysis, prevention, and detection of attacks on critical infrastructure, and to enhance the recovery from such attacks.”<sup>85</sup> A group of eight industry organizations, including the National Association of Manufacturers (NAM), Edison Electric Institute, American Petroleum Institute, and the ITAA wrote to lawmakers in October 2001 encouraging them to pass S.1456. The last major action involved hearings held by the Senate Committee on Energy and Natural Resources in October 29, 2001.

Finally, Congress should remove tax penalties that make it more difficult for the private sector to invest in security measures. Industry is only allowed to depreciate its spending for security-related purchases, often over an extended period. This creates a tax on investment spending, which, in turn, increases the effective cost while discouraging businesses from spending on security.<sup>86</sup> Removing tax penalties on companies that invest in security will encourage the private sector's participation in domestic preparedness. Congress should revise the tax code to permit infrastructure owners to deduct the full cost of security-related spending in the year that such expenses are incurred.<sup>87</sup>

These three frameworks (*regulatory*, *rewarding*, and *removing barriers*) and their methods are by no means comprehensive, yet this list may serve as a guide to government action. These policy tools, however, are most effective only after private sector and government needs have been researched properly through a private-public commission, and risk and threat assessments have been issued. There are both advantages and disadvantages to each framework as policy tools. For reasons detailed in the following paragraphs, a step in the right direction would favor the *removing barriers* framework, as opposed to the

*regulatory* or *rewarding* frameworks. After the *removing barriers* framework has been successfully implemented and its shortfalls revealed, a mix of *regulatory* or *rewarding* factors may then be augmented, depending on need.

### Advantages/Disadvantages

Each of the frameworks has its merits and drawbacks. A benefit of the *regulatory* framework is that it would help standardize security efforts. On the other hand, regulatory models (especially on the more stringent side) may be politically difficult to maneuver, as most businesses balk at government regulation of their trade. Second, rigid standards enforced by a regulatory model often do not allow firms to adapt these standards according to their own organizational capacity and needs. Another disadvantage of the regulatory model is that it might discourage, or worse, stymie, any innovation of private sector solutions to security problems. When the private sector takes responsibility for security, the internal regulatory strategies may perhaps be even less costly and more effective than they would be under government standards.<sup>88</sup> Finally, the enforcement of the regulatory model would be subject to constant or continual evaluations or measurements, checking if businesses are sufficiently prepared. This could be costly to both parties, without a distinct end-point in the development of private sector preparedness.

The *rewarding* framework may encourage greater information-sharing and investment in security in the private sector without incurring the political difficulties of the regulatory framework. A significant disadvantage to the rewarding framework, however, is that it might be costly in a period of economic decline. Using rewards and incentives may also give certain companies competitive advantages that they would not ordinarily possess unless the rewards were distributed to companies across the board. Economic policy might be skewed towards favoring larger corporations that the government has targeted as necessary information sources. It should be noted that there is a trade-off that occurs when governments target specific companies for rewards; the government may be compromising a bit of security standardization when targeting

only a specific number of companies for rewards.

The *removing barriers* framework, although not a complete solution, poses the best point of entry for government to encourage private sector investment. However, responsible and careful the use of exemptions and tax penalty removals may be, removing barriers may still be seen as solely promoting corporate welfare. It is beneficial to all, however, insofar as it encourages companies to share information crucial to national defense, encourages cooperation on efforts to protect critical infrastructure, and removes legal and financial obstacles to security investment.

### State And Local

The above recommendations demonstrate options for federal activism. Initiatives that integrate the private sector on a state and local level are also important. Public-private partnerships cannot be built without the involvement of local governments. One means of encouraging local level involvement would be to place business leaders on state counterterrorism task forces.<sup>89</sup> Many of the already existing state task forces would likely benefit from the perspective of the private sector.

Regional coordination is another means of fostering private sector engagement at the state level. With regional coordination, mutual aid agreements provide a structure for resource-sharing and assistance among jurisdictions in response to an emergency.<sup>90</sup> Because individual jurisdictions may be short-handed in an emergency, these agreements allow resources to be deployed quickly across a region. In some cases, these agreements may provide a means for the state to share services, personnel, supplies, and equipment with counties, towns, and municipalities within the state, with neighboring states, or with states bordering Canada. Other agreements also provide cooperative planning, training, and exercises for private and public entities to prepare for emergencies.<sup>91</sup> The Emergency Management Assistance Compact, or EMAC, is an example of an interstate mutual aid agreement that allows states to assist one

another in responding to natural and man-made disasters. Currently, there are forty-two states and two territories that are members of EMAC.<sup>92</sup>

Since September 11, businesses have responded to the continuing threat of terrorism in a variety of ways. One rather dramatic means has been the relocation of businesses to areas less likely to be victimized, such as Connecticut and New Jersey. There is, however, a more measured, and more realistic, response. Cities and commerce will likely be the targets of terrorism, or, as one commentator put it, “density kills.”<sup>93</sup> That is likely true, but hardly illuminating. Instead of “running for the hills,” a more collaborative approach towards integrating the private sector into domestic preparedness planning may go far in minimizing and mitigating the harm to property, commerce, and most importantly, people.

Homeland security is a task that involves not only public entities and officials, but private entities and officials as well. Currently, there is a lack of integration with the private sector in domestic preparedness programs because of historical reasons, cost concerns, and legal impediments. The need for public-private partnerships, however, is vital for many reasons. Research by a public-private commission, government assistance in issuing threat and risk assessments, and the utilization of policy instruments will likely benefit not only the public sector, but the nation as a whole.

---

*This project was supported by Grant No. 1999-MU-CX-0008 awarded by the Office for State and Local Domestic Preparedness Support, Office of Justice Programs, U.S. Department of Justice. The Assistant Attorney General, Office of Justice Programs, coordinates the activities of the following program offices or bureaus: the Bureau of Justice Assistance, the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.*

The authors thank Robyn Pangi for her substantive and editorial comments, Robert Peck, George Vradenburg, Judith Russell, Ernest Tollerson, and Ira Jackson for their insights on public-private partnerships, Marshall Carter for engaging in peer review, and editor John Gravois for his attention to details.

## NOTES

1. SAIC is the nation's largest employee-owned research and engineering firm.
2. Neil Irwin, "Area's Private Sector Weighs Role in Emergency Plan," *The Washington Post* (November 29, 2001) p. E01.
3. Dennis Couchon, "For Many on Sept. 11, Survival was No Accident," *USA Today* (December 20, 2001) accessed at <[www.usatoday.com/news/attack/2001/12/19/usatcov-wtcsurvival.htm](http://www.usatoday.com/news/attack/2001/12/19/usatcov-wtcsurvival.htm)> The Port Authority also made other crucial improvements prompted by the 1993 attacks: placing reflective paint on stairs, railings, and stairwell doors; adding arrows to guide people along corridors to stairway connections; installing loudspeakers so that building managers could speak to people in their offices and hallways; and adding a second source of power for safety equipment.
4. Ibid.
5. Adam Cohen, "Fighting Terror at Home: Rough Justice," (December 2, 2001) accessed at <[www.time.com/time/nation/article/0,8599,186603,00.html](http://www.time.com/time/nation/article/0,8599,186603,00.html)>
6. White House Report, "Securing the Homeland, Strengthening the Nation," p. 8, accessed at <[www.whitehouse.gov/homeland/homeland\\_security\\_book.html](http://www.whitehouse.gov/homeland/homeland_security_book.html)>
7. Richard Falkenrath, "The Problems of Preparedness: Challenges Facing the U.S. Domestic Preparedness Program," Belfer Center for Science and International Affairs Discussion Paper 2000-28 (December 2000) pp. 4-5.
8. Interview with President Bob Peck, February 28, 2002.
9. "After September 11, 2001: The Impact of Terrorism on Corporate America," *Business Facilities*, accessed at <[www.facilitycity.com/busfac/bf\\_01\\_10\\_cover.asp](http://www.facilitycity.com/busfac/bf_01_10_cover.asp)>
10. Ibid.
11. Deloitte & Touche Report, "Business Continuity Management: Unique Perspectives from Ground Zero," p. 3, accessed at <[www.deloitte.ca/en/Pubs/AA/BCM\\_E.pdf](http://www.deloitte.ca/en/Pubs/AA/BCM_E.pdf)>
12. Ibid, p.6.
13. Ibid, p.5.
14. Special Report: Overview of Current Situation (March 21, 2002) *Tenantwise.com* accessed at <[www.tenantwise.com/032002wtc.asp](http://www.tenantwise.com/032002wtc.asp)>
15. "Moving Back Downtown?," *Wall Street Journal Online* (March 15, 2002) accessed at <[online.wsj.com/public/resources/documents/MovingBack-2--2-03-15.htm](http://online.wsj.com/public/resources/documents/MovingBack-2--2-03-15.htm)>
16. Michael Siconolfi, "Wall Street Firms Rebuild," *The Wall Street Journal* (March 11, 2002) p. M1
17. Neil Kaufman, Jack Pullara, Mary Grace Davenport, and Chris Thompson, "Insights from the Events of September 11: Is your organization prepared?" *PriceWaterHouseCoopers Global*, accessed at <[www.pwcglobal.com/extweb/manissue.nsf/DocOD/0D079AF005641DD285256B49005E1AF1](http://www.pwcglobal.com/extweb/manissue.nsf/DocOD/0D079AF005641DD285256B49005E1AF1)>

18. "Solemn Tribute for Cantor Fitzgerald," *MSNBC.com* (October 1, 2001) accessed at <[www.msnbc.com/news/636359.asp](http://www.msnbc.com/news/636359.asp)>
19. Neil Kaufman, et. al, "Insights from the Events of September 11th: Is your organization prepared?"
20. Ibid.
21. Ibid.
22. Deloitte & Touche Report, "Business Continuity Management: Unique Perspectives from Ground Zero," p. 7.
23. Interview with President Bob Peck, February 28, 2002.
24. Interview with George Vradenburg, February 19, 2002.
25. GAO Report to the Subcommittee on Technology, Terrorism, and Government Information, Committee on the Judiciary, "Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities," GAO-01-323 (April 2001) p.9.
26. Public Law 107-71, 107th Congress, 1st sess. (19 November 2001) *Aviation Security Act of 2001*. The Aviation Security Act, S. 1447, became Public Law No. 107-71 on November 19, 2001.
27. Ibid.
28. Neil Adler, "Officials preach regional response to emergencies" (December 7, 2001) accessed at <[www.gazette.net/200149/business/news/83117-1.html](http://www.gazette.net/200149/business/news/83117-1.html)> The local official quoted is Gene Lynch, deputy chief of staff to Governor Parris N. Glendening from Maryland.
29. White House Report, "Securing the Homeland, Strengthening the Nation" p. 6. at <[www.whitehouse.gov/homeland/homeland\\_security\\_book.html](http://www.whitehouse.gov/homeland/homeland_security_book.html)>
30. Transcript of Governor Tom Ridge, "Issues Briefing" with National Manufacturers Association (February 13, 2002) p. 5 at <[www.nam.org/tertiary.asp?TrackID=&CategoryID=513&DocumentID=24287](http://www.nam.org/tertiary.asp?TrackID=&CategoryID=513&DocumentID=24287)>
31. Gilmore Commission, *Third Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (December 15, 2001) p. 41.
32. Sandra Swanson, "National Security Council Contemplates Computer Security Issues," *InformationWeek.com* (October 31, 2001) accessed at <[www.informationweek.com/story/IWK20011031S0008](http://www.informationweek.com/story/IWK20011031S0008)>
33. The private sector also is a producer of innovative technology, medicines, services, and products that help combat terrorism. Many private companies, for instance, work as subcontractors to government agencies or as outsourcers of critical functions in an emergency.
34. Potomac Conference White Paper, "Regional Preparedness and Recovery" (November 29, 2001) pp. 3-4 provided by Karen Roberts, Director of the Potomac Conference, via email 2/11/02.
35. Ibid.
36. Statement of David M. Walker, GAO Testimony before the Senate Committee on Governmental Affairs, "Homeland Security: A Framework for Addressing the Nation's Efforts," GAO-01-1158T (September 21, 2001) p. 4.
37. *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952) (Steel Seizure Case).
38. Juliette N. Kayyem, "U.S. Preparations for Biological Terrorism: Legal Limitations and the Need for Planning," Belfer Center for Science and International Affairs Discussion Paper 2001-4 (March 2001) pp. 12-13.

39. Deloitte & Touche Report, "Business Continuity Management: Unique Perspectives from Ground Zero," p. 4.
40. Stan Gibson, "Reporter's Notebook: Disaster Recovery," eWEEK (October 22, 2001) accessed at <[www.eweek.com/article/0,3658,s%253D704%2526a%253D15168,00.asp](http://www.eweek.com/article/0,3658,s%253D704%2526a%253D15168,00.asp)>
41. Deloitte & Touche Report, "Business Continuity Management: Unique Perspectives from Ground Zero," p. 11.
42. AT Kearney Pamphlet. "Business Continuity and Corporate Security: A Timely Solution for Today's Challenges." on file with the author. For more information, please access <[www.atkearney.com](http://www.atkearney.com)>
43. Potomac Conference White Paper, "Regional Preparedness and Recovery" (November 29, 2001) p. 12.
44. Raymond Hernandez, "Bush Offers Details of Aid to New York Topping \$20 Billion," *The New York Times* (March 8, 2002) p. A1.
45. Kathryn S. Wylde, "The Old Downtown Economy Won't Return," *The New York Times* (March 29, 2002)
46. Potomac Conference White Paper, "Regional Preparedness and Recovery" (November 29, 2001) p. 8.
47. Rachel Zimmerman, "Workplace Security (A Special Report): Tools to Protect Mail," *The Wall Street Journal* (March 11, 2002) p. R7.
48. Maureen Tkacik, "Workplace Security (A Special Report): Ready Response: Plenty of companies are aiming to cash in on the security business, but so far it's no bonanza," *The Wall Street Journal* (March 11, 2002) p. R12.
49. A Report of the Heritage Foundation Homeland Security Task Force, "Defending the American Homeland," The Heritage Foundation (2002) p. 22-23.
50. Email correspondence from Potomac Director of Communications relaying quote (March 5, 2002).
51. Executive Summary, "Bioterrorism in the United States: Threat, Preparedness, and Response," Chemical and Biological Arms Control Institute (November 2000) p. 27.
52. Y2K Risk Assessment Task Force, "Y2K: A Global Ticking Time Bomb?," CSIS accessed at <[www.csis.org/html/y2k.html](http://www.csis.org/html/y2k.html)>
53. Final Committee Report, "Y2K Aftermath—Crisis Averted," The United States Senate Special Committee on the Year 2000 Technology Problem (February 29, 2000) p. 11 accessed at <[www.senate.gov/~bennett/y2k.html](http://www.senate.gov/~bennett/y2k.html)>
54. Y2K Risk Assessment Task Force, "Y2K: A Global Ticking Time Bomb?," CSIS
55. Statement of Henry L. Hinton, Jr., GAO Testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations House Committee on Government Reform, "Homeland Security: Progress Made; More Direction and Partnership Sought," GAO-02-490T (March 12, 2002) p. 12. The five categories are taken verbatim from this statement.
56. Statement of David Walker, "Homeland Security: A Framework for Addressing the Nation's Efforts," p. 6.
57. Liza Porteus, "Ridge calls homeland security a Y2K problem with no deadline," *GovExec.com* (February 28, 2002) accessed at <[www.govexec.com/dailyfed/0202/022802td1.htm](http://www.govexec.com/dailyfed/0202/022802td1.htm)>
58. There are other regional organizations that work on emergency preparedness activities, such as various regional councils of governments, regional chambers of commerce (such as in Florida or South Carolina, where chambers of

commerce concentrate on preparedness and recovery from hurricanes), and regional civic organizations, such as the Orange County Business Council and the South Bay Economic Development Partnership in California, and the Regional Plan Association's "Civic Alliance to Rebuild Downtown New York," in New York.

59. Regional Task Force on Preparedness and Recovery Status Update, The Potomac Conference (January 10, 2002) accessed at <[www.bot.org/html/news/News-TPC011802.asp](http://www.bot.org/html/news/News-TPC011802.asp)>

60. The four groups are tasked with various responsibilities, including: identifying common terminology to convey threats and emergency procedures in order to minimize confusion; developing a "best practices" tool kit along with a resource bank of mentors and coaches that may be used for continuity planning; integrating their work with regional tourism and economic development initiatives in order to encourage regional economic growth; and developing methods of informing the public during an emergency so that they may decide what actions to take within their households.

61. For more information, please access website <[www.nycp.org](http://www.nycp.org)>

62. Interview with NYCP's Senior Vice President, Ernest Tollerson and Vice President of Research and Policy, Judith Russell, March 20, 2002.

63. GAO Report to Congressional Requesters, "Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks," GAO/NSIAD-99-163 (September 1999) p. 5-6.

64. Ibid.

65. Ibid.

66. GAO Report to Congressional Committees, "Combating Terrorism: Selected Challenges and Related Recommendations," GAO-01-822 (September 2001) p. 45.

67. Ibid.

68. Kris Maher, "Workplace Security (A Special Report)—Life Goes on...but Differently: For many workers, day-to-day life has changed, in ways both small and large," *The Wall Street Journal* (March 11, 2002) p. R14 and Dennis K. Berman, "Workplace Security (A Special Report)—Tools to Protect Against Future Threats," *The Wall Street Journal* (March 11, 2002) p. R10.

69. Rachel Zimmerman, "Workplace Security (A Special Report): Tools to Protect Mail," *The Wall Street Journal* (March 11, 2002) p. R7.

70. Susan Warren, "Workplace Security (A Special Report: Tools to Protect Buildings)," *The Wall Street Journal* (March 11, 2002) p. R6.

71. "Defending the American Homeland," The Heritage Foundation, p. 24.

72. Ibid.

73. Statement of Raymond J. Decker, GAO Testimony before the Senate Committee on Governmental Affairs, "Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts," GAO-02-208T (October 31, 2001) p. 6.

74. Statement of Patricia A. Dalton, GAO Testimony before the Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform, House of Representatives, "Combating Terrorism: Intergovernmental Cooperation in the Development of a National Strategy to Enhance State and Local Preparedness," GAO-02-550T (April 2, 2002) p. 15.

75. It should be noted that the first two models are more stringent than models numbered three through five.

76. States that have promoted commercial and industrial applications of renewable energy technologies, for example, have provided incentives such as income tax credits, property tax exemptions, state sales tax exemptions, loan programs, special grant programs, industry recruitment incentives, accelerated depreciation allowances, as well as project development grants.
77. Statement of Patricia A. Dalton, "Combating Terrorism: Intergovernmental Cooperation in the Development of a National Strategy to Enhance State and Local Preparedness," GAO-02-550T, p. 15.
78. "'Defending the American Homeland,'" The Heritage Foundation, p. 24.
79. Ibid.
80. FOIA exemptions make the following records exempt from disclosure: 1. information vital to national defense; 2. information related to solely internal personnel rules and practices; 3. information specifically exempted from disclosure by statute; 4. information that is a trade secret; 5. information contained in inter- or intra-agency memorandums or letters that would not be available by law; 6. information that violates personnel and medical files; 7. information compiled for law enforcement purposes. For more information please access <[www.federalreserve.gov/generalinfo/foia/exemptions.cfm](http://www.federalreserve.gov/generalinfo/foia/exemptions.cfm)>
81. "Defending the American Homeland," The Heritage Foundation, p. 22.
82. Statement of Joel C. Willemsen, GAO Testimony before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives, "Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer Based Attacks," GAO-01-1168T (September 26, 2001) p. 28.
83. Previously the S. 2392, the Year 2000 Information and Readiness Disclosure Act became Public Law 105-271 on October 19, 1998.
84. "Defending the American Homeland," The Heritage Foundation, p. 23.
85. *Critical Infrastructure Information Security Act of 2001*, 107th Congr., 1st sess., S. 1456.
86. "Defending the American Homeland," The Heritage Foundation, p. 24.
87. Ibid.
88. This idea originated from a working paper that focused on managing environmental improvement within organizations. Cary Coglianese and Jennifer Nash, "Bolstering Private Environmental Management," JRWP01-011, John F. Kennedy School of Government Faculty Research Working Paper Series (April 2001) p. 2.  
For more information, please access <[www.researchmatters.harvard.edu/story.php?article\\_id=290](http://www.researchmatters.harvard.edu/story.php?article_id=290)>
89. In a meeting with National Association of Manufacturers (NAM), Governor Ridge requested that more private sector leaders be engaged in security initiatives on a local level. Transcript of Governor Tom Ridge, "Issues Briefing" with National Manufacturers Association (February 13, 2002) p. 12-13.
90. Statement of Patricia A. Dalton, "Combating Terrorism: Intergovernmental Cooperation in the Development of a National Strategy to Enhance State and Local Preparedness," GAO-02-550T, p. 15.
91. Ibid.
92. For more information, please access <[www.nemaweb.org/emacs/index.cfm](http://www.nemaweb.org/emacs/index.cfm)>
93. Steven Johnson, "Blueprint for a Better City," *Wired Archive* (September 12-December 2001) accessed at <[www.wired.com/wired/archive/9.12/mustread\\_pr.html](http://www.wired.com/wired/archive/9.12/mustread_pr.html)>

## Executive Session Members

### Professor Graham T. Allison

Professor of Government and Director  
Belfer Center for Science and International Affairs  
Kennedy School of Government

### Professor Alan Altshuler

Professor of Urban Policy and Planning and Director  
Taubman Center for State and Local Government  
Kennedy School of Government

### Mr. Thomas Antush

Senior Program Analyst  
Transportation Security Administration  
U.S. Department of Transportation

### Dr. Joseph Barbera

Clinical Associate Professor of Emergency Medicine  
George Washington University

### Mr. Bruce Baughman

Director, Office of National Preparedness  
Federal Emergency Management Agency

### Mr. Peter Beering

Indianapolis Terrorism Preparedness Coordinator

### Lieutenant General (Ret.) Thomas N. Burnette, Jr.

Former Deputy Commander in Chief, U.S. Joint Forces  
Command

### Professor Ashton B. Carter

Professor of Science and International Affairs,  
Kennedy School of Government

### Mr. Hank Christen

Emergency Response Consultant,  
Unconventional Concepts, Inc., FL

### Chief Rebecca Denlinger

Chief, Cobb County Fire Department, GA

### Major General (Ret.) John Fenimore

Former Adjutant General, New York National Guard

### Ms. Ellen Gordon

Administrator, Iowa Emergency Management Division

### Dr. Margaret Hamburg

Vice President for Biological Programs  
Nuclear Threat Initiative, Washington, DC

### Mayor Clarence Harmon

Former Mayor, City of St. Louis, MO

### Mr. Francis X. Hartmann

Executive Director, Program in Criminal Justice Policy/  
Management and Malcolm Wiener Center for Social Policy,  
Kennedy School of Government

### Professor Philip Heymann

Professor of Law, Harvard Law School

### Dr. Arnold M. Howitt

Executive Director, Taubman Center for State and  
Local Government, Kennedy School of Government

### Ms. Juliette Kayyem

Executive Director, Executive Session on Domestic  
Preparedness, Kennedy School of Government

### Dr. Robert Knouss

Director, Office of Emergency Preparedness  
U.S. Department of Health and Human Services

### Peter LaPorte

Director, District of Columbia Emergency Management  
Agency

### Major General Bruce M. Lawlor

Senior Director for Protection and Prevention  
Office of Homeland Security

### Dr. Marcelle Layton

Assistant Commissioner, Bureau of Communicable  
Disease, New York City Department of Health

### Dr. Scott Lillibridge

Professor and Director, Center for Biosecurity  
University of Texas Health Science Center  
School of Public Health

### Mr. John Magaw

Undersecretary of Transportation for Security  
U.S. Department of Transportation

### Chief Paul Maniscalco

Deputy Chief, New York City Emergency Medical  
Services Command

### Mr. Gary McConnell

Director, Georgia Emergency Management Agency

### Mr. Stanley McKinney

Vice President for Business Continuity Management  
Bank of America

### Professor Matthew S. Meselson

Professor of the Natural Sciences, Harvard University

### Dr. Steven Miller

Director, International Security Program,  
Kennedy School of Government

### Mr. Andrew Mitchell

Deputy Director, Office for Domestic Preparedness,  
Office of Justice Programs, U.S. Department of Justice

### Major General Paul D. Monroe, Jr.

Adjutant General, California National Guard

### Major General Phillip E. Oates

Adjutant General, Alaska National Guard

### Chief Charles Ramsey

Chief, Metropolitan Police Department, Washington, DC

### Lieutenant General (Ret.) James Terry Scott

Partner, Watson and Associates, TX

### Ms. Leslee Stein-Spencer

Chief, Division of Emergency Medical Services and  
Highway Safety, Illinois Department of Public Health

### Chief Darrel Stephens

Chief, Charlotte-Mecklenburg Police Department, NC

### Dr. Jessica Stern

Lecturer in Public Policy, Kennedy School of Government

### Chief Steve Storum

Assistant Chief, Phoenix Fire Department, AZ

### Sheriff Patrick J. Sullivan, Jr.

Sheriff, Arapahoe County, CO

### Mr. Ralph Timperi

Assistant Commissioner, Massachusetts Department of  
Public Health and Director, Massachusetts Department of  
Public Health State Laboratory

### Chief Alan D. Vickery

Deputy Chief, Special Operations,  
Seattle Fire Department, WA

### Dr. Frances Winslow

Director, Office of Emergency Services, San Jose, CA

---

## Executive Session Staff

**Arnold M. Howitt**  
Director

**Juliette Kayyem**  
Executive Director

**Rebecca Storo**  
Assistant Director

**Robyn Pangi**  
Research Associate

**Patricia Chang**  
Research Assistant

**Rebecca Horne**  
Project Assistant