

FROM THE STOREFRONT  
TO THE FRONT LINES:

*The Private Sector  
and Homeland  
Security Investment*



**BOARD OF DIRECTORS**

**THE HONORABLE CHARLES BASS**  
*New Hampshire*

**CHARLES KOLB**  
*Committee for Economic Development*

**PAM PRYOR**  
*Convoy of Hope*

**CECILIA MARTINEZ**  
*Executive Director*

**FROM THE STOREFRONT TO THE FRONT LINES:  
THE PRIVATE SECTOR & HOMELAND SECURITY INVESTMENT**

**PROJECT DIRECTORS**

**TINA GUTHRIE**  
*Reform Institute*

**ROBERT W. KELLY**  
*Managing Partner*  
*CenTauri Solutions, LLC*  
*Senior Advisor, Reform Institute*

*Editor*

**CHRIS DREIBELBIS**  
*Reform Institute*

**The Reform Institute**  
**300 North Washington St, Suite 600**  
**Alexandria, VA 22314**

**Tel (703) 535-6897**  
**Fax (866) 863-5510**

**[www.reforminstitute.org](http://www.reforminstitute.org)**



## HARNESSING TECHNOLOGY AND BUILDING A MORE RESILIENT AMERICA: A MESSAGE FROM SENIOR ADVISOR ROBERT W. KELLY

The United States recently observed anniversaries regarding the terrorist attacks of September 11, 2001 and Hurricane Katrina in late August 2005. The repercussions of these tragic events still haunt us. The indelible images of suffering and destruction and of the heroic efforts of first responders and ordinary citizens remain with us. Another legacy of these episodes is the lingering concern over our ability to respond to and bounce back from a catastrophic event.

In the case of both September 11 and Hurricane Katrina, first responders were hampered in their efforts by the lack of proper equipment and the inability of responders in different agencies to communicate with each other. The World Trade Center in New York City was chosen as a target on 9/11 because it represented America's economic power. The major stock exchanges in New York were closed for several days after the attacks and financial markets remained anxious long after the attacks, which exacerbated a recession that was already underway. In the aftermath of Hurricane Katrina, damaged and destroyed offshore oil platforms and refineries in the region caused a significant spike in gas prices across the country. Damaged infrastructure impeded efforts to assist and evacuate victims in the Gulf Coast and affected the shipping of goods to and through the region. The Gulf Coast is still far from recovering economically from the disaster and progress in rebuilding the infrastructure there has been slow.

Much of the emphasis at the federal level remains on preventing another terrorist attack. Although authorities deserve much credit for the absence of any terrorist attacks on U.S. soil since 9/11, we cannot afford to ignore the fact that our enemies are still actively trying to strike us again, nor can we prevent natural disasters from occurring. The U.S. must do more to strengthen the resiliency of our critical infrastructure and supply chain so that the nation can withstand a catastrophic event without severely disrupting economic and social activity. Channeling the technological advancements being generated by our entrepreneurial economy towards developing a more resilient society will vastly improve our security prospects.

Resiliency will be the major focus of the Reform Institute's work in homeland security. This is the first of a series of reports to advance innovation, collaboration, and leadership in building a more resilient nation. This report examines a cross section of technology solutions that involve the following sectors: emergency response, port security, transportation, and interoperability. The Institute will also study critical issues such as cargo container security, protecting the global supply chain, and the link between drug trafficking and terrorism in upcoming monographs.

Robert W. Kelly  
Managing Partner, CenTuari Solutions, LLC  
Senior Advisor, Reform Institute



## ACKNOWLEDGEMENTS

Tina Guthrie

Robert Kelly

Matthew Freedman

Suzanne Luft

Cecilia Martinez

Chris Dreibelbis

Motorola, Inc.

Sprint Nextel

C-AT, Communications-Applied Technology

Planet Associates Inc.

CSX Transportation

Iridium Satellite LLC

ICx Technologies, Inc.

Powell Fabrication & Manufacturing, Inc.

Foster-Miller, Inc. – QinetiQ North America

Google

Alcatel Lucent

General Electric Global Research



## TABLE OF CONTENTS

<i>A Message from Senior Advisor Robert Kelly</i> .....	i
<i>Acknowledgements</i> .....	ii
<i>Introduction: Embracing Private Technology for the Public Good</i> .....	1
<i>Chapter 1: Emergency Response</i> .....	3
<i>Chapter 2: Port Security</i> .....	8
<i>Chapter 3: Transportation</i> .....	11
<i>Chapter 4: Interoperability</i> .....	14
<i>About The Reform Institute</i> .....	21





## INTRODUCTION

# EMBRACING PRIVATE TECHNOLOGY *for the Public Good*

Cutting-edge technologies such as Global Positioning System (GPS) tracking devices, geospatial mapping, and wireless availability have become pervasive in our society. While the average consumer has benefited immensely from new technologies and the innovative uses developed for them by enterprising firms in a competitive market, the public sector has yet to effectively capitalize on these advancements. In order to build a more secure and resilient nation, we must embrace private sector innovations and technology and develop ways to implement them in a cost-effective manner. Taking advantage of the new technologies coming to the forefront every day must be a critical component of the government's homeland security strategy.

The Department of Homeland Security (DHS) and the individual state homeland departments must reform their practices in order to adopt technology that will have a substantial impact in advancing our national security. Although technological advances offer promising solutions to some of our greatest national security concerns, homeland security authorities must be discerning consumers in procuring such technology. As former Homeland Security Secretary Tom Ridge warned in an interview with IBIA, the government needs to be careful it isn't persuaded to buy technology that does not meet mission requirements. "Vendors are strong in this town," he

said, referring to Washington. "The government can end up buying technology that might not be the most appropriate for a task and have only a marginal impact." Lessons from the private sector offer guidance for the public sector. The private sector invests in technology using a return on investment model. It is highly motivated to purchase technology that is not only appropriate for the task but that also will yield the greatest return. This mindset is sorely lacking in the public sector.

**IN ORDER TO BUILD A MORE  
SECURE AND RESILIENT NATION,  
WE MUST EMBRACE PRIVATE SECTOR  
INNOVATIONS AND TECHNOLOGY  
AND DEVELOP THEM IN A COST-  
EFFECTIVE MANNER.**

Entrepreneurial companies are constantly researching and developing new technologies to support and enhance existing products. According to the *Wall Street Journal*, sixty-three percent of cell phones sold in 2007 will be equipped with a GPS locator. A new cell phone program started by a company called **Loopt** uses GPS tracking to allow users within the network

to locate other participating users utilizing an online map or a cell phone that has access to the internet.<sup>1</sup> Such off-the-shelf technologies could have major implications for homeland security and emergency preparedness personnel. During a disaster, these new GPS linking networks could aid emergency responders in search and rescue efforts. Friends and family could go online and find the location of loved ones affected by a disaster, which could then be passed on to Red Cross and emergency responders.

New technology companies, such as Loopt, have the potential to become an invaluable partner to DHS and emergency preparedness personnel, allowing them to be more effective when conducting search and rescue operations. Partnering with the private sector in advance also increases coordination effectiveness of first responders and the private sector. These partnerships also establish strong working relationships between the private and public sectors that pay long-term dividends.

Innovative technologies offer benefits to homeland security beyond aiding first responders. This report identifies and pro-

motes technologies and solutions that present a high probability of success in decreasing our national vulnerabilities to specific threats.

The Reform Institute is dedicated to promoting innovation, collaboration and leadership in homeland and national security policy. Developing and applying cutting-edge innovations in protecting the nation will require extensive collaboration between the public and private sectors. The report includes examples of successful public/private partnerships in producing and deploying new technologies. Finally, as shown in these examples, leadership from homeland security authorities is required to adapt these technologies for use in the demanding public safety and homeland security environment.

The goal of this report is to raise awareness within the Department of Homeland Security (DHS), Congress, state and local government, and state homeland security centers on ways in which to capitalize on technological advancement in the private sector for the public good. In addition, the report provides insight into the private sector's ability to reconstruct new or existing technologies in order to protect our nation.





## CHAPTER 1

# EMERGENCY RESPONSE: *Empowering First Responders and Citizens*

**E**mergency responders including police, fire and emergency medical service are on the frontlines of any major catastrophe and cannot afford to be hindered by lack of proper tools. Emergency responders are primarily funded by the states. The federal government also provides monies to the states through the Homeland Security Grant Program.<sup>2</sup> The recently passed legislation enacting many of the recommendations of the 9/11 Commission titled, *Improving America's Security Act of 2007*, allows for a greater percentage of the funds allocated to the states to be distributed according to a risk-based formula, with the fixed funding to the states reduced.<sup>3</sup> The fixed pool of money from the federal government to the states has been shrinking over recent years, and the new requests for grants need to be more targeted to the new funding mechanism. This chapter will highlight technology that is already in existence, and that can be updated for homeland security use in the states, and highlights some new technologies that are on the horizon.



### **Alabama Googles “Help”**

In past articles and Congressional testimony, the Reform Institute has noted that geospatial mapping programs such as **Google Earth** provide an excellent resource for empowering emergency responders and the public to better plan and make decisions in times of disaster. As we witnessed in New Orleans with Hurricane Katrina,

the immediate aftermath of a catastrophe is a crucial period when individuals often must make decisions and take action before authorities can respond. Empowering individuals to create and share response plans with their families or co-workers remains an essential unmet need. Google Earth is an off-the-shelf technology that can be enhanced to meet the needs of emergency responders and the public.

Alabama has partnered with Google Earth to create a new program called “Virtual Alabama.”<sup>4</sup> The Alabama Department of Homeland Security (AL DHS) states that this program allows users to view a wide variety of information, including infrastructure, evacuation routes, flood zones,

**“THE GOOGLE EARTH ENTERPRISE HAS PROVIDED A HIGHLY EFFECTIVE FRAMEWORK IN WHICH TO SUPPORT PUBLIC SECTOR PROGRAMS IN ALABAMA.”**  
**—ALABAMA STATE HOMELAND SECURITY OFFICE.**

school districts and watersheds. Agencies using the program access this information through a secure, Web-based application. The program began by creating a database of police stations, hospitals, utility lines, and other pertinent infrastructure. This was done through a collaborative effort from all the counties in the state. All government workers have access to the website, and can either send in their information, or they can upload their information directly to the online program. The platform allows them to create 3D modeling of buildings, critical infrastructure mapping, and emergency evacuation routing.

“What makes Virtual Alabama so remarkable is the input and collaboration with counties and other state agencies,” said Alabama Homeland Security Director Jim Walker. “We are literally building this program from the ground up and it is very encouraging to see all levels of government and industry working so well together. It’s really a grassroots effort that allows the people who will benefit from the program to help create it.”

According to AL DHS, future applications of the ongoing project are to include: delivering detailed views of the interiors of buildings, including furniture and live footage; directing responder teams in emergencies through the platform; overlaying real-time data (traffic, etc.) with route mapping to better manage and control resources; and integrating a public emergency broadcast system. “The Google Earth Enterprise has provided a highly effective framework in which to support public sector programs in Alabama. As a platform, it has helped produce the common operational

picture needed to protect lives and safeguard Alabama citizens in times of man-made or natural disasters. Having a secure, dynamic, common information-sharing platform has allowed Alabama to reach the next level in emergency preparedness and disaster management,” according to the state homeland security office. “When a tornado hit the state on March 1, the Federal Emergency Management Agency, National Guard and other organizations helping in the clean-up were able to connect to the site and find useful data on gas pipelines, property owner names and other pertinent information.”

The program is currently operational in 56 out of 57 counties with more than 1500 users representing hundreds of agencies. The success of the program will depend on how the Alabama state government uses the new web portal to inform the public during an emergency. In order to be efficient, the public will need timely information on evacuation routes, hospital and shelter availability and closures, and availability of water and fuel during evacuation delays. It is critical that key players in all hospitals, shelters, media outlets, and the Department of Transportation have access to update the information online during an emergency. Because situational awareness is the first priority in an emergency, access to the system for these key players will provide important management tools for crisis managers and first responders. The public will also be better informed as a result of this cohesive effort by the state.

Alabama and Google Earth have done commendable work in coordinating this initial effort. By manipulating this program to make it more robust, the public will be provided with the most up-to-date information possible. This also provides the opportunity for individuals to find the information themselves online or through the local media without burdening the already overwhelmed emergency responders.

### **Electronic Mapping That is Easy to Use and Distribute**

During a major catastrophe, first responders need to have access to the most up-to-

date information available. During Hurricane Katrina in 2005 incomplete information relayed between responders at the scene and officials in Washington, namely the Federal Emergency Management Agency (FEMA) and DHS, exacerbated the chaotic situation. Initially, DHS thought that there was only one location where the survivors had been positioned; they had assumed that the Superdome and the Convention Center were the same location. If there was a more up-to-date mapping capability, this confusion could have been negated. Both maps would have been distributed to all parties, and would have provided situational awareness to all involved. In addition, federal authorities would have had a clearer picture of the amount of people that needed food, water, supplies, and eventual evacuation.

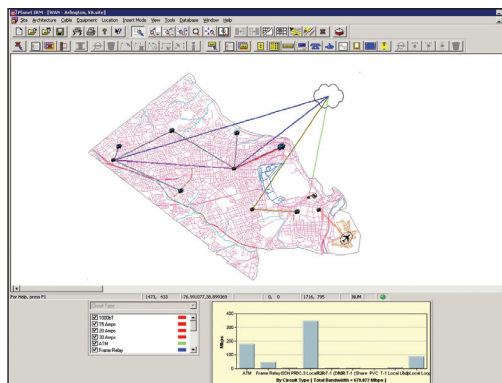
**Planet Associates Inc.** is looking to solve many of these distribution problems.<sup>5</sup> The company has created an Intelligent Infrastructure PDF (iiPDF) system targeted to improve situational awareness for emergency responders, state emergency management personnel, FEMA, and DHS. This device would send floor plans, maps, and other details needed to the first responder, which would be readable in PDF format. The newer PDF version also includes the ability to view embedded data and click through the documents in a layered approach. This will allow information to pop-up and bring documents that contain geospatial data, CAD drawings, maps, and spreadsheet data.

Ideally these new software platforms should be easy to use and require little training. This system should only require one to two days for training and because it uses a PDF format, which most people have used in their day-to-day life, it uses an existing technology that would be easily adopted.

### Texting Alerts on Campus

The recent tragedy at Virginia Tech University highlights the need for increased preparedness at our schools. On April 16, 2007, Seung-Hui Cho, a Virginia Tech student, murdered 32 people on campus and injured 25 before he committed suicide. The university's response to the incident

has been criticized for not alerting students to the shootings and encouraging them to stay in their dorm rooms. The first shooting occurred on campus at 7:15 a.m. and the university did not inform students until 9:26 a.m. that there had been a shooting on campus. The information was relayed over e-mail. When the second incident occurred there was a second e-mail sent within eight minutes of the shooting warning students to stay indoors and to lock the doors. Another alert system that could have been used to warn students was the school's siren, but it was not considered because it was only used for weather-related warnings. The school did not have a mechanism in place to inform all students of the shooting. E-mails are not useful to students in transit or those already in the classroom.



According to M:Metric researchers, 16.6 million college students have cell phones, which represents 95 percent of the 17.5 million full- and part-time college students counted by the Census. These statistics point to a remarkable opportunity to provide emergency information to students in a timely manner during a crisis. Texting and instant messaging over cell phones represent contemporary modes of communication that are widely used, especially by members of Generation Y (ages 18-30). These technologies can be used to inform communities about pending natural disasters or other emergencies.

Since the school shootings, Virginia Tech has contracted with the **National Notification**

**Network**, which will provide cell phone alerts, phone calls directly to dorm rooms, and instant message pop-ups working with AOL, MSN, and Yahoo starting at the beginning of the new fall semester.<sup>6</sup>

**Roam Secure Inc.**, another alert notification company, holds a current contract with Virginia state agencies to provide this important service.<sup>7</sup> The company's most recent contract is with the University of Mary Washington in Virginia. The contract will cost \$40,000 with annual renewal fees. This service will also provide text alerts to cell phones during an emergency to all students and faculty, nearby graduate and professional studies students, and to parents. "The recent tragedy at Virginia Tech emphasized the importance of having such a system in place," Teresa Mannix, director of news and public information at the university, said in an e-mail. "It is our goal that we can be prepared for any crisis."

Many universities across the country have now begun to assess the viability of text alert systems, including colleges in Texas, Florida, New York, and Pennsylvania. This important tool has also been recognized by such diverse institutions as the U.S. Air Force, Homeland Security's National Medical Response Teams, the Red Cross, and the Los Angeles County Department of Health. **Mir3**, based in San Diego, holds the contracts with these entities.<sup>8</sup> The company also holds smaller contracts with local grocery stores that utilize the service for removing recalled food items.

Preparedness plans must include redundancies. There is no one plan that will notify everyone across campus, but involving more people in the network and in the decision making process will make communities safer and more resilient in the long term. Also, in addition to alerting students for prevention, additional steps should be taken to prepare for response. For example, establishing short range secure wireless mesh systems on college campuses that first responders could use to access interior video security cameras in a hostage situation would provide additional situational awareness useful for incident response.

### Using Wi-Fi to Connect Responders

After a large-scale disaster, such as the bridge collapse in Minneapolis, Minnesota in August 2007, triage units are set up in order to provide immediate care to the victims of the event. This can be an extremely confusing time, trying to shuffle patients to hospitals that may already be full or over-capacity. Depending on the amount of injuries and casualties, it can be very difficult for family and friends to locate loved ones because there is no database to track each person's whereabouts. New wireless technologies are now allowing the process of triaging patients to be more efficient, and less of a logistical nightmare.

According to Jonathan Teich, professor of medicine at Harvard University and an attending physician in emergency medicine at Brigham and Women's Hospital (BWH), "It's very hard to keep those patients in track and make sure we are handling all of the most serious cases right away." The University of California, San Diego is also starting an initiative called the Wireless Internet Information System for Medical Response in Disasters project (WIISARD). The most recent drill was held last summer, and all on-scene first responders and public health personnel received iTags, which are electronic Wi-Fi tags used to enter the data. The Wi-Fi enabled personal digital assistants (PDAs) were able to scan a barcode on the tags that would catalog patient information including health status and medicines that had been distributed; the scanner was also used to upload patient information.

During the exercise, supervisors were given a Wi-Fi enabled tablet to assess the scene, and scan the victims' barcodes in order to track which hospitals would be receiving specific patients. All data was then sent to the database at the university and then forwarded to the incident command center.

The company **Motion Computing Inc.**, based in Austin, Texas, uses the technology to help with interoperability issues to connect

other wireless systems.<sup>9</sup> This device works to improve workflow with single integrated data capture and allows for facilitation of real-time communications. It was originally used in consumer electronics and gaming applications. Now this technology has been reinvented to provide much needed assistance to our emergency responders.

It is important to note that for many of the technologies mentioned above to be available, operability of the communications infrastructure must exist. During disasters the very infrastructure that these technologies rely on to be functional is impaired due to the destructive nature of natural or manmade events. In order for the technologies to be available for emergency response, plans and arrangements must be in place prior to a disaster at local, state and

federal levels to allow for the necessary restoration of the communications infrastructure.

The White House *Federal Response to Hurricane Katrina: Lessons Learned* report includes the recommendation for commercial rapidly deployable communications capabilities to restore operability and achieve interoperability. It is important that federal, state and local jurisdictions have arrangements to deploy communication capabilities to augment existing infrastructure impaired during a disaster and increase capacity in areas saturated with emergency response users. **Sprint Nextel** has Emergency Response Teams with scalable capabilities to rapidly deploy mobile infrastructure with support teams managing the entire effort and providing support to end users. Operable communications are essential to emergency response.



## CHAPTER 2

# PORT SECURITY: *Using Innovation to Protect Shipping*

Securing our ports is a critical aspect of protecting the supply chain. America's ports are an integral part of the U.S. economy. According to a study conducted by Martin Associates, United States deep-draft seaports and seaport-related businesses generated approximately 8.4 million American jobs and added nearly \$2 trillion to the economy.<sup>10</sup> A terrorist attack at a U.S. port or a catastrophic event that causes ports to shut down would severely disrupt economic activity. Exploiting technology to enhance port security will contribute substantially to strengthening the resiliency of the U.S.

Port security has been a major focus of recent action in Congress. The new law implementing many of the 9/11 Commission recommendations that had not previously been addressed will require 100 percent scanning of cargo headed for American ports by the year 2012.<sup>11</sup> Technology is now at the forefront of this implementation requirement. Currently, DHS pre-screens many of the shipping companies; once they are prov-

en credible all of their containers are considered safe and not individually scanned. The screening process is inadequate because it assumes that the container is secure throughout the transport process. Technology exists that can neutralize this concern by guaranteeing container security throughout its travel.

### Container Security Devices

New devices are helping to contain the fears that the next dirty bomb can be brought into the

country through our shipping lanes. A container security device (CSD) has been manufactured that will lock the cargo doors from the inside. The system designed by the Dutch firm **ZOCA** locks and unlocks the device remotely.<sup>12</sup> Handheld devices are distributed to customs officials and can scan and relay



the barcode information back to the company for verification. The company also verifies the security code and the coordinates before access is granted to the container. Many companies use GPS and global precipitation measurement

(GPM) technologies in order to track cargo, but because these technologies are not available everywhere, ZOCA partnered with **Iridium Satellite** system to monitor shipping containers remotely to further reduce the threat.<sup>13</sup>

**General Electric Global Research** has also been investing time and money into the area of port security research.<sup>14</sup> Their first generation cargo security technology includes a container security device similar to the device that ZOCA has created. The CSD is palm-sized and attaches to the doorjamb inside the container. The CSD communicates its location and when and where it has been opened to a wireless reader at the port. When the container arrives at the port, the customs officials have access to this information as well.

While these technologies are improving the safety of our commercial traffic, there is still concern that the container walls can be breached and that the cargo container can be penetrated by simply removing the entire door. General Electric is focusing its research to include security provisions to address these concerns. Light sensors and motion sensors can be added to the interior of the container, which would alert the manufacturers and customs officials if someone has entered the container through the doors or through the walls. In addition, General Electric VeriWise technology uses a multi-sensor network to track the cargo and report on environmental conditions of the cargo, such as temperature. This technology could be moved inside of the cargo container at the beginning of its delivery.

### Protecting Ships

Cargo ships are not immune from attacks either. The USS Cole was attacked in 2000 by a small boat carrying explosives. In 2002, the Limburg oil tanker was attacked by a small boat filled with explosives, which killed one crew member and sent more than 90,000 barrels of oil into the Gulf of Aden.<sup>15</sup> Concerns over attacks on the shipping industry were understandably elevated after September 11, 2001.

Small boat attacks on Liquid Natural Gas (LNG) ships are a particular concern for the state

of Massachusetts, where LNG tankers and oil product tankers dock and unload fuel near residential areas. The explosion that would result if a LNG ship is attacked would be disastrous and could kill thousands in its path, according to a study on the vulnerability of Tractabel's Everett Boston facility.<sup>16</sup> Authorities closed Boston to LNG imports immediately following September 11, 2001, and LNG tankers bound for the Massachusetts port still require U.S. Coast Guard escorts while 200 miles at sea.<sup>17</sup>

**ACCORDING TO A STUDY CONDUCTED BY MARTIN ASSOCIATES, UNITED STATES DEEP-DRAFT SEAPORTS AND SEAPORT-RELATED BUSINESSES GENERATED APPROXIMATELY 8.4 MILLION AMERICAN JOBS AND ADDED NEARLY \$2 TRILLION TO THE ECONOMY.**

The future locating of LNG facilities in Boston and other areas is still a concern for local residents and state and local politicians. In a letter to the Federal Energy Regulatory Commission opposing an LNG facility planned near the city of Fall River, then-Governor Mitt Romney of Massachusetts explained that, "There is simply no way that (it) makes sense to site an LNG facility in this location in the post 9/11 world."<sup>18</sup>

In order to address these security issues and stop a small boat attack, **Foster-Miller, a QinetiQ** company, has proposed development of an advanced Boat Trap system.<sup>19</sup> According to their website, Boat Trap is a non-lethal, ballistic net that is deployed from a helicopter at high speed to ensnare the propellers of a targeted speedboat, which would cause the craft to stop immediately. The system was tested in 2005 at Camp Lejeune, North Carolina and at South Padre Island, Texas, and at CAPEX demonstrations in Honolulu, Hawaii with 100 percent success. In addition to homeland security pro-

tection for ports, the new system could also be used by the Coast Guard for drug interdictions.

Ships can also be targeted underwater by individuals or with explosive devices. The Underwater Port Security System (UPSS) is a combination of an Underwater Inspection System and an Integrated Anti-Swimmer System. The UPSS is a portable device that can be used with any ship. The Underwater Inspection system uses divers or a remote device that can be used when conditions are dangerous to look for any evidence of tampering with the hull of the ship or devices under the piers.

The Integrated Anti-Swimmer system uses high-frequency sonar images to detect that it is indeed a swimmer and not some sort of marine mammal or another object. The Coast Guard has also tested this system with swimmers to try to fool it. According to Petty Officer 2nd Class Jacob Smith, “We’ve had the divers go at the system at all speeds and from all angles, and it detects them every time.”

### **This Fido Needs No Bone**

The *Support Anti-Terrorism by Fostering Effective Technologies Act of 2002* (SAFETY) was enacted by Congress to encourage the development and deployment of new and innovative anti-terrorism products and services by providing liability protections. The law affords significant legal liability protections for providers of Qualified Anti-Terrorism Technologies, which covers both products and services. This designation has encouraged the development and operation of anti-terrorism technologies that otherwise might be delayed or abandoned because of liability concerns.

The Fido unit, created by a Washington D.C. based company, **ICx**, is one of the products with the SAFETY Act preferred status designation. Fido is a bomb sniffing device that is handheld or can be mounted on a vehicle or robot. The applications are widespread. The Transportation Security Administration (TSA) began pilot-testing the units to screen sealed liquid bottles, and the District of Columbia Department of Park and Recreation used them to scan the National Mall for explosives.

According to ICx’s website, “Fido explosives detectors utilize proprietary amplifying fluorescence polymers (AFP) to detect trace levels of explosive materials in parts per quadrillion (ppq). This level of detection is comparable to that of highly trained explosives detection canines, the gold standard in explosives detection technology. Unlike the alternative, the exquisite sensitivity of the Fido supports detection of both explosive vapor and particulates without the need to modify the system in any way. This unique design enables previously unheard of functionality for explosives detection equipment.”

The portability of the equipment is ideal in a port where it is not feasible to have a single checkpoint. There is also very little training involved with the equipment; this contrasts with that of a K-9 unit where the Explosive Detection K-9 course is a ten week program for the handlers and the dogs receive six weeks of training on explosive odors prior to meeting their handlers, according to the North American Police Work Dog Association. ICx is also working on long-term solutions to provide new low-cost, easy-to-use capabilities for the detection of explosives on fishing boats, container vessels, pleasure boats and other watercraft.





## CHAPTER 3

# TRANSPORTATION: *Practical Solutions to Protecting the Supply Chain*

The United States ground transportation system, which includes rail, mass transit and trucking, affects all Americans and is a vital part of our economy. According to the American Trucking Association, in 2005 truckers hauled 10.7 billion tons of freight. This accounted for 68.9 percent of the freight moved in the country. The railroads carried more than 30 million rail cars loaded with coal, chemicals, lumber, food and automobiles. Protecting critical infrastructure is essential to our economy. Only recently has rail and ground transportation received sufficient attention from federal policymakers. *Improving America's Security Act of 2007* will appropriate more than \$4 billion over four years for rail, transit, and bus security grants. Additionally, the bridge collapse in Minnesota has precipitated heightened interest in Congress in strengthening our aging infrastructure. Increased federal investment should complement efforts already being undertaken by the states and private companies.

Smuggling of weapons of mass destruction into the U.S. via trucks has always been a major concern, but border security must be balanced with sustaining the commercial activity that this nation relies upon. Many of the trucks that pass through our borders from Mexico and Canada are given special status under the North American Free Trade Agreement (NAFTA) and now under the Customs-Trade Partnership

Against Terrorism (C-TPAT) program. If the companies are certified under NAFTA or C-TPAT, they are allowed to move through the "Green Lane" at the border with an expedited inspection process.

### **Electronic Manifests**

In October 2006, U.S. Customs and Border Protection (CBP) mandated that foreign trucks transmit advance manifest information before entering the United States through land ports of entry.<sup>20</sup> Maine and Minnesota are the latest states to begin using the system; they have 90 days to use and test the system and will be fully operational beginning October 16, 2007.

Trucking companies are adapting to the new security demands and complying with the additional requirements. "CTA and the provincial trucking associations have been working directly with carriers, CBP and U.S. customs brokers to resolve technical issues in order to make e-manifest functional. This has been a difficult and long process, but much has been accomplished," said Canadian Transportation Authority Chief Executive Officer David Bradley in a press release.

Electronic manifests are an important tool in identifying potential smuggling attempts by workers and terrorists alike. Companies like **Maddocks Systems Inc.**, headquartered in Beachwood Ohio, are providing a valuable asset in the fight against



smuggling and terrorism. These electronic manifests also provide additional benefits to the carriers, including reduction of processing times at ports and the ability to track the status of crew, conveyances, equipment, and shipments, such as notices that shipments have arrived, are being held, or have been released.

### Emergency Shut-Off Valves

The transport of chemicals across the country also represents a serious public safety concern. Responding to the threat, the U.S. Chemical Safety and Hazard Investigation Board (CSB) issued a safety bulletin in June 2007 to emphasize the importance of installing, testing, and maintaining chlorine detection and emergency shutdown devices on chlorine rail car transfer systems.<sup>21</sup> The chlorine threat is not hypothetical. In Missouri, a 2002 chlorine release caused by a faulty emergency shutdown system discharged 48,000 pounds of chemicals into the air. Hundreds of residents were evacuated or sheltered-in-place.

According to the Occupational Safety and Health Administration (OSHA), severe acute effects of chlorine exposure in humans have been well documented since World War I, when chlorine gas was used as a chemical warfare agent. Other severe exposures have resulted from the accidental rupture of chlorine tanks. These exposures have caused death, lung congestion, pulmonary edema, pneumonia, pleurisy, and bronchitis.<sup>22</sup> Chlorine is an important chemical used in the manufacture of bleach, pharmaceuticals and for water purification.

The CSB has found that approximately 30 percent of rail cars do not have emergency shut-down devices installed. Private manufacturers are producing emergency shut off valves that fill this need.

**Powell Fabrication and Manufacturing Inc.’s** Emergency Gas Shut Off Valve Closure Systems are designed to prevent significant releases of hazardous gases like chlorine.<sup>23</sup> In the case of an accidental release, the emergency valve closure system will close the valves in ten seconds or less, effectively preventing further release from the container.

Instituting the CSB’s recommendations throughout the rail system is essential to protecting our communities. “Chlorine is a very useful, but highly toxic substance that needs appropriate safeguards to prevent releases and protect the public,” said safety board member John Bresland. Technological advances available on the market will facilitate the safe and orderly transport of this key commodity.

### Protecting the Rails Through Public/Private Partnerships

Hazardous materials travel through major metropolitan areas in the U.S on a daily basis. The nation’s economy is dependent on the movement of these materials across the country; were an attack to be carried out, the homeland security implications of such an attack would be enormous. An accident or terrorist attack against a train carrying hazardous materials while traveling through a heavily populated area could endanger millions of people and severely disrupt an indispensable part of our transportation system. Close collaboration between the public and private sectors is required to deal with this challenge.

Authorities in New Jersey, New York and Kentucky have formed partnerships with **CSX Transportation (CSXT)** to address this issue.<sup>24</sup> “Ensuring that our freight rail system is secure is a top priority for my administration,” said New Jersey Governor Jon Corzine. “CSXT deserves credit for stepping up and serving as a model for a collaborative public/private security initiative.”<sup>25</sup>

The partnership between the three states and the rail industry enhances security by facilitating communication and information sharing between relevant government authorities and CSXT regarding resources and the railroad's infrastructure. CSXT has also allowed access to its Network Operations Workstation (NOW System) to state security and law enforcement officials. According to CSXT, the system is an online tool that enables state officials to independently track the location of the trains and provides contents of rail cars being hauled to each state. All states will analyze the data through their local intelligence fusion centers.

Access to the system allows states to pro-

vide an enhanced situational awareness to first responders during an emergency. The list of chemicals would be provided as well as location of the train. Because the events are being monitored on a daily basis, any emergency that arises will be responded to immediately. This improves the effectiveness of the clean-up and the response time of the first responders. In addition, New Jersey, New York, Kentucky and CSXT are taking further steps by conducting joint law enforcement and emergency responder training, providing the state and their communities a list of hazardous materials, and undertaking joint initiatives to reduce vulnerabilities at critical points.



## CHAPTER 4

# INTEROPERABILITY: *The Missing Link in Emergency Response*

**T**he 9/11 Commission cited that the inability to communicate was a critical element at the World Trade Center, Pentagon, and Somerset County, Pennsylvania crash sites, where multiple agencies and multiple jurisdictions responded. The commission found that compatible and adequate communications among public safety organizations at the local, state, and federal levels remains a problem and must be addressed. States have begun to recognize how vital it is for all emergency responders to be able to communicate quickly and effectively in times of emergency.

In general, interoperability refers to the ability of emergency responders to work seamlessly with other systems or products without any

special effort. Wireless communications interoperability specifically refers to the ability of emergency response officials to share information via voice and data signals on demand, in real time, when needed, and as authorized. For example, when communications systems are interoperable, police and firefighters responding to a routine incident can talk to each other to coordinate efforts. Communications interoperability also makes it possible for emergency response agencies responding to catastrophic accidents or disasters to work effectively together. Finally, it allows emergency response personnel to maximize resources in planning for major predictable events such as the Super Bowl or an inauguration, or for disaster relief and recovery efforts.

There are a variety of challenges to interoperability: some are technical, some financial, and some stem from human factors such as inadequate planning and lack of awareness of the real importance of interoperability. According to a report published in February 2003 by the National Task Force on Interoperability, the emergency response community views the following as the key issues hampering emergency response wireless communications:

- Incompatible and aging communications equipment;
- Limited and fragmented budget cycles and funding;

**“COMMUNICATIONS IN  
NEBRASKA IS NOT GEE-WHIZ.  
WHAT WE’VE DONE IS NOT  
FLASHY, BUT IT WORKS.”**  
—AL BERNDT, NEBRASKA  
EMERGENCY MANAGEMENT  
AGENCY ASSISTANT DIRECTOR

## Motorola in the States



*"Wireless communications is a critical tool for our nation's public safety agencies, especially given today's heightened homeland security concerns. It is the mechanism for providing*

*our first responders with the right information at the right time and in the right place, whether that information is transferred via voice, data, or images. Spectrum designated for exclusive use by public safety is the lifeline to their emergency response, detection and prevention capabilities. Simply put, without access to adequate spectrum, wireless communications cannot take place, effectively and ubiquitously."* Gregory Brown, President and Chief Operating Officer of Motorola, in prepared testimony before the U.S. House of Representatives Subcommittee on Telecommunications and the Internet, June 11, 2003

The State of Michigan "Michigan Public Safety Communications System" (MPSCS) provides a perfect example of statewide shared networks that serve the communications needs for multiple levels of government. The August 2003 blackout, which was the largest in United States history, proved the value of MPSCS. While commercial wireless carriers were failing due to overuse and lack of emergency power systems at their tower sites, MPSCS continued to provide dependable uninterrupted communications to its users. MPSCS also played a role to State of Michigan Emergency Management through its Network Communications Center,

by identifying the blackout area through its alarm and control capabilities. Recently, MPSCS has provided interoperable communications for multiple agencies for large-scale events like the 2005 All-Star Game and the 2006 Super Bowl.

STARCOM21 is a statewide digital Project 25 (P25) trunked mobile radio system built, owned and operated by **Motorola** in partnership with the State of Illinois. STARCOM21 provides public safety agencies with the sophisticated tools they need to do their jobs more effectively plus the interoperability to allow communications with federal, state and local agencies. Participating public safety agencies pay Motorola a monthly fee, based on a contract-specified service level to utilize the network.

Another essential quality of the STARCOM21 solution is the incorporation of 700 MHz spectrum into the design. STARCOM21 users have the opportunity to immediately take advantage of this additional spectrum since most of the State of Illinois is clear of the incumbent TV broadcasters in the band. The STARCOM21 architecture will accommodate the new spectrum and allow for continued growth of the network.

New spectrum provides the needed capacity for the expansion and continued build-out of mission critical systems. The DTV bill which Congress recently passed will clear 24 MHz of new spectrum for critically important public safety interoperable communications and provide \$1 billion for new public safety radios. The new 700MHz spectrum can provide a graceful migration path to P25 standards-based solutions and will bring added features.

- Limited and fragmented planning and coordination;
- Limited and fragmented radio spectrum; and
- Limited equipment standards.

### Linking Responders

Law enforcement, fire service, emergency medical service, and other emergency response personnel are making progress towards effective and modern mission critical communication systems. Spending habits in the states are also reflecting this focus. Federal grant funds

have shifted from spending 28 percent on communications equipment in 2003, to over 70 percent in 2006. Much of the communications equipment used by emergency responders is being upgraded to the Project 25 (P25) suite of standards-based digital equipment, which improves communication between state and local governments and between neighboring local jurisdictions. A partnership among user representatives from federal agencies, state and local governments, plus industry manufacturers is driving a standards process that enables the

offering, competitive procurement, and operation of interoperable digital two-way wireless communications products and systems that meet mission critical needs of public safety practitioners.

**“HAVING AN ICRI WILL REALLY MAKE A DIFFERENCE BECAUSE WE RESPOND TO A LOT OF MUTUAL-AID SITUATIONS, AND IT WILL HELP US BRING EVERYONE TOGETHER AND HELP US DO OUR JOBS BETTER.”**

**—MOUNT LAUREL (NJ) POLICE DEPARTMENT  
LIEUTENANT JOSEPH LEHMANN JR.**

A key enabler for interoperability is the existence or planned deployment of statewide or regional public safety networks. Many states and regions have significant investments in large-scale shared networks. These networks offer a high degree of interoperability within their geographic coverage areas and can be linked to other networks through gateways. To date, thirty-one states have or are in the process of deploying statewide networks (three more are currently in procurement). Recent trends towards regional, multi-jurisdictional and multi-disciplinary approaches can meet the needs of city, county and local users while improving day-to-day mission effectiveness and incident response interoperability when needed.

In Nebraska, studies conducted as early as 1992 found gaps in radio coverage, outdated equipment, and incompatible communications systems. According to the assistant director of the Nebraska Emergency Management Agency, Al Berndt, “Communications in Nebraska is not gee-whiz. What we’ve done is not flashy, but it works.” With federal dollars, Nebraska has acquired hand-held radios and car-mounted mobile radios and pagers, built new towers, and replaced old dispatcher consoles.

While standards for compatibility and interoperability may address communications between disparate technologies, they do not address the need to communicate across systems and radios operating in different frequency bands. Multi-band and software defined radio technology will allow first responders to roam and operate directly on systems that employ different spectrum. To facilitate communications between urban first responders using an 800 MHz trunked radio system and a rural sheriff with a high band radio system, companies like **Communications-Applied Technology, C-AT**, a Virginia based, veteran-owned, small business telecommunications company, are looking to support state agencies and incorporate rapidly deployable solutions that will allow for quick set-up during a natural disaster or man-made incident.<sup>27</sup>

According to the company’s website, the Incident Commanders’ Radio Interface (ICRI) provides for tactical radio interoperability for emergency response personnel, and interconnects municipal public safety radios, state and federal radios and telephone in just a couple of minutes through the unmanned ICRI. It also helps to enhance the radio link between an emergency response team operating in areas of poor radio frequency transmission, such as in tunnels or buildings. DHS has also seen the value in providing small communities with tactical interoperable communications equipment. Under the Commercial Equipment Direct Assistance Program (CEDAP) program, FEMA distributed 71 of the ICRI devices to select smaller communities with populations of less than 100,000 people.

In New Jersey, the Mount Laurel police department has been a recipient of the CEDAP program. The interface has been extremely successful in solving the interoperability issues they have been having. The New Jersey State Police operate on 800 MHz and will be moving to the digital 700 MHz frequency in the near future. Other agencies in the area can be found on VHF and UHF. According to MLPD Lieutenant Joseph Lehmann Jr., “Having an ICRI will really

make a difference because we respond to a lot of mutual-aid situations, and it will help us bring everyone together and help us do our jobs better.” In the future cities may opt for other solutions including wireless infrastructure and Internet Protocol (IP)solutions, but because these alternatives are years away from functionality, an interface system will be extremely helpful for fire, EMS and law enforcement in the short term.

The challenge for the federal government in the area of interoperability does not end with funding for equipment. Equipment for our first responders is a priority, but along with that should come dedicated funding for maintenance, updating software, and on-going training for new software. If there is not an investment in the long term viability of the equipment, it will sit stationary and the federal monies will be wasted in the long run. Either the federal government needs to dedicate funding for long-term strategies or the states need to show that they can support this technology for long-term prior to receiving funding.

In addition to C-AT, **Motorola** is working to develop multi-band radio capability and software based waveforms to overcome frequency limitations to land mobile radio (LMR) based communications technology.<sup>28</sup> Motorola also recognizes that private IP networks and the Internet offer great potential for addressing interoperability barriers with the vast number of disparate systems in operation today. According to Bill Anaya, Motorola’s vice president of government relations, “as opposed to the new digital systems going in today that are based on the open P25 standard, many legacy LMR communications systems in use today are widely incompatible, they do not facilitate communication with users on other systems under normal operating conditions. Getting these disparate systems to support interoperability is a challenge due to different operating frequencies and types of technologies. Motorola is delivering IP-based interoperability solutions that can connect users on any network, any technology and any frequency band for voice interoperability.”

In 2005, the State of Georgia used funding from the Law Enforcement Terrorist Prevention Program to procure a statewide IP-based interoperability solution intended to address the communications challenges faced in metro Atlanta and other parts of the state. The state awarded a phased implementation contract to Motorola for a MOTOBRIDGE IP solution. Today, this phased approach to a regional system in metropolitan Atlanta is connecting disparate systems in lieu of a statewide system. Gradual deployment minimizes the budget impact while making steady progress toward the interoperability results needed by first responders in the region.

### **Aiding Emergency Personnel**

Hurricane Katrina brought many challenges for emergency responders. First responders had to contend with power outages, fires, flooding, and communications issues. Long distance communication was affected because the switch controlling the phone lines was located below sea level; with reports of flooding in the area, the switch had to be powered down. The flooding made it extremely difficult to get the personnel on site to gauge the extent of repairs.

**Sprint Nextel** partnered with the American Red Cross during Hurricane Katrina to provide wireless phones and service to enable critical communication in order to ensure speedy recovery of victims and distribution of supplies.<sup>29</sup> The company was preparing days before the storm hit by pre-positioning resources for the recovery efforts. The business continuity office referenced their Living Disaster Recovery Planning and ensured that all personnel were available and on-site to assist during the disaster. Within three days, the command post was up and running. The Sprint Nextel command post included a mess tent, showers, approximately 40 RVs and a helicopter that was used for initial damage assessments.

The company estimated that damages to its network infrastructure were between \$150-200 million. The infrastructure had been damaged over a 90,000 square mile, three-state

region. Retail stores were damaged and all the relief for impacted customers was very costly. According to Greg Fenell, director, business continuation, Sprint Nextel, “It’s pretty close to a worst case scenario; it is the largest escalation we’ve had in a long time. Our wireless and long distance networks were really impacted. The only thing worse would be a major earthquake in Los Angeles or San Francisco.”<sup>30</sup>

Through all this damage to their own operations, their Sprint Nextel Emergency Response Teams were directly involved in the distribution of Direct TalkSM-enabled mobile phones to emergency responders. “Direct Talk is an off-network walkie-talkie service that allows enabled phones to communicate handset-to-handset within a range of up to 6 miles (terrain, structures, and other environmental factors permitting), completely independently of any wireless network.” They delivered over 20,000 phones to 110 state, local and federal emergency personnel in the affected areas enabling operable and interoperable communications. They also deployed five Satellite Cell Sites On-Light Trucks in the affected areas to provide enhanced service and augment existing infrastructure damaged by the hurricane.

The assistance they provided to the states also enabled them to speed recovery to their own operations. Sprint Nextel personnel were placed in the Emergency Operations Centers (EOC’s) at the state and local levels. Through this partnership they could learn first hand which areas power was being restored to and could rapidly deploy personnel to those areas to restore phone service. Because the Sprint Nextel personnel were based in the EOC’s, this access also authorized them to move quickly through checkpoints to provide service to customers and to provide communication situational awareness to local and state officials. The partnership with the state, the American Red Cross and private business served an essential role in the response to this disaster. It not only facilitated returned service to the people in New Orleans, but also to the emergency responders and state authorities.

## A Capital Idea

**Alcatel-Lucent** has partnered with the National Capital Region in order to build a wireless broadband network needed to manage the many different municipalities in the region. This is the first wireless network established in the states for emergency response. This Regional Wireless Broadband Network will be based on off-the-shelf technology and will give the police and fire fighters access to send images through the network which could include blue prints, maps, and photos of suspected targets. Motorola also played a role in this broadband network by developing the mobile video application software used by the pilot system to enable and manage group video calls among multiple first responders in a user-friendly manner. These programs will provide enhanced capabilities for emergency responders and give them the tools necessary to protect our citizens.

The National Capital Region consists of the District of Columbia and 18 other jurisdictions in Virginia and Maryland. The coordination of all these jurisdictions requires a cohesive infrastructure plan for an effective interoperable communication network. “If we did this separately, we would end up with the interoperability problems like we have had in land mobile (radio) today,” Robert LeGrande, former interim chief technology officer for the District of Columbia said. “We all agreed to do the same technology and same frequency at the same time in a network-of-networks design. It gives us seamless roaming, seamless operability.” This network-of-networks will also provide for a layout for a potential nationwide plan for interoperability.

According to the National Governors Association, principles for a nationwide plan include:

- An integrated system-of-systems in regular use, which would allow all emergency responders to use and communicate through data, voice, and video with anyone that has access to the system in real time;
- The burden of federal interoperability should remain in federal hands;



- The burden of interoperability within the local, regional and tribal agencies should remain in the state government;
- Collaboration with neighboring agencies in the planning and acquisition of communications system; and
- Grant funding should be a priority for states and the federal government.<sup>31</sup>

Funding for the program is coming from the Department of Homeland Security’s Urban Area Security Initiative grants. The network will cost \$110 million under a five-year Indefinite Delivery Indefinite Quantity contract (IDIQ). The benefit of this contract allows for more jurisdictions to buy in at a later date. “The IDIQ allows for other cities to procure systems off this contract, gaining speed and efficiency in the process,” said Andy Smith, director of public safety for LGS, an Alcatel-Lucent subsidiary.

The challenge for the capital region initiative was coordinating the many municipalities to agree to work together on the same system and the same frequency. This hurdle was overcome. Once the system is up and running, the next challenges will include prioritizing access to the system, and communicating with other agencies on a regional basis. Inter-agency coordination is often hampered by the different lingo and nomenclature used by various agencies. Many times the language and acronyms that are used

in one agency are different from another. The federal government is seeking solutions to this problem.

The National Information Exchange Model (NIEM), a partnership of the U.S. Department of Justice and the U.S. Department of Homeland Security, “is designed to develop, disseminate, and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations,” according to their website.<sup>32</sup> “NIEM supports the day-to-day operations of agencies throughout the nation, and seeks to break down barriers to information sharing by developing standards for information sharing between communities of interest at all levels of government.”

### Conclusion

Local, state, and federal government emergency response employees deserve to have access to technology that will enable them to prepare, prevent and recover from all hazards including natural disasters, commercial accidents, and terrorist action against the United States. Technology that in many cases is already available should be used to prevent these catastrophes. Where such an event cannot be prevented, we must be resilient enough to mitigate its cascading effects. Our security and our future depend on our ability to learn from the examples above.

## Endnotes

1. Loopt Inc., <https://loopt.com/loopt/sess/index.aspx>.
2. State Contacts and Grant Award Information, The Department of Homeland Security, <http://www.dhs.gov/xgovt/grants/>.
3. United States. Cong. Senate. 110th Congress, 1st Session. S.4, Improving America's Security Act of 2007, 110th Congress. Congressional Bills, GPO Access. 4 January 2007 [http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110\\_cong\\_bills&docid=f:h1enr.txt.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h1enr.txt.pdf).
4. Virtual Alabama, August 24, 2007, <http://www.virtual.org/>.
5. Planet Associates Inc., <http://www.planetassoc.com/>.
6. 3n (National Notification Network), <http://www.3nline.com/company/index.php>.
7. Roam Secure, <http://www.roamsecure.net/>.
8. MIR3 Intelligent Notification, <http://www.mir3.com/>.
9. Motion Computing, <http://www.motioncomputing.com/>.
10. Martin Associates, "United States Port-Sector Economic Impacts – 2006," August 2007, <http://aapa.files.cms-plus.com/PDFs/Port%20Sector%20Economic%20Impacts%20Chart.pdf>.
11. Kean, Thomas H., Chair and Hamilton, Lee H., Vice-Chair. 9/11 Commission Report. National Commission on Terrorist Organizations. July 22, 2004. <http://www.9-11commission.gov/report/911Report.pdf>.
12. ZOCA, <http://www.zoca.nl/>.
13. Iridium Satellite LLC, <http://www.iridium.com/>.
14. General Electric Global Research, <http://www.ge.com/research/>.
15. United States Department of State, International Information Programs, Press Statement on USS Cole Attack. Updated November 16, 2006. [http://usinfo.state.gov/is/international\\_security/terrorism/uss\\_cole.html](http://usinfo.state.gov/is/international_security/terrorism/uss_cole.html).
16. Fay, James, *Spills and Fires from LNG and Oil Tankers in Boston Harbor*, March 26, 2003. [http://www.borderpowerplants.org/pdf\\_docs/boston\\_LNG\\_tanker\\_fire\\_impact.pdf](http://www.borderpowerplants.org/pdf_docs/boston_LNG_tanker_fire_impact.pdf).
17. The Jamestown Foundation, Al Qaeda And Maritime Terrorism, Part II, Volume 1, Issue 5. November 7, 2003. <http://jamestown.org/terrorism/news/article.php?articleid=23400>.
18. Reynolds, Mark, *Lloyd's likens LNG attack to nuclear explosion: U.S. regulators don't share the concerns of the top official at the world's second-largest commercial insurer*. The Providence Journal, September 21, 2004. [http://www.projo.com/massachusetts/content/projo\\_20040921\\_ma21ng.134600.html](http://www.projo.com/massachusetts/content/projo_20040921_ma21ng.134600.html).
19. Foster-Miller, Inc. - QinetiQ North America, <http://www.foster-miller.com/>.
20. United States Customs and Border Protection, ACE Overview for Truck Carriers – Mandatory Electronic Manifests. December 12, 2006. [http://www.cbp.gov/xp/cgov/newsroom/fact\\_sheets/trade/ace\\_factsheets/ace\\_overview/ace\\_carriers.xml](http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/trade/ace_factsheets/ace_overview/ace_carriers.xml).
21. U.S. Chemical Safety and Hazard Investigation Board. Emergency Shutdown Systems for Chlorine Transfer. No. 2005-06-I-LA. June 2007. [http://www.csb.gov/safety\\_publications/docs/CSBChlorineShutdownBulletin.pdf](http://www.csb.gov/safety_publications/docs/CSBChlorineShutdownBulletin.pdf).
22. Occupational Safety and Health Organization. [Hathaway et al. 1991; Gosselin 1984]. OCCUPATIONAL SAFETY AND HEALTH GUIDELINE FOR CHLORODIPHENYL (42% chlorine) <http://www.osha.gov/SLTC/healthguidelines/chlorodiphenylchlorine/recognition.html>
23. Powell Fabrication and Manufacturing Inc., <http://www.powellfab.com/>.
24. CSX Transportation, <http://www.csx.com/>.
25. CSX Transportation, Press Release, July 17, 2007. [http://www.csx.com/?fuseaction=media.news\\_detail&i=49292](http://www.csx.com/?fuseaction=media.news_detail&i=49292).
26. National Task Force on Interoperability. Safecom Program. What Public Officials Need to Know About Interoperability. February 2003. [http://www.safecomprogram.gov/NR/rdonlyres/4B5F0FC8-4339-407E-8AD8-08AEB931068/0/When\\_They\\_Cant\\_Talk\\_Lives\\_are\\_Lost\\_NTFFI\\_Brochure.pdf](http://www.safecomprogram.gov/NR/rdonlyres/4B5F0FC8-4339-407E-8AD8-08AEB931068/0/When_They_Cant_Talk_Lives_are_Lost_NTFFI_Brochure.pdf).
27. C-AT, Communications-Applied Technology, <http://www.c-at.com/>.
28. Motorola, [http://www.motorola.com/mediacenter/news/detail.jsp?globalObjectId=4939\\_4227\\_23](http://www.motorola.com/mediacenter/news/detail.jsp?globalObjectId=4939_4227_23).
29. Sprint Nextel, <http://www.sprint.com/index.html>.
30. Miller, Kevin C. *Hard Times in the Big Easy: Sprint Nextel's Response to Hurricane Katrina*, Strohl Systems. [http://www.recoverychronicles.com/MediaPR/\\_files/eNewsletter/53/SprintNextel.pdf](http://www.recoverychronicles.com/MediaPR/_files/eNewsletter/53/SprintNextel.pdf).
31. Trella, Joe, Strategies for States to Achieve Public Safety Wireless Interoperability, National Governor's Association, November 20, 2006. <http://www.nga.org/Files/pdf/0903INTEROP.pdf>.
32. National Information Exchange Model, <http://www.niem.gov/>.



## THE REFORM INSTITUTE'S UNIQUE, INDEPENDENT VOICE

The Reform Institute is a not-for-profit 501(c)(3) educational organization, representing a unique, independent voice working to strengthen the foundations of our democracy and build a resilient society. The Institute champions the national interest by formulating and advocating for valuable, solutions-based reforms in vital areas of public policy, including **homeland and national security, energy independence and climate stewardship, economic opportunity, immigration policy, and government and election reform.**

The Institute is committed to advancing a solutions-based reform agenda. Resolving the most intractable problems confronting our society will require fundamental reform at the core of our democratic system. As a nonpartisan public policy organization, the Institute conducts objective research and analysis on critical issues and promotes reforms that restore Americans' faith in government and the political process.

The Institute was founded in 2001 by a group of people knowledgeable about campaigns and elections who were deeply disillusioned with corrupt fundraising activities and the political "closed shop." The initial bipartisan Honorary Chairs of the Advisory Committee were **Senator John McCain** (R-AZ) and former **Senator Bob Kerrey** (D-NE). In recent years, the Institute has expanded its work to critical issues that reveal the need for significant reform of the political process and demand bipartisan leadership.

The Institute is a unique, independent voice in the constellation of nonprofit organizations. The Institute brings together a broad base of reformers from all ideological spectrums, including business leaders, policy experts, and retired and current elected officials and, most importantly, average Americans who are tired of politics as usual.

The Institute's distinctive network is reflected in the members of our Advisory Committee—a bipartisan group of notable academics, legal experts, election administrators, and public officials. This includes the **Honorable Ralph Munro** (Former Secretary of State, Washington State), **Tami Buhr** (Harvard University), **Marion Just** (Wellesley College), **Norm Ornstein** (American Enterprise Institute), **Tom Mann** (Brookings Institution), **Anthony Corrado** (Colby College), **U.S. Senator Lindsey Graham** (R-SC), **David Pottruck** (former CEO, Charles Schwab), and **former U.S. Senators David Boren** (D-OK) and **Bob Kerrey** (D-NE). These and other members have joined forces to carry forward the reform agenda from a centrist vantage point.

The Reform Institute's Board of Directors is comprised of former Congressman **Charles Bass** (R-NH), **Charles Kolb** (Committee for Economic Development), and **Pam Pryor** (Convoy of Hope). In addition, **Daniel Ortiz** of the University of Virginia's School of Law serves as Legal Advisor and **Cecilia Martinez** is the Executive Director.

**The Reform Institute**  
**300 North Washington Street, Suite 600**  
**Alexandria, VA 22314**

Tel (703) 535-6897 ★ Fax (866) 863-5510

[www.reforminstitute.org](http://www.reforminstitute.org)