

# THE 9/10/11 PROJECT

PREPAREDNESS

## Are We Ready for the Day Before Tomorrow?

**Imagine it is September 10, 2011** – 9/10/11 – a full decade since the devastating terrorist attacks of September 11, 2001. Is our nation equipped for whatever catastrophe may happen tomorrow? How have our prevention, preparedness, response and resiliency structures changed, matured and become operational?

The Homeland Security & Defense Business Council's 9/10/11 Project looks at how far the country has come since the day before 9/11/2001. Through fresh interviews with industry leaders the Council is seeking to vividly illustrate the strides our government at all levels, working with the private sector, has made to secure the country and to stay at least one step ahead of events and disasters that could destroy our way of life.

On the 10th of each month through September 2011, the Council will provide a historical context for how far we have come and where we are now, as well as an assessment of the future of the most pressing homeland security issues. Each monograph will include a running timeline (interactive on our website) illustrating the events, incidents, and critical government responses pertinent to that month's topic. This month's monograph focuses on **Preparedness**.

## Preparedness Through The Generations

*Preparedness, when considered in the context of national security, was pretty simple at one time: We protect our borders and we maintain a military as a deterrent or a force against foreign aggression. Today, preparedness extends to all manner of natural and man-made disasters, wherever they may occur, and virtually everything is now a matter of national as well as local concern. This is a relatively new way of thinking in American tradition and experience. It also underscores a widely held view among professionals in the homeland security community that some needed changes in our culture of preparedness may take another generation to mature.*

To see how much time such changes can take, it's useful to look back to one of the great natural calamities in the first half of the Twentieth Century — the Mississippi River flood of 1927.

Unlike the sudden and relatively short-lived Hurricane Katrina several decades later, the 1927 flood was widely foreseen and long in duration. Its cause was ordinary rainfall, but in extraordinary amounts. Seemingly never-ending downpours soaked the entire Midwest throughout the summer and into the fall of 1926. The water-logged landmass extended from Illinois to the north, Oklahoma to the west, and West Virginia to the east. Gradually it wrung itself out into the streams and tributaries feeding the Mississippi and then to the Big Muddy itself. A few weeks into spring, and the swollen Mississippi had broken through its levee system in 145 places along several states.

By June of 1927, altogether 27,000 square miles of the Mississippi River watershed were inundated, "roughly equal to Massachusetts, Connecticut, New Hampshire and Vermont combined." About 330,000 people had been rescued from rooftops, trees, isolated patches of high ground, and levees. The American Red Cross ran 154 tent cities in seven states — Kentucky, Tennessee, Missouri, Illinois, Mississippi, Arkansas, and Louisiana. Deaths ran into the thousands.

1803

The Congressional Act of 1803 designated funds for a New Hampshire town that had suffered a damaging fire. In the U.S.'s first century, the government handled disaster relief on an ad-hoc basis

1885

The American Red Cross, previously primarily a battlefield relief organization, responded to a large flood in Johnstown, Pennsylvania. The Red Cross distributed medical supplies and constructed shelters, providing relief to an estimated 25,000 individuals

APRIL 1927

Massive flooding in the Mississippi River basin prompted the federal government to assume responsibility for flood control in the region, culminating in the Flood Control Acts of 1928 and 1936

JANUARY 22, 1932

The Reconstruction Finance Corporation (RFC), authorized in legislation passed the previous year, began operation. Along with other duties, the RFC authorized loans for repair and relief following natural disasters

# Public Sector Leaders

- ✓ 20 of the 20 Top Global Governments
- ✓ 20 of the 20 Top U.S. Counties
- ✓ 20 of the 20 Top U.S. Cities
- ✓ All 15 U.S. Federal Cabinet Agencies
- ✓ All 50 U.S. States

**Get Better Results With Oracle**

**ORACLE®**

**[oracle.com/goto/government](http://oracle.com/goto/government)  
or call 1.800.633.0584**

The response of the federal government? As the catastrophe unfolded, President Calvin Coolidge mostly turned a deaf ear to repeated pleas for help, which came from dozens of governors, mayors, and editorial pages. Finally, on April 22, after the worst of the levee breaks, Coolidge relented. He named his commerce secretary, Herbert Hoover, to head up a cabinet-level team to reckon with recovery efforts.

Hoover took up his task with energy and dedication (incidentally paving the way for his own rise to the White House), but he was an exception. Most people thought what Coolidge thought, "that the [federal] government should do nothing. Direct aid had always been considered charity, and charity stigmatized recipients." So writes John M. Barry in *Rising Tide*, his extensive history of the flood. Barry notes that even *The New York Times* applauded Coolidge for his refusal to heed demands that he convene a special session of Congress to address the disaster. *The Times* deemed Hoover's program to be sufficient.

Such was the culture of preparedness at the time.

It was also a time, however, when thinking began to change. A year after the flood, Coolidge signed into law a bill declaring in effect that "the federal government took full responsibility for the Mississippi River. In doing so, the law set a precedent of direct, comprehensive, and vastly expanded federal involvement in local affairs."

Even so, federal disaster relief was, by definition, focused largely on ameliorating the effects of a disaster, and less so on preparedness. And it was still essentially an ad hoc affair. Which is to say that if a disaster was big enough to draw the attention of Congress, it was treated as a singular event, needing careful deliberation by Congress as to the amount of funds to be allocated, the type of federal equipment to be sent, the number and type of personnel to go to a stricken area, and so on. Quick action was not practical or possible.

What was still needed was some sort of blanket authorization that committed the federal government to deliver aid, promptly, for state or local disasters without the requirement for congressional deliberation and action. Blanket authorization did come, but not until a full generation after the great flood of 1927. In 1950, Congress passed and President Harry S. Truman signed the Disaster Relief Act. The act gave the President sole authority to order federal aid delivered to the scene of a natural catastrophe if the President determined that state and local capabilities had been overwhelmed.

Most of the experts on domestic security and emergency management with whom we consulted for this piece agree that it's important to be cognizant of the extended time it takes for attitudinal changes to work their way through a large society. These are changes that must take place before the society can really bring its preparedness systems to a new level. Marko Bourne, for example, is a principal in the Homeland Security Emergency Management and Response practice at Booz Allen Hamilton. "The generational gap is definitely a major consideration in how we plan for preparedness," he says. For instance, he cites the creation in 2004 of the National Incident Management System (NIMS). "Up until 2004," he says, "there was no single incident-command system that first responders across the country could use. There were hundreds of such systems, and each one used a slightly different command process — i.e., how do we organize ourselves to operate at an emergency scene? The processes were wildly different, depending on what part of the country you were in. So the question was: How do we build some commonality? Booz Allen Hamilton, in helping write the National Response Plan and the National Response Framework, distilled all the lessons learned from disasters in the '90s, and certainly from 9/11, about the need for a common understanding of principles and doctrine around the idea of incident command." (NIMS was subsequently refined and brought into a more elaborate organizing effort called the National Response Framework, but more on that later.)

Bourne adds — and this is his point — that there was a growing expectation throughout the '80s and '90s and into the '00s that the federal government would do most of the heavy lifting during a major disaster, and that states, local governments, and the public might not have to do as much because the federal government would pick up the slack."

Such was the distance that the culture of preparedness had travelled since 1927.

## From Nuclear Defense to Counter-terrorism to All-hazards

The range of potential emergencies receiving attention in preparedness planning has gone through a number of phases. When the Federal Emergency Management Agency (FEMA) was set up, in 1979, its focus was largely on preparedness for an attack against the U.S. homeland by a hostile foreign power. Fourteen years and a number of reorganizations later, FEMA and its mission were included among the subjects of a document

**1941**  
The Office of Civilian Defense was established to ensure the continuity of government, protection of critical resources, and organization and defense of the civilian population in the event of enemy attack during World War II.

**JANUARY 1951**  
President Truman created the Federal Civil Defense Administration to educate the civilian population and coordinate and plan for the possibility of nuclear attack.

**SEPTEMBER 1961**  
Life magazine published a letter from President Kennedy advising Americans to prepare fallout shelters. The letter was part of a larger government campaign to increase American preparedness for nuclear attack and sparked a nation-wide fascination with fallout shelters.

**1968**  
The National Flood Insurance Plan was authorized by the signing of the National Flood Insurance Act. The NFIP provides insurance to communities living in flood plains in exchange for adopting government regulations designed to minimize flood damage; in 1973, Congress reinforced the NFIP to make flood insurance mandatory for buildings acquired or built in flood plains.

**1960s**  
A series of natural disasters, including the Anchorage Earthquake in 1964 and Hurricane Camille in 1969, demonstrated the weakness of American natural disaster preparedness and response.

prepared under the direction of Vice President Al Gore with the aim of improving the efficiency of the federal government. With regard to FEMA, it called for a shift in the agency's focus from preparedness for nuclear war to preparedness for disasters of all kinds — what became known as the all-hazards approach. Not coincidentally, this was only months after the February 1993 bombing at the World Trade Center and less than two years after the dissolution of the Soviet Union.

FEMA underwent further reorganization and realignment at the start of the Bush Administration. Then came the attacks of September 11, 2001, which sparked a vast re-examination of domestic security systems. And the federal government's focus turned almost exclusively to counter-terrorism. FEMA and dozens of other security and law enforcement agencies were combined to create, in November 2002, the new Department of Homeland Security (DHS).

But after Hurricane Katrina made landfall on the Gulf Coast, on August 29, 2005, the focus shifted again. Authorities were back to an all-hazards approach. An all-hazards approach had actually been ordered put into effect by President George W. Bush prior to Hurricane Katrina, but its implementation did not really gain momentum until after the catastrophe. It "makes perfect sense," according to Chet Lunner, a former DHS official who now runs a Washington-based security consultancy. "It has to be all hazards. It probably always had to be, because the people who do the emergency responding are always the same people, no matter what the cause is — whether it's man made or natural. You can't have one set of responders for one causative factor and another set for another causative factor."

Bob Connors agrees. As the director of preparedness at Raytheon Company, he says, "At Raytheon, we have to have an all-hazards focus. We have people in all 50 states and on all seven continents, so we need to be prepared for severe weather, geologic events, wildfires, political or civil unrest, terrorist attacks, and myriad other threats. No matter what happens or where, we have to be prepared to respond to, and possibly recover from, an incident. I believe most agencies and businesses have now taken an all hazards approach to preparedness, and that's the right and necessary approach."

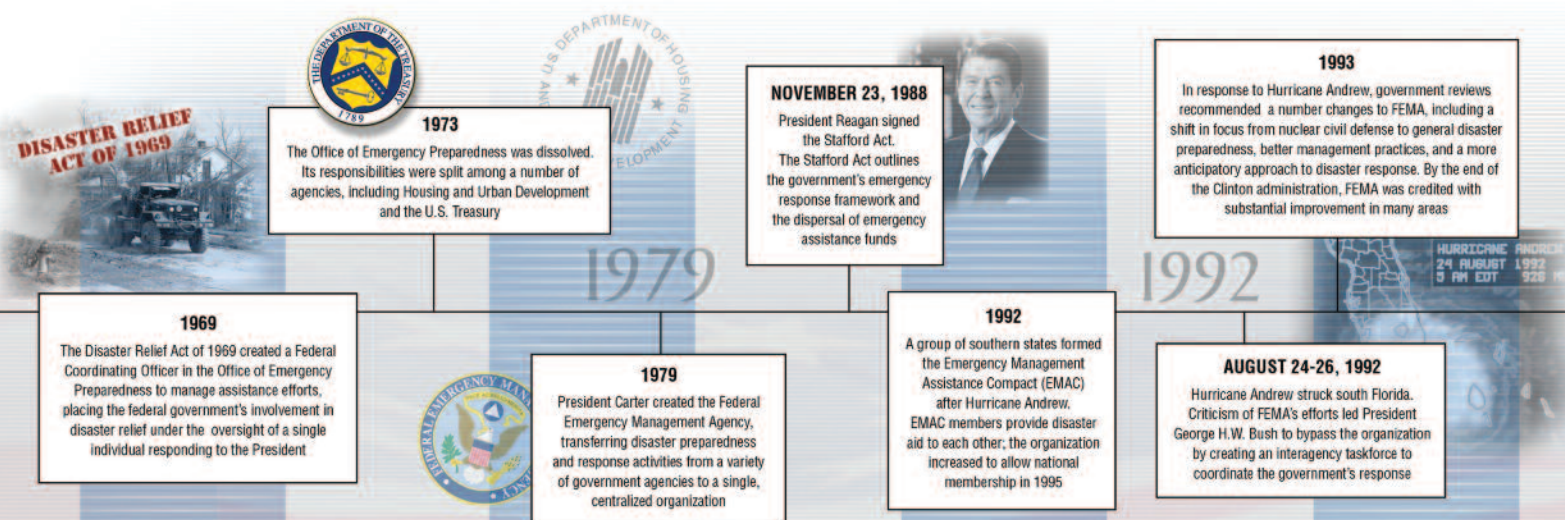
Chet Lunner adds that "the way you make your staff more efficient is by broadening their responsibilities, broadening their exposure to the whole roster of homeland security professionals." That, in fact, is a recurring theme among preparedness experts: that emergency responders cannot be introducing each other and exchanging business cards at the scene of a disaster. Those relationships, and the different roles and responsibilities, must be established and clarified beforehand.

### Bridging The Public/Private Divide

Government can do almost endless amounts of planning and strategizing about preparedness, but government still lacks the technological and production facilities internally to bring most of those plans and strategies to fruition. Those facilities are developed, produced, and implemented by the private sector. Getting the two sectors to mesh, and to mesh efficiently, is often slow and difficult, but actual emergencies typically provide opportunities for both sectors to learn and improve.

The events of 9/11, for example, exposed major weaknesses in key aspects of preparedness. Perhaps the most glaring was the failure to "connect the dots" — which typically referred to lapses in exchanging human intelligence. But it also included the lack of interoperability in communications systems used by police, fire, EMS, and other first responders; and between those local entities and federal and state authorities, and among the whole panoply of federal agencies. That shortcoming played havoc in many instances with needed coordination and cooperation. To address the "dots" problem, the DHS and the Department of Justice sponsored the establishment of fusion centers around the country. One or more of such centers were set up in each of the states and operated largely by state and local authorities, with additional help from the private sector. There are more than 70 fusion centers today, and they're intended to promote information sharing among all levels of government as well as with the private sector.

Peter Doolan, a business-continuity expert who heads the public sector unit of the software company Oracle, says preparedness consists of organizational as well as technological components. "It's as much to do about getting the right information at the right time to the right person as it is to have wind-up radios and the other things you think you need for the first



72 hours after a disaster. The business of the fusion center is to fuse data and catch bad people before terrible things happen. To do that, you need a reliable and resilient data and business infrastructure. Fusion centers,"he continues,"are assuming a role that requires a level of business continuity and performance and resilience not unlike what you would expect from the largest banks and airlines and car-rental agencies around the world."

Virtually every law-enforcement and emergency-response organization in the country has since 9/11 made it a top priority to address the interoperability issue. In so doing they have forged partnerships with a host of private-sector companies, including of course Oracle, but also such well-known names as BAE Systems, General Dynamics, Raytheon, and Unisys.

A sampling of some of the projects in which those companies are involved — not to mention hundreds of others — may give an idea of the range of preparedness-related services and technologies the private sector provides:

The Public Sector unit of Oracle is addressing the interoperability problem in a big way, leveraging its traditional strength in database software and its more recently acquired strength in processing hardware. The latter came from its acquisition, completed early last year, of Sun Microsystems:

- Oracle in late 2010 began implementing at U.S. Customs and Border Protection a new system for monitoring overseas cargo and passengers headed for U.S. destinations. It is a hardware and database software design that aims for "extreme performance." (Exadata) combines massively parallel supercomputing with ultra-sophisticated relational-database-management technology, all assembled in a box about the size of a refrigerator.

Doolan explains further that the Exadata box "receives all the different signals coming in from all the different databases at all the different authorities around the globe and puts them through a unifying intelligence that can extract a near-real-time picture of any suspicious patterns."

The Exadata box, Doolan adds, is packaged in a turn-key configuration — "so it can be rolled off a truck and plugged in and be ready to go without the need for special IT expertise on the part of the user." A number of Exadata systems are headed for the fusion centers.

- Oracle is helping DHS drive adoption of a new data-sharing standard, called the National Information Exchange Model (NIEM), that will provide

enhanced capabilities for organizations to share data across federal, state, local, and tribal lines.

Unisys has a major concentration on state and local infrastructures.

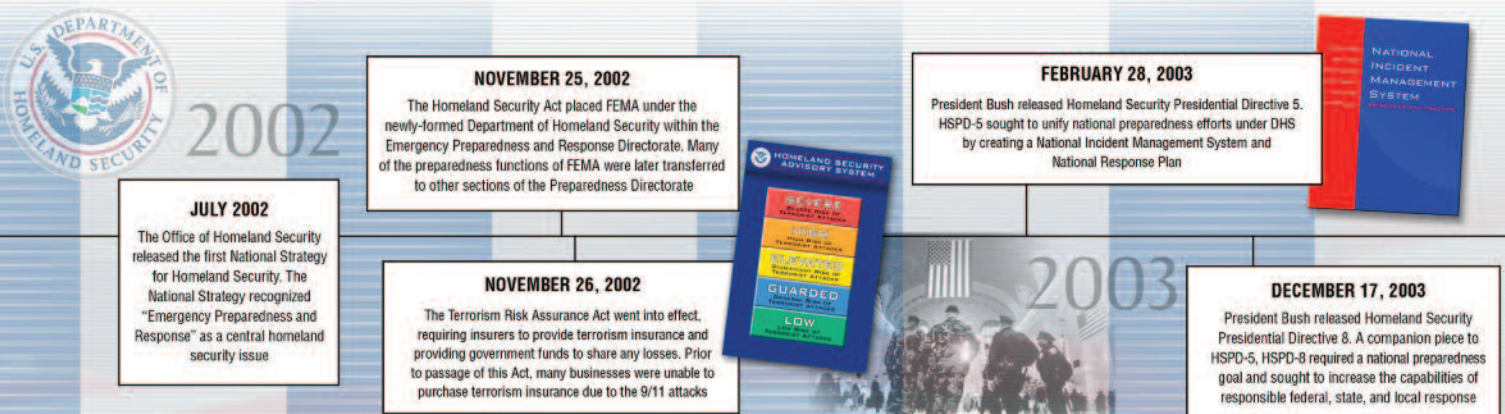
- Unisys has engagements with several local and state police departments across the country to help upgrade and automate their 911 emergency dispatch systems. Ensuring commonality among these systems is an essential goal. "Integral to 911 emergency dispatch systems and agency preparedness is the interoperability of tactical communications," explains Martin Mackes, vice president and partner at Unisys. Unisys is helping the Federal Protective Services (FPS) redesign their tactical communications infrastructure nationwide. FPS is the organization that provides integrated security and law enforcement services to federally owned or leased assets and properties.

At the C4 Systems unit (C4S) of General Dynamics, engineers and designers specialize in command and control, communications networking, and hardened systems for ensuring computing and information availability. Additionally, there's a strong emphasis on interoperability solutions for a variety of federal agencies.

- C4S is the prime contractor for the Integrated Wireless Network (IWN) program being overseen by the Department of Justice and joined in by DHS and Treasury. James Norton, director of the Homeland Security & Federal Strategy business at C4 Systems, describes what IWN is replacing this way: "If you were to get into an FBI agent's vehicle right now, you'd probably see one radio for the FBI, a different radio for the DEA, a third for the ICE agents, and so on and so forth, all sitting on the car's console. IWN will allow them to have one radio for all these entities. That one radio interoperates with all the different radio-frequency bands and protocols."

- In the cybersecurity realm, General Dynamics has developed one of the first operational examples of what's known as a multi-level security protocol for the communication of sensitive information. Called the Trusted Network Environment (TNE), it works by enabling computers to process information with different security levels, permitting users who have different security clearances and different needs-to-know to access the same databases simultaneously

BAE Systems, particularly its Intelligence & Security group, is engaged with FEMA and other DHS agencies to help improve their preparedness posture.



- Because FEMA needs to be prepared to help people reassemble their lives after a disaster, the agency has developed the Disaster Assistance Improvement Program (DAIP), which greatly simplifies the process by which an individual disaster victim might interact with the federal government. Prior to DAIP, a disaster victim might have to interact separately with up to 16 different federal agencies offering more than 50 different forms of disaster assistance. With DAIP, the individual needs to call only one number to gain access to all the relevant aid programs. BAE Systems has supplied much of know-how to make that happen.

- BAE has provided the tools that FEMA is using to ensure the prompt availability of needed supplies in a disaster situation. (Total Asset Visibility) gives FEMA the ability to better manage inventories of things like blankets, cots, food, and water, and to get such assets delivered more quickly to where they are needed.

With regard to that last item, FEMA's drive to improve its logistical preparedness may have been inspired by the efficiencies that the private sector demonstrated in the aftermath of Hurricane Katrina. Walmart, for example, has an emergency operations center that is continually staffed by decision-makers who have access to all of the company's systems. Because of that, it was one of the first organizations to move food, water, generators, and other goods into New Orleans.

"Walmart has a much better distribution system than any entity in the United States government," says Don Loren, special assistant for national security at The Tauri Group, a consultancy based in Alexandria, VA. Loren is also a retired Navy rear admiral, a former senior executive with the National Counterterrorism Center, and the former Deputy Assistant Secretary of Defense for Homeland Security Integration. "So what we are learning in the homeland security business," he says, "is that it is critically important to include the private sector in that type of planning and preparation. Everything is inexorably linked, whether it be at the governmental level — federal, state, local, tribal — or the private sector."

## Strategies, Oversight, and Funding from the Public Sector

Where the public sector has significant capability, of course, is in very large-scale strategic planning, oversight, and funding. As an example DHS streamlined 15 different categories of emergency described in the National Planning Scenarios document of 2004 and narrowed them down to

the more digestible and manageable eight emergency situations specified in the National Response Framework of 2008.

What was especially emphasized in the Framework document was the evolutionary nature of preparedness planning. "Since planning is an ongoing process," it said, "a plan is an interim product based on information and understanding at the moment, and is subject to revision. That is why plans are best described as 'living' documents."

The eight emergency preparedness planning scenarios that currently pertain are:

1. Explosive attack, i.e., bombing using improvised explosive device.
2. Nuclear attack.
3. Radiological attack – using radiological dispersal device.
4. Biological attack, a category subdivided by pathogen type (aerosol anthrax, plague, food contamination, foreign animal disease).
5. Chemical attack, a category subdivided by chemical type (blister agent, toxic industrial chemicals, nerve agent, chlorine tank explosion).
6. Natural disaster, a category subdivided into major earthquake or major hurricane.
7. Cyber attack.
8. Pandemic influenza.

The Tauri Group's Don Loren applauds the development of these planning scenarios, but he also acknowledges (quoting the renowned Prussian general Helmuth von Moltke) that "no plan of battle survives the first contact with the enemy." A plan, however, says Loren, "at least gives you understanding of what's available, how everybody can interact, and how things tie together."

Of the eight scenarios, the one that is currently getting the lion's share of attention is cyberattacks. Scott Weber, an attorney at the firm of Patton and Boggs who specializes in homeland security issues, agrees that "cybersecurity is hugely important. If your enterprise uses any computers, any IT, the likelihood of your being a victim of a cyberattack is probably greater than any of the other categories of hazard." (See the council's October 10, 2010 monograph)

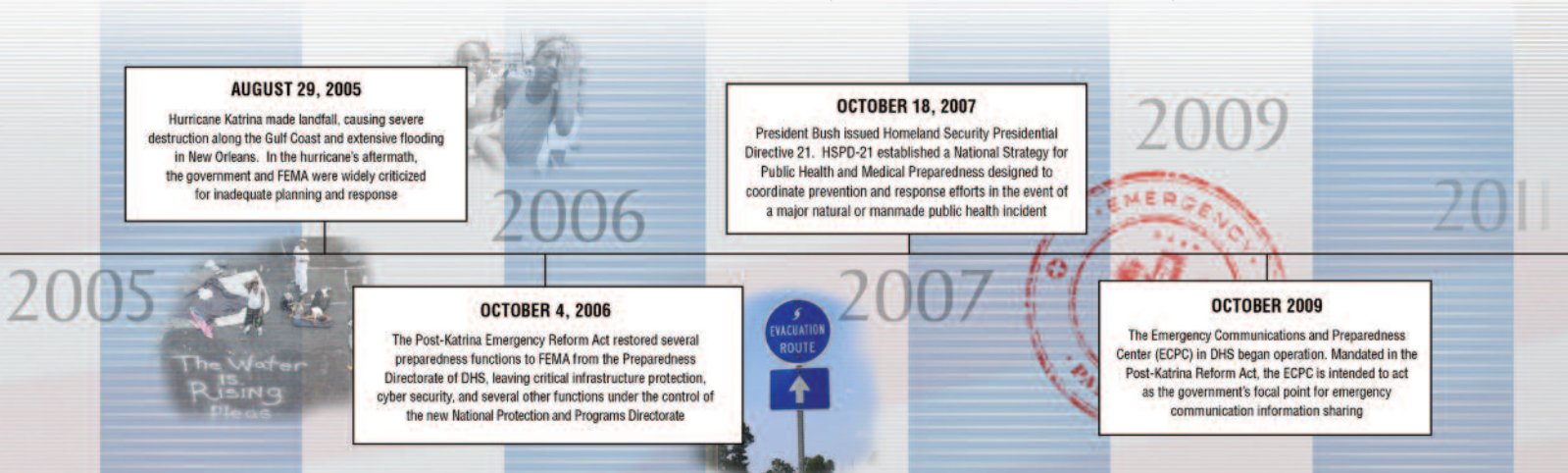
Some experts, however, would still rank natural disasters a little higher as a priority concern. Bob Connors, for example, the director of preparedness at Raytheon, says, "From our perspective, natural disasters are the most likely incident that will impact our employees, operations, or suppliers. The

**AUGUST 29, 2005**  
Hurricane Katrina made landfall, causing severe destruction along the Gulf Coast and extensive flooding in New Orleans. In the hurricane's aftermath, the government and FEMA were widely criticized for inadequate planning and response

**OCTOBER 18, 2007**  
President Bush issued Homeland Security Presidential Directive 21. HSPD-21 established a National Strategy for Public Health and Medical Preparedness designed to coordinate prevention and response efforts in the event of a major natural or manmade public health incident

**OCTOBER 4, 2006**  
The Post-Katrina Emergency Reform Act restored several preparedness functions to FEMA from the Preparedness Directorate of DHS, leaving critical infrastructure protection, cyber security, and several other functions under the control of the new National Protection and Programs Directorate

**OCTOBER 2009**  
The Emergency Communications and Preparedness Center (ECPC) in DHS began operation. Mandated in the Post-Katrina Reform Act, the ECPC is intended to act as the government's focal point for emergency communication information sharing





Centre for Research on the Epidemiology of Disasters found that in the last decade there have been over 3,800 disasters that have affected nearly 2 billion people and cost \$960 billion. While you can't really predict or prevent a natural disaster, you can certainly do a lot to prepare for it and reduce your risk."

## "PS-Prep" – Preparedness Standards for Private Sector Companies

To better involve private-sector companies in the preparedness mission, DHS has developed and is promulgating an accreditation and certification program designed to "promote private sector preparedness, including disaster management, emergency management, and business continuity programs." Known as PS-Prep, for Private Sector Preparedness — the program is voluntary. The preparedness standards that the program has endorsed have been drawn up by private-sector organizations, namely the American Society for International Security (ASIS), the British Standard Institution (BSI), and the National Fire Protection Association (NFPA).

Scott Weber, who was senior counselor to former DHS Secretary Michael Chertoff, describes the program as "best practices and standards that can be used for benchmarking and guidance to help the private sector establish a preparedness program that is comprehensive enough to address all hazards. It's meant to ensure that a business can continue with its mission-critical functions."

Weber says the standards that the DHS has endorsed in this program represent a tremendous amount of trial-and-error learning in the private sector over the last several decades, especially about things like maintaining business continuity after a disaster. They embody a lot of best practices, he adds, and the program as a whole is an implicit acknowledgement by the public sector that "good national preparedness can't be decreed from on high, and that they need the private sector's engagement in these matters."

## Taking Aim at Complacency

If not imposed from on high, neither can an optimal level of preparedness be expected to percolate up spontaneously and naturally from private individuals across the country. "The most prepared we've ever been," estimates Martin Mackes, vice president and partner at Unisys, "was probably the year or two immediately after the 9/11 events. Since then," he says, "we have not suffered a major attack, so it's not surprising that people just stopped paying as much attention."

Interestingly, that may not be for want of information. It may come from too much information. With the advent of cable news and the Internet and the resulting 24-hour news cycle, what used to be local types of emergencies and disasters are now effectively nationalized. The most parochial

event can now become the lead story on cable news or go viral on the web regardless of the fact that it may have no national import to it at all. Many in the homeland security environment suspect that people have become so inured to reports of run-of-the-mill incidents that they tune out things that may pose much more serious threats.

"Complacency and denial are overwhelming forces for emergency managers to deal with," says Bob Connors at Raytheon. "We have to consider these forces when communicating to the public or our employees. Disaster managers live and breathe preparedness, but we're often talking to an audience that doesn't want to think about bad things happening. We have to employ innovative ways to reach these folks and encourage them to 'be prepared, not scared.'"

In any event, the homeland security community is genuinely concerned about public complacency. Could it be because of the perception that the folks in Washington are taking care of everything so we don't have to? Perhaps so.

## Conclusion

We are an accomplished nation evolving to become more resilient in our preparedness for emergencies and disasters. We have demonstrated an ability to learn and adapt, drawing lessons and deriving better and best practices from the catastrophic events that have impacted our communities. From an under-reliance during the Mississippi floods to an over reliance on the public sector during hurricane Katrina, we understand better that collectively—each individual, company and community—has a responsibility and obligation to prepare for all hazard events. And, we understand the necessity to partner and team with BOTH the private and public sector as an engaged player. While much of this newfound understanding has evolved through our experience drawn from the significant events of the past decade, we must not be deterred in meeting our responsibilities despite reduced budgets and other limitations on resources. In fact, despite these issues, we need to participate and encourage the trend toward greater public-private partnership and think more strategically about how we can leverage resources and relationships to a greater degree. Only when we recognize and fully integrate all of our resources – private and public – will we – and the nation – achieve a greater level of preparedness.

*The Homeland Security & Defense Business Council (HSDBC) works to ensure that the perspective, innovation, expertise and capabilities of the private sector are recognized, respected and integrated with the public sector. The 9/10/11 Project has called upon critical thought leaders and subject matter experts, including the chief writer for this monograph, William Dunne. For more information on the Council's 9/10/11 Project visit: [www.homelandcouncil.org/91011-Project.html](http://www.homelandcouncil.org/91011-Project.html)*

**For a more complete timeline, visit the Council's website**

For more information on the Homeland Security & Defense Business Council visit: [www.homelandcouncil.org](http://www.homelandcouncil.org)

**Homeland Security & Defense Business Council** • 1140 Connecticut Avenue Suite 1008 • Washington, D.C. 20036 • (202) 470-6440

Marc A. Pearl, *President/CEO* • Kristina Tanasichuk, *Vice President & Project Director*

# Fastest Ever Database Performance



**Sun**  
SPARC

**30 Million**



**IBM**  
P7

**10 M**



**HP**  
Superdome

**4M**

tpmC Transactions/Minute

**ORACLE®**

Source: Transaction Processing Performance Council, [www.tpc.org](http://www.tpc.org) as of 12/2/10. Oracle SPARC SuperCluster with T3-4 Servers, 30,249,688 tpmC, \$1.01/tpmC, available 6/1/11. IBM Power 780 Server, 10,366,254 tpmC, \$1.38/tpmC, available 10/13/10. HP Integrity Superdome-Itanium2, 4,092,799 tpmC, \$2.93/tpmC, available 8/6/07. More at [oracle.com/sunoraclefaster](http://oracle.com/sunoraclefaster).