

# GETTING BACK ONLINE by Going Off the Beaten Path

A Practical Guide to Protecting Your Information Assets and  
Ten Things You Wished You Knew Before the Disaster Struck



*“A towel has immense psychological value...any man who can hitch the length and breadth of the galaxy, rough it, slum it, struggle against terrible odds, win through, and still knows where his towel is is clearly a man to be reckoned with.”*

— Douglas Adams, *The Hitchhiker's Guide to the Galaxy*

# Introduction: What Are You Going to Do?

In the early morning hours of August 30th, 2005, the 17th Street canal broke through a concrete flood wall, ultimately leaving 80 percent of New Orleans underwater. Only six weeks later, Pan American Life became the first major office building to re-open on October 10th at 601 Poydras Street. This return to near-normal business operations was a signal that rebuilding had begun, and was a testament to the merits of a thoroughly planned and expertly executed business continuity and disaster recovery plan.

Stories emanating from recent natural disasters have, unfortunately, focused more on what not to do or what should have been done to ensure business continuity and disaster recovery — also known as *continuity of operations* in the public sector. Still, government has much to learn to prepare for the next inevitable disaster. Although hindsight is 20/20, having a vision, drafting and finalizing a plan and being able to execute when it is needed — is preferable to being unprepared and left with the question, “Well, now what are we going to do?”

Service interruptions are inevitable in a complex world characterized by natural and manmade disasters. Proper preparation can be governments' insurance policy, and is important for entities that, for the most part, are self-insured. A new focus on continuity of operations planning (COOP) has emerged — complete with enterprise-level security assessments, continuity planning (through standardization, documentation, and evaluation), and well-constructed, implemented and tested disaster recovery.

This white paper provides an overview of the COOP disciplines as the basis of a sound policy framework. It will then deliberately diverge off the beaten path and suggest different approaches to consider, including a continuity of operations plan that some planners may not have considered as part of their current planning efforts. Since there are multiple sources of information you can use to supplement your planning, there is no need to “go it alone.”

## Not “Going it Alone”: the Discipline of Continuity and Disaster Recovery Planning

The endgame of information technology (IT) continuity and disaster recovery planning is to maintain high availability and security. Even more importantly, as planning relates to an organization's information assets and, by extension, the ability to do its work, especially during times of emergency. Government agencies should understand that they do not have to muddle through this process alone. It is useful to begin by first defining these disciplines.

Like the terms “love and marriage” and “privacy and security,” “continuity of operations and disaster recovery planning” are nearly always joined together in a single phrase. Still, they have characteristics that differentiate them from each other.

- *Continuity of operations planning* (COOP) is characterized as a proactive activity. COOP tries to reduce the impact of a possible risk. Plans

are designed to help keep the organization operating until disaster recovery efforts have been achieved.

- Conversely, *disaster recovery planning* is reactive because it focuses on restoring the organization at least to the state it existed in prior to the event of disaster.

There are many organizations that have contributed to these disciplines and have extensive educational resources at their disposal. A variety of documents, plans, tools and approaches to design high quality continuity of operations and disaster recovery frameworks to emulate have been developed.

## Leaders in COOP and Disaster Recovery

One internationally recognized framework used to maintain and enhance protection and control over data, information, information technology and its associated risks is COBIT (Control Objectives for Information and related Technology). COBIT is issued and maintained by the IT Governance Institute under the auspices of the Information Systems Audit and Control Association (ISACA). The purpose of COBIT is to provide an analysis framework that links control objectives to the domains of IT governance so that potential omissions can be identified. COBIT also maps to other standards (ITIL<sup>1</sup>, CMMI<sup>2</sup>, COSO<sup>3</sup>, PMBOK<sup>4</sup>, ISF<sup>5</sup> and ISO 17799<sup>6</sup>).

Additionally, COBIT establishes performance indicators and aligns organizational goals with IT goals.<sup>7</sup> ISACA offers professional certification through a Certified Information Systems Auditor (CISA) program. According to the ISACA, more than “44,000 professionals have earned the CISA since its inception.” This program has also been accredited by the American National Standards Institute (ANSI) under ISO/IEC 17024:2003, General Requirements for Bodies Operating Certification Systems of Persons. ANSI, a private, nonprofit organization, accredits other organizations to serve as third-party product, system and personnel certifiers.<sup>8</sup>

Two other influential organizations making major contributions to COOP and disaster recovery planning are the National Emergency Management Association (NEMA) and the Association of Contingency Planners (ACP). NEMA is a nonprofit association dedicated to “enhancing public safety by improving the nation’s ability to prepare for, respond to and recover from all emergencies, disasters, and threats to our nation’s

security.”<sup>9</sup> One of NEMA’s key contributions has been their advocacy for the creation of the Incident Command System (ICS). The Sept. 11 Commission supported NEMA’s longstanding position when it “highlighted the lack of coordination of command and control in their report by calling for all emergency response agencies to adopt the Incident Command System (ICS) and structures for unified command. . . ICS is an all-hazards system that can be used for all incidents, regardless of the cause or size.” The report also recommended that Congress fund homeland security only if recipients adopt and use ICS and unified command. This stance has led, at least in part, to the Department of Homeland Security’s initiative to craft the National Incident Management System (NIMS) with state and local governments. NIMS is being created to address the lack of coordination in command and control structures.

Despite these positive developments, NEMA warned that these planning efforts may not yield desired results, in part because they believe that insufficient federal funds have been allocated to emergency management programs. NEMA cites the current fiscal 2007 budget request as evidence for their claim. The budget request reduces the current funding level on the Emergency Management Performance Grant Program (EMPG) from \$183.1 million to \$170 million. The EMPG supports preparedness programs for state and local governments.<sup>10</sup>

One other important organization contributing to COOP is the Association of Contingency Planners (ACP). According to the organization, “ACP is a nonprofit trade association dedicated to fostering continued professional growth and development in effective Contingency & Business Resumption Planning.”<sup>11</sup> ACP has 36 chapters in 23 states.

# Federal Laws Add a Layer of Complexity — COOP Best Practices Can Help

Adding to the web of COOP complexity are the policy layers that exist as a result of federal laws or regulations; the Health Insurance Portability and Accountability Act (HIPAA) is a prime example. An already

complex and ambitious environment is further confounded by the potential residual affect of Sarbanes-Oxley on state and local government practices (see the sidebar describing these two key federal laws).

## HOW DO YOU SPELL COMPLIANCE? HIPAA AND SOX

### About HIPAA and Sarbanes-Oxley

#### HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) is a law that was enacted by Congress in 1996. Relevant to e-mail management are the Title II provisions that establish national standards for security, privacy and electronic data interchange of health data. Multiple organizations within state and local government are covered under the umbrella of HIPAA, and therefore must comply with the law and with the U.S. Department of Health and Human Services regulations that interpret the law.<sup>12</sup>

#### Sarbanes-Oxley (SOX)

In the wake of Enron and other corporate scandals, the Sarbanes-Oxley Act (SOX) was established by the U.S. Congress in 2002 with far-reaching effects, ranging from the freezing and dissolution of future company pensions to the restructuring of corporate America's oversight boards. While SOX only applies to publicly held companies, it serves as a fair example of the need for good governance.

The American Society of Association Executives summarizes 13 key provisions of SOX.<sup>13</sup> The SOX provisions most likely to have an impact on government are the audit, document destruction or alteration, and internal control provisions. The federal government is already establishing new internal controls via SOX-like provisions. The internal controls framework is published by the Committee of Sponsoring Organizations (COSO)<sup>14</sup>, an umbrella group of accounting and financial management organizations. The framework forms the

backbone of Sarbanes-Oxley's section 404. The Government Accountability Office (GAO), the investigative arm of Congress, has adopted the COSO framework for the federal government. It should be noted that although state and local governments do not currently fall under the umbrella mandate of SOX, voluntary compliance to some SOX provisions or even "copycat" legislation at the state level may be in the offing.<sup>15</sup>

#### SEC Storage of Electronic Records Rule 17-CFR 270.17a-4

Since 1934, the U.S. Securities and Exchange Commission (SEC) has had a comprehensive set of rules that govern the preservation of records. These rules have been updated to require brokers, dealers and exchange members to follow electronic storage management procedures including e-mail management. Although these requirements, not unlike SOX, only apply to the securities industry, many of these practices provide excellent guidance for better management of electronic government records. Courts are increasingly relying upon e-mail to support the discovery process when suits involving a government are filed. Discovery is frequently a labor intensive process that can be aided significantly by modern searchable e-mail archiving and storage tools.

The issue is that e-mail and other electronic communications technology (including instant messaging, text-messaging, e-mail enabled phones and wireless-enabled handheld devices) are increasingly being used to execute and document major business transactions and policy decisions, yet are not retained in a disciplined way for future inspection or disclosure — violating the spirit of SOX and the letter of state public disclosure laws.

# Five IT Solutions State & Local Government Might Consider in COOP Planning

IT's primary role in the overall COOP effort is in the arena of cybersecurity. Solutions that IT operations centers might consider while developing COOP planning and implementation capabilities include:

## **DEPLOY ANTI-VIRUS/ANTI-SPYWARE/MALWARE/ ANTI-SPAM DETECTION AND REMOVAL SOFTWARE**

These solutions will prevent or reduce the impacts of "cyber-plagues," including:

- lost employee productivity,
- poor performing desktops and servers,
- overuse of already taxed storage capacity,
- misuse of computer resources by rogue programs that launch denial of service attacks or spam, and
- the inadvertent or purposeful alteration or destruction of mission critical data.

## **ESTABLISH RAPID BACK-UP AND RECOVERY PROCESSES AND TOOLS**

Unplanned outages happen. These tools are critical not only in response to outages but also in achieving regulatory compliance and e-discovery.

## **SET UP STORAGE MANAGEMENT PROCEDURES AND AUTOMATE THEM**

Automate data migration through tools that assist movement between platforms while retaining high availability to assist in disaster recovery and continuity of operations.

## **SELECT, IMPLEMENT AND TEST DATA MANAGEMENT TOOLS**

Data management tools protect and rapidly recover data without disrupting system availability. Some of these solutions allow organizations to create real-time snapshots that permit quick data or failed systems restoration to a specific point in time, without having to manually rebuild and restore data, without reinstalling.

## **ESTABLISH DATA VAULTS**

Data vaults are designed to integrate and automate records retention policies.

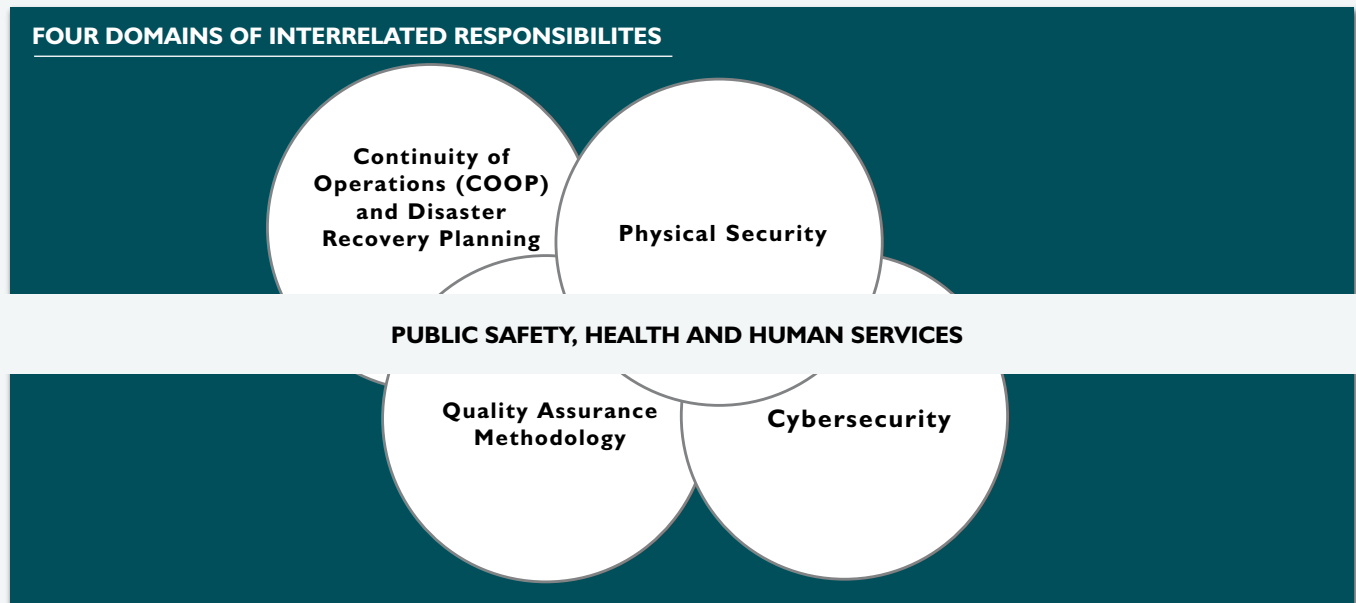


Figure 1 shows the interrelationships among the four domains: Continuity of Operations Planning (COOP), Physical Security, Quality Assurance Methodologies, and Cybersecurity. The four domains must be effectively coordinated with each other to ensure effective public safety, public health and the provision of needed human services in the midst of a crisis.

# Ten Points to Think About Before the Next Disaster Strikes

To realize the benefits of careful planning and wise investments in the security and resiliency of information technology, there are a number of dependencies that cannot be taken for granted — practical matters that are ignored or neglected at an organization's risk. Practicality is not a bad thing, although it often seems obvious in retrospect. Author Douglas Adams' character Ford Prefect, the hero whose quote begins this paper, understood this level of pragmatism when he wrote his guide to hitchhiking the galaxy and brought particular attention to the value of a most practical article — the towel.

In the spirit of having a towel close at hand, the paper now shifts focus to 10 practical and helpful considerations that may not have received the attention they deserve in your organization's planning process.

## 1) PUT PEOPLE FIRST

People run the organization, so take care of the people first. Find them a place to work and establish personnel accountability. Set up a Web site for employees to communicate with each other. Consider setting up a Wiki. Wiki is software used to create and edit a Web page using a Web browser, and creates an "open editing" environment. It encourages democratic and dynamic collaboration and allows users to participate in the direct supply and editing of content without the direct intervention of technical experts.<sup>16</sup>

Also, make sure your employees can access buildings where they work by having a ready supply of interoperable physical badges on hand. (See section number 8 on "Standards").

## 2) INTERNAL SECURITY IS INTEGRAL

While it is essential to ensure employee access, it is equally important to understand that without proper protection, a disaster can quickly put an organization at risk. Disasters can make organizations vulnerable to security breaches such as data tampering, theft and misuse.

Modern security best practices emphasize that securing the network only by protecting the borders is never enough. Although most employees are trustworthy and try to protect the organization's assets, it is also well known that some of the most serious and damaging security breaches have happened as a result of an "inside" job. Furthermore, as data sharing across government silos becomes more prevalent, the data value also increases exponentially. With data value on the rise, its theft or inappropriate use will have a devastating effect on the custodians of data (the agencies), and on citizens or public employees whose personal data may be breached by other unscrupulous employees with either a dollar to make or an axe to grind.

Restricting access to root directories, establishing field level encryption of the most sensitive data within databases or setting up secure vaults for files and data can go a long way to prevent criminal activity that may emanate from inside the firewall.

## 3) THINK SECURITY — A GREAT SOLUTION FOR SMALL AND LARGE DISASTERS

Harden the network against security breaches. Don't forget about prevention. It is more important than you might think. Security breaches can hurt a brand or the reputation of even the most respected institution. A security breach put eBay out of business for one day and its stock dropped 52 percent the next day. Stockholders have long memories, as do voters.

## 4) TREAT NEW DELIVERY CHANNELS AS MISSION CRITICAL, NOT JUST CONVENIENT

IT infrastructure today is riskier than ever, because it is mission critical in what government does — and how. The lesson of IT ubiquity is that today, it is not just IT that fails. When IT fails, government fails because IT is embedded in the fabric of government.

Think of the security and privacy in terms of e-government and citizen trust. Years of good will cultivated by e-government initiatives can be wiped away by a major security breach. Moreover, new service channels such as 3-1-1 call centers have also embedded themselves into the critical operational core of government. Originally implemented to take and rank public service requests in order of importance, the underlying customer relationship management (CRM) system is now being used as a workflow management system among governmental departments — but not yet included in COOP plans.

## 5) UNPLANNED OUTAGES

Unplanned outages can happen at any time. Traditional back-up and recovery approaches may not be enough to keep an organization running in the event of a serious incident. Traditional back-up and recovery approaches do not work particularly well for an organization's most valuable data, or when the public's safety is at stake. Fortunately, modern tools are available in the marketplace that allow for data to be continuously protected in real time. Although just a few years ago it was tantamount to heresy, forward thinking government IT shops now have the tools available to them which allow users to recover their own files; users can simply use Internet browsers to do so. Improved disk technology has converged with lower storage costs to create a sweet spot where user self-service is now an affordable reality.

## 6) DON'T FORGET THE FOURTH BRANCH OF GOVERNMENT — MEDIA

Every COOP plan should have a section devoted to dealing with the media. Think about the difference in public officials' responses after Sept. 11 and after Katrina for a hint about why this is important.

## 7) DESIGNATE A PARTNER CITY

Whether it is a hurricane like Katrina or terrorists' use of weapons of mass destruction (dirty bombs, attacks on nuclear facilities), cities may become uninhabitable for months or even years. A local government will need to relocate to handle the immediate aftermath of a catastrophe and its lingering affects. Designating one or more partner cities for relocation of the government seat and citizen population should be hard-wired into any COOP plan. When designating a city, consider matching with comparable entities that are located outside geographic threat circles. Also, consider who can mirror IT operations (hardware, software, operating systems and culture) during a localized emergency.

## 8) THINK STANDARDS

There is little value in relocating employees if they cannot get into the new facilities. One solution for all government agencies would be to adopt the FIPS 201 ID card standard<sup>17</sup> to permit employees to have logical and physical access to the resources needed to do their jobs in a new location. This will reduce the ramp-up time, allow staff to get into the building and more easily authenticate to networks and information systems. This also helps with external entities that may arrive at a disaster site to assist in the aftermath, if all cards follow the same standard.

## 9) HAVE YOUR OTHER IT DUCKS LINED UP IN ADVANCE

You are not ready to "bug out" of a compromised location until you have answers to these questions:

- How quickly do you need to get back up on your feet from a systems point of view? How soon do you need the Internet, data center operations or applications access? Is the time measured in seconds, minutes, days, hours, weeks? Determine which services are mission critical and how quickly each would need be brought back up and prioritize in what order.
- Do you have well-defined Service Level Agreements (SLAs) that specify the performance expectations about these IT assets, network and application availability and recovery timelines? Do you have them both with internal customers and external contractors?
- Do you have pre-awarded vendor contingency contracts in place? If not, do you have clearly defined emergency powers to enter into contracts quickly? Understand that predefined contracts may be preferable for most situations, while using emergency powers for many purchasing decisions may result in an increased risk for fraud, error, waste and abuse with the latter. Think: 22,000 federally

purchased mobile homes deteriorating in a mud-filled field in Hope, Arkansas while 55,000 Louisiana families wait for the right unit to arrive.<sup>18</sup>

- Do you have a plan to power your response and recovery? New Orleans CTO Greg Meffert reminds us that if an IT shop has a back-up generator for the data center that runs on diesel, don't assume you will have access to fuel. Consider a 10-day back-up supply.<sup>19</sup>
- How will you track what matters during response and recovery? Mississippi state CIO David Litchlitter recommends that to prepare for future disasters, government IT professionals should make sure they have application software to meet the needs of humanitarian efforts related to the disaster response. "This would include software for missing persons, warehouse and distribution management, and volunteer/donations management," Litchlitter said. Speaking about the last hurricane season, Litchlitter recalled: "We were forced to write or locate software for these functions."<sup>20</sup>

## 10) THINK ABOUT ROLES

What people do changes — and matters more — when confronted with an emergency. In reprioritizing work during the response and recovery period, consider:

- appointing and training an individual to serve as Chief Triage Officer. This person must have the authority to work across all boundaries and make decisions that stick.
- making a friend in accounting. Actuarially accurate threat scenarios are more likely to be funded when risk and cost can be properly balanced.
- ensuring depth and bench strength. Who is the backup to the backup to the backup?
- planning around the actual health and physical abilities and disabilities of a person when assigning tasks for a disaster scenario. The disaster is not the time to find out the electrician in the hazmat suit has a heart condition.
- getting some rest. One of the biggest individual problems in a disaster is the lack of sleep. Make sure you have designated a "Sanity Checker;" an individual not directly involved in the day-to-day activities of dealing with the disaster. Before asking someone, make sure you trust their judgment. Report to them frequently during the disaster and trust their judgment.

## If You Have a Telework Plan, Think of Making it Part of Your COOP Plan

If you don't have a telework plan consider getting one. (See the Center for Digital Government's strategic planning guide *Telework 360°* to provide a head start in putting a telework plan in place.) This is particularly important if you have a help desk and your help desk employees cannot get to their desks. Create a virtual help desk where employees

can perform duties from home or from a laptop where they can plug in to a wired network or access a Wi-Fi network. Set up the ability to do Internet voice calling, referred to as Voice Over Internet Protocol (VOIP).

## Think Third World, Act New World in New Ways

The phrase "blasted back to the stone age" applies here. Many technologies being used in developing countries may come in handy when "New World" technologies fail to deliver. Also, continue to think about how to use new world technologies partially or in different ways. The following list is not exhaustive but provides a starting point for thinking through the little things that will have big impacts when operations are under siege.

- When your cell phone doesn't work, try text messaging (sometimes this service works even when voice does not).
- Try instant messaging. There may be no standard phone connections but the Internet may be accessible.
- Cell platforms can be brought in on wheels, boats or floated in on balloons.<sup>21</sup>
- Consider setting up a Family Radio Service (FRS) in advance, such as the network created in the D.C. metro area.<sup>22</sup>
- Set up an ad-hoc, mobile, low-power wireless network. The Champaign-Urbana Community Wireless Network (CUWiN) nodes run on batteries powered with two to 14 watts of electricity; wireless-equipped handhelds are deployed in key locations to form a mesh infrastructure; the devices would "virally update first responders with needed information..."<sup>23</sup>

- Use hand-cranked computers.
- Use bike-powered generators.
- Use solar and wind power.
- Use portable water purifiers/filters; purifiers are the safest and straw filters are the most convenient (the caveat with choosing these devices is to investigate risk vs. reward).
- Use runners and mountain bikers for communication.
- Use hand tools.
- Ensure (in advance) that there are bridges between radio, wireless and Wi-Fi, all running across IP (Internet).
- Have satellite voice and data phones on hand.
- Keep a sex offender database on a thumb drive if you manage a shelter.
- Keep Gigs of portable flash memory around for data and images.

## Conclusion: Because Disasters are not a Matter of “If” but “When,” What are You are Going to Do?

In a complex world characterized by natural and manmade disasters, service interruptions are inevitable. Proper preparation is both the governments' and the public's insurance policy, redeemed when disasters strike. State and local governments have much to learn from the discipline of continuity of operations planning in the public and private sector while preparing for the next inevitable disaster.

Learning from the COOP discipline, reviewing the policy framework and understanding the resources available from key contributors to the continuity of operations planning arena are all important approaches that state and local governments can use today. The endgame of IT continuity and disaster recovery planning is to maintain high availability and security as it relates to an organization's information assets, and automated tools and solutions are available to assist in organizations' preparation.

There are also several practical tips that are broader than IT solutions. These are solutions that government officials may not have considered when developing COOP plans. These recommendations run the gamut from designating partner cities and creating a virtual help desk to using new world technologies and technologies created for developing countries when advanced technologies fail to deliver in disasters.

# Endnotes

- <sup>1</sup> Office of Government Commerce, Information Technology Infrastructure Library (ITIL), Internationally recognized best practice processes for IT Service Management. <http://www.itil.co.uk/>
- <sup>2</sup> Software Engineering Institute, Carnegie Mellon, "What is CMMI?" Updated February 2, 2006. <http://www.sei.cmu.edu/cmmi/general/general.html>
- <sup>3</sup> The Committee of Sponsoring Organizations of the Treadway Commission (COSO), Responsible for the "internal controls framework" for enterprise risk management. COSO is an umbrella group of accounting and financial management organizations. <http://www.coso.org/publications.htm>
- <sup>4</sup> Project Management Institute, "Project Management Body of Knowledge (PKBOK Guide)," 2005. <http://www.pmi.org/>
- <sup>5</sup> Information Security Form (ISF) is a leading world authority and information security, "The Standard of Good Practice for Information Security Version 4.1." January 2005. [http://www.isfsecuritystandard.com/index\\_ie.htm](http://www.isfsecuritystandard.com/index_ie.htm)
- <sup>6</sup> ISO17799 is "a comprehensive set of controls comprising best practices in information security" published by the American National Standards Institute (ANSI) <http://webstore.ansi.org/ansidocstore/product.asp?sku=ISO%2FIEC+17799%3A2005>
- <sup>7</sup> the Information Systems Audit and Control Association (ISACA), "COBIT 4.0 Released." December 16, 2005. <http://www.isaca.org/>
- <sup>8</sup> the Information Systems Audit and Control Association (ISACA), Certified Information Systems Auditor Program, 2005. [http://www.isaca.org/Template.cfm?Section=CISA\\_Certification&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=16&ContentID=4526](http://www.isaca.org/Template.cfm?Section=CISA_Certification&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=16&ContentID=4526)
- <sup>9</sup> <http://www.nemaweb.org>
- <sup>10</sup> David E. Liebersbach, Immediate Past-President, National Emergency Management Association And Director, Alaska Division Of Homeland Security And Emergency Management, "Incident Command, Control, And Communications During A Disaster." Testimony Before The House Committee On Homeland Security Subcommittee On Emergency Preparedness, Science And Technology, The United States House Of Representatives, September 29, 2005. <http://www.nemaweb.org/?1457>
- <sup>11</sup> Association of Contingency Planners <http://www.acp-international.com/index.htm>
- <sup>12</sup> Centers for Medicare and Medicaid Services, HIPAA Security Final Rule. [http://www.cms.hhs.gov/Securit yStandard/02\\_Regulations.asp#TopOfPage](http://www.cms.hhs.gov/Securit yStandard/02_Regulations.asp#TopOfPage)
- <sup>13</sup> Department of Health and Human Services Office for Civil Rights, HIPAA Privacy Rule Summary. <http://www.hhs.gov/ocr/privacysummary.pdf>. Hugh K. Webster, "Association Governance in the Post-Enron Era." Association Law & Policy, American Society of Association Executives, December 2003. <http://www.asaenet.org/Publications/EnewsletterArticleDetail.cfm?ItemNumber=10991>
- <sup>14</sup> The Committee of Sponsoring Organizations (COSO), "Enterprise Risk Management — Integrated Framework." September 2004.
- <sup>15</sup> Hugh K. Webster, "Association Governance in the Post-Enron Era." Association Law & Policy, December 2003. <http://www.asaenet.org/Publications/EnewsletterArticleDetail.cfm?ItemNumber=10991>
- <sup>16</sup> Bo Leuf and Ward Cunningham, The Wiki Way Website, 2000. <http://wiki.org/>
- <sup>17</sup> National Institute of Standards and Technology, "Personal Identity Verification of Federal Employees and Contractors." February 25, 2005. <http://csrc.nist.gov/piv-program/>
- <sup>18</sup> Eric Lipton, "Trailer Dispute May Mean Thousands Will Go Unused." New York Times, February 14, 2006.
- <sup>19</sup> Merrill Douglas, "After the Storm." Public CIO and Government Technology, February 2006.
- <sup>20</sup> Ibid.
- <sup>21</sup> James MacPherson, "N.D. to Test Balloons for Cellular Service." Associated Press, January 30, 2006. <http://www.breitbart.com/news/2006/01/30/D8FF53180.html>
- <sup>22</sup> The DC Emergency Radio Network uses small handheld walkie-talkie radios that family and friends use to keep in touch. In an emergency users can tune to Channel 1 and assist in message relay. <http://www.dcradio.org/dcern.html>
- <sup>23</sup> Sascha Meinwrath, "Disaster Recovery & CUWiN." Public Ponderings Blog, August 30, 2005.



© 2006 e.Republic, Inc. All rights reserved.  
100 Blue Ravine Road  
Folsom, CA 95630  
916.932.1300 phone  
916.932.1470 fax  
[www.centerdigitalgov.com](http://www.centerdigitalgov.com)

Underwritten by:



Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at [www.symantec.com](http://www.symantec.com).

CENTER FOR  
**DIGITAL**  
GOVERNMENT

**Acknowledgements:**

**Al Sherwood**, Senior Fellow for the Center for Digital Government and former deputy CIO for the state of Utah

**Paul W. Taylor, Ph.D.**, Chief Strategy Officer for the Center for Digital Government and the Center for Digital Education

**Richard Varn**, Senior Fellow for the Center for Digital Government, former CIO for the state of Iowa and former Iowa state senator

The Center for Digital Government, a division of e.Republic, Inc., is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century.

The Center's special reports and papers provide two decades of experience and insight into the most important policy and management issues facing governments, and offer strategic approaches for planning and implementing technology, funding sources, and case studies from jurisdictions.