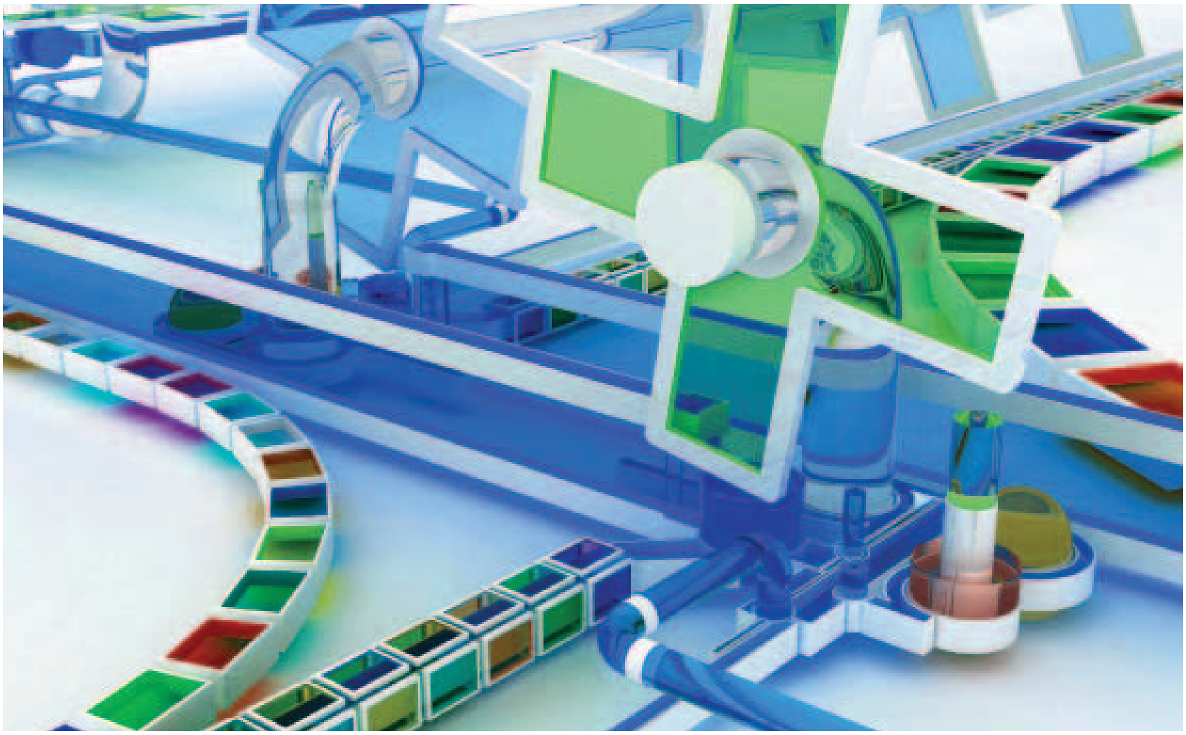
Continuity of Operations

Full strategic report at: www FCW.com/COOP2010



Inside:

Federal Executives Describe Continuity Planning Progress

In light of the recent gulf oil spill, one of the most devastating environmental catastrophes in history, the complete lack of an adequate incident response or disaster recovery plan has been widely criticized both in the media and in the halls of Congress.

Luckily, it appears that the ongoing public sector investment in continuity of operations planning (COOP) technologies and practices is starting to pay off.

More than half of 250+ respondents to a recent survey entitled, Continuity of Operations in the Federal Government, A Candid Survey of Federal Executives said their agencies were moderately prepared to function during an emergency and individually, 66% reported they would be able to function with little or no disruption in the aftermath of an interruption or disaster. Meanwhile, an additional 21 percent believe they could function, but with significant disruption.

Overall, more than 90% of respondents said the ability to perform their jobs in the aftermath of an emergency is critical, or at least very important. The survey was conducted via email by the Government Business Council and sponsored by CDWG and EMC. The survey was sent by email to a sample of federal executives, and only federal executives of GS-9 grade or higher are included in the analysis.

Key findings from the survey include:

- Seven in ten federal executives said they could identify actions taken by their agencies to develop a Continuity of Operations (COOP) plan. More than half of respondents said the agencies have published a policy or plan, and almost as many have identified requirements for COOP.
- More than 50% of federal executives said they can be away from their worksite and still complete the core responsibilities of their job, even for six days or more. An additional 20 percent could do so for one to five days. The rising use of mobile technologies and Telework were cited in the report as possible reasons for this finding. On the flip side, eight percent say they can not function in their job away from their workplace regardless of their eligibility to Telework.
- Just over half of the survey's respondents agreed their agencies have provided sufficient training to deal with emergencies. However, 80 percent reported their agencies could do a better job of preparing them to ensure continuity in the event of an emergency or disaster. Approximately 40 percent said their agencies have provided training, developed recovery priorities, or allocated IT resources. But fewer, (27 percent) said their agencies have allocated financial resources to ensuring COOP.
- More than half of respondents (55 percent) said their agencies hold drills annually or more often, and 49 percent report their agencies hold information or training sessions at least annually. Just over a third said their agencies provide multimedia content for training. Just over half (57 percent) said their agencies use a published plan for COOP. Remarkably, however, 24 percent of respondents didn't know what their agencies have done to develop a continuity of operations plan.

Challenges Remain

Despite a seemingly growing confidence in their ability to function away from their work locations, federal executives still reported extensive concerns about ensuring continuity of operations. More than 80 percent are concerned about operational issues, and 85 percent reported concerns about technical issues. The most often mentioned operational concerns are that worksites will not be accessible, mentioned by 65 percent of respondents, and that programs and services will be interrupted, cited by 63 percent.

Among the top technical concerns mentioned in the survey were that communications technologies will fail (mentioned by 62 percent) or that data won't be accessible from a remote or offsite location (54 percent). Just under half are concerned that servers will be overloaded. Approximately half of federal executives surveyed also worry that they have insufficient tools for remote access, despite previously proclaiming the ability to work remotely. Data recovery issues are relatively low on the list of technical concerns in an emergency situation. Less than one in four federal executives (24 percent) worry about the time it will take to recover data, or the loss of data.

In particular, 65 percent of federal executives expressed concern about worksite accessibility during an emergency. Almost as many (63 percent) are worried about the general interruption of programs and services. About half of federal executives also worry that agency employees are unsure of what to do to in the event of an emergency or disaster. At the same time, however, far fewer (23 percent) expressed concern about compromising the security of information, or an interruption in the chain of command, which was mentioned by 26 percent.

Although a variety of obstacles may have contributed to hindering agency preparedness, no single challenge was identified by a majority of respondents. Thirty-six percent of federal executives cite a lack of training, and 30 percent believe lack of coordination and restrictions on Telework have hindered COOP preparations. Only 20 percent believe that any kind of lack of technological tools is a significant obstacle. Indeed, while most federal executives believe a wide variety of tools are critical to ensuring continuity of operations, they were far less likely to report actually having access to these tools. For example, Almost 70 percent believe updates and advisory messages are critical, but only 40 percent report such messages are provided by their agencies. In addition, most federal executives said mobile data devices are critical to COOP, but only 44 percent report they are currently provided by their agency. Meanwhile, an overwhelming majority of federal executives (85 percent) said remote access is critical, but only half reported their agencies currently provide it. Similarly, four in five respondents said data backup and recovery systems are critical, but only 56 percent said those systems are provided.

Obstacles Ahead

Federal executives reported a variety of obstacles to ensuring continuity of operations, ranging from lack of training to lack of technology. They select an average of three challenges or obstacles each. Still, no single issues stood out in the survey as the largest impediments, and no single obstacle was selected by a majority of respondents. For instance, about a third of respondents say lack of training and coordination, lack of understanding, and Telework eligibility requirements are obstacles to successful COOP planning. Twenty-seven percent reported COOP is not an agency priority. A quarter or fewer of respondents said a lack of funding, security regulations, or a lack of technological tools play a role in hindering agency preparedness.

As hacks on agency web sites have grown more sophisticated, and reports are rising that hackers may have ties to foreign governments or criminal organizations, the entire survey underscores how federal COOP and security strategies must be more closely aligned to address viable threats. Clearly, the ongoing threat of a terrorist attack, pandemic or other natural or manmade disaster isn't likely to go away. "The good news is federal executives are definitely better prepared than a few short years ago, as COOP adoption rates are up, along with the use of remote access solutions for employees," said Jeff Godlewski, manager of server storage solution architects for CDWG.

At the same time, it's also clear still more must be accomplished. For instance, Godlewski said, there's a need for greater communication of continuity plans, especially when it comes to including more staff and bringing together more divisions and groups that were previously siloed, such as human resources and building facilities organizations. "Communication of the plan and the inclusion of all personnel simply hasn't been given the same attention as failover technologies, but can help any organization prepare more effectively," he said.

As federal agencies and departments continue to sharpen their focus on the most likely threats and protecting their most critical functions, Industry watchers say reaching out to industry partners, and taking the time to connect with peers to share best practices and 'out of the box' thinking may also help improve COOP and lighten the financial burden of ongoing COOP investments. ▼

USGS Bolsters COOP Using a Content Delivery Network

Just over a decade ago, the U.S. Geological Survey (USGS) identified replication and redundancy as key requirements to its mission, following multiple data processing and delivery disruptions due to network outages, hurricanes and other unpredictable events.

In August and September 1999, Hurricanes Dennis and Floyd caused significant disruptions in the analysis and delivery of North Carolina data and became the catalyst for the creation of a more resilient processing and delivery system. That's when the USGS Water Resources National Water Information System (NWIS) Program began investigating how to ensure that "near real-time 'streamflow' data could be reliably processed and served via the Web," said Kevin T. Gallagher, USGS CIO and Associate Director for Geospatial Information.

A team from across the USGS was brought together including data, database, network, computing and process experts to evaluate requirements for data acquisition, analysis and delivery. At about the same time, in October 1999, a magnitude 7.1 earthquake rocked southern California, squashing the USGS Earthquake Hazard Program server in Menlo Park. The organization quickly determined that three distributed servers might work better. Those distributed servers were in place by the time the Nisqually earthquake hit the same region in February 2001, and USGS analysts noted that using Squid proxy and caching servers in front of Web servers significantly improved data delivery. However, officials understood building enough infrastructure to manage 'flash crowds' – the instantaneous peak in demand for data from people who feel earthquakes – and ensure availability would not be cost effective.

Instead, the USGS decided to use a combination of redundant servers at its data centers and a commercial content delivery network (CDN) service. The CDN service manages 'flash crowds' for earthquake data requests and provides cached access to data from globally distributed systems. Access to source data is critical to USGS's primary mission, providing updated, refreshed content to citizens as well as internal programs and processes. "A CDN allows us to get the job done with an infrastructure we don't own, but rather lease through the CDN contract, to reduce our costs," Gallagher said.

USGS entered into a contract with Akamai Technologies Inc., in 2002 to ensure delivery for content that experiences extreme spikes. "This contract was expanded to provide round-robin Domain Name Server (DNS) support to fan out requests between available USGS servers, which are mirrored," Gallagher said.

By September 2003, the USGS National Water Information System Web System (NWISWeb) was fully rolled out to provide emergency backup data processing and replicated delivery. Since then, Gallagher maintains, using a CDN to ensure the availability of high visibility USGS data has proven highly effective. Because the USGS is required to provide the most up-to-date information available, the CDN delivers reliable access to source data for content that has rapid, or frequent updates. "Having a replicated infrastructure to both manage and provide data to all distribution points is very important to ensuring the continuous availability of the most recent content," Gallagher said.

The agency now collects and shares data using a combination of redundant servers at its data centers and the CDN services. In 2009, the Akamai contract was up for renewal and Level 3 Communications, Inc. was awarded the new contract in

A Little Background

At the U.S. Geological Survey (USGS), the mission is science – including the collection, analysis and distribution of data and information used to help answer an array of complex questions that span multiple disciplines in the realm of natural sciences, to serve U.S. interests.

The USGS has 8,500 employees in 400 locations around the world. USGS maintains data centers in the U.S., but its technology reach extends to stream gauges, volcano sites and earthquake reporting stations around the world.

In 2009, USGS reported the following from Netflow statistics and log file analysis:

- 2.2 petabytes of data transferred from all ports in and out of the USGS;
- 660 terabytes of Web traffic in and out of USGS, not including content delivered by Level 3 to the public earthquake related web sites and www.usgs.gov;
- 127 terabytes of data delivered by NatWeb, which hosts half of the USGS Web sites including www.usgs.gov, but not NWISWeb or the earthquake sites.

Source: USGS

June. So far, the CDN services provided by Akamai and then Level 3 have worked well to handle 'flash crowds' such as the one that occurred, striking USGS servers during the July 2008 Chino Hills earthquake, when a record peak of 17,000 hits per second was set. That record was later broken in April 2010, when an earthquake measured at a 7.2 magnitude hit the Baja California region on Easter Sunday, and a new record of 52,000 hits per second was set.

During such events, the CDN performs 'bursting,' replicating requested data through the global network, serving increasingly more bandwidth to users until peak demand is satisfied. Then, the CDN eases off replicating, as demand drops back to more typical levels. USGS pays service fees both for DNS and bursting charges.

Data coming into USGS, such as earthquake sensor and streamflow data, travels multiple paths from thousands of stations to redundant systems to ensure delivery to the USGS emergency notification system and to the public. USGS Web content hosted within the NatWeb infrastructure, such as local science centers and many National USGS Program sites, is managed within a cloud of file and Web servers at three data centers across the U.S. Each center's servers are configured identically for backup purposes, with data replicated among all servers.

The current environment supports the agency's COOP plan, and allows USGS to continue to provide access to natural resources data – no matter the demand. A CDN with a worldwide presence reduces geographic latency, or the distance between the requester and server, Gallagher explained.

Lessons Learned

Over the years, USGS has learned testing the system is important. In addition, monitoring web sites before, during and after an event can help improve resiliency and recoverability as well. In all phases of the information lifecycle, organizations must build and account for redundancy. Gallagher recommends that organizations design any web infrastructure with both performance demands, and outages in mind, and plan for the necessary redundancy up-front. The current server infrastructure, along with the use of a CDN, allows the USGS to gather data and keep it available even when demand peaks during emergency situations.

As part of life cycle planning, the Enterprise Web Program and USGS will continue to evaluate strategies for delivery of USGS content and information taking into account a fluctuating budget, security, performance and technology requirements. ▼

NIST Updates Federal IT Contingency Planning Guidelines

The National Institute of Standards and Technology (NIST) recently issued a first update to its primary contingency planning guideline document, which is already widely used throughout federal, state and local governments as well as many private sector organizations.

As the institution responsible for developing standards and guidelines that provide adequate information security for all agency operations and assets, NIST made several substantive changes in Revision 1 of Special Publication 800-34. According to Marianne Swanson, Senior Advisor for Information System Security, NIST in Gaithersburg, Md., the overarching changes in this revision include:

- Coverage of three common types of platforms, making the scope more inclusive of client/server environments, telecommunications systems and mainframes. Previous categories, including desktop computers, servers, web sites, local area networks, wide area networks and distributed systems have been consolidated into the three platform types.
- There is a bigger focus on the Information System Contingency Plan (ISCP) as it relates to its impact on Federal Information Processing Standards (FIPS), specifically FIPS 199. More information about FIPS 199 is available at *http://csrc.nist.gov/publications/fips/fips199/FIPS- PUB-199-final.pdf*
- Categories for General Support Systems (GSS) and Major Applications (MA) have been removed.
- Introduces the concept of resiliency and shows how ISCP fits into an organization's resiliency effort.
- Works to more clearly define different types of plans included in resiliency, continuity and contingency planning.
- Incorporates the use of 'call out' boxes to clarify specific differences and relationships between COOP and ISCP.

Resiliency is a concept gaining widespread acceptance in contingency planning. An effective resiliency program includes risk management, contingency and continuity planning, and other security and emergency management activities, Swanson said in her presentation on the newly revised NIST 800-34 Rev 1.

Another important change, the Business Impact Analysis (BIA) was revised to more closely tie to federal standards and guidelines. The BIA process now takes into consideration that impact levels are determined as part of the security categorization process.

Also, the 'Testing, Training and Exercises Section' was more closely linked to other federal standards and guidelines, including NIST SP 800-84 the Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, which is available at *http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf*

And this section was also more closely linked to FIPS 199 to reflect appropriate timing for testing of contingency plans. For low-impact systems, a yearly tabletop exercise is sufficient, while for moderate-impact systems, a yearly functional exercise should be conducted, and for high-impact systems, an annual full-scale functional exercise should be conducted. ▼

Upcoming COOP Related Planning Guidance

Federal agencies and departments should look for additional contingency planning-related guidance, which is expected to be published by NIST in 2010, such as:

- NIST SP 800-39, Enterprise-wide Risk Management: Organization, Mission, and Information Systems View, public draft release in June 2010.
- NIST SP 800-53-A Rev.3, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, public draft release in June 2010.
- NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, public draft expected July 2010.
- NIST SP 800-18 Rev.2, Guide for Developing Security Plans for Federal Information Systems and Organizations, public draft expected in October 2010.

Telework Gets a Boost in Congress After Winter Closures

During the sweltering D.C. summer, the National Labor Relations Board released a report on employee productivity driven by last February's punishing winter storms in the national capitol region which forced the closure of government offices for four straight days.

White House officials want Congress to approve more Telework options for federal workers, arguing the government could save millions in lost productivity during bad weather if employees could work from home during major snow events, or other emergencies, such as a possible pandemic outbreak. Also, The Patent and Trademark Office issued a separate statement outlining productivity savings achieved during the snow closures. So far, however, two similar bills faced mixed results in House and Senate votes. The Senate approved legislation to expand Telework opportunities for federal employees, after a setback for a similar bill in the House early in May. By unanimous consent, the Senate passed the Telework Enhancement Act (S. 707) sponsored by Sens. Daniel Akaka (D-Hawaii) and George Voinovich (R-Ohio). The Senate bill remains tabled as of presstime as amendments have forced a reexamination of the legislation's costs.

The 100 Year Storms

Early in 2010, when storms in the mid-Atlantic dumped more snow than at anytime in the last 100 years, the Office of Personnel Management was forced to close government offices throughout the D.C. metropolitan area. Several news reports estimated the cost of the closure at $100 million per day - based on work being completed by federal employees during that time. However, the survey conducted via email by the National Labor Relations Board found that on a verage 179, or 49.6 percent of headquarters employees engaged in Telework for approximately 3.32 hours on any given day of the closure. In total, those employees worked 1,867 hours. Another 6.4 percent of survey respondents reported coming into the office at least one day during the closure event, for a total of 128 hours.

The email survey, commissioned by Inspector General David Berry achieved an 87.9 percent completion rate and was conducted in accordance with quality standards for inspections issued by the President's Council on Integrity and Efficiency. Agency officials said the National Labor Relations Board has devoted significant resources to building and maintain its IT infrastructure in recent years, which is why agency systems can now be accessed by employees from any location with an Internet connection. Even the agency's email is available to computers and mobile devices with Internet access. More than two-thirds (67 percent) of respondents have a government laptop computer which they can take home. And approximately 44 percent access agency networks and systems via the use of RSA tokens. Almost 36 percent of employees had a government laptop at home during the storm closure.

If and when it's signed into law, the Telework Enhancement Act could go a long way toward increasing the use of Telework for government employees. While some industry observers still see the goal of a Results Only Work Environment (ROWE) as a distant dream, this approach to managing employees based on the work they do, not when or where they do it, is starting to take hold in some industries. Using ROWE, where an employee is located doesn't matter, as long as all job tasks are completed. Regardless whether the federal government can fully embrace Telework for large numbers of employees, the recent evidence from federal agencies shows that Telework offers great promise as a tool for operational continuity during emergencies. ▼

COOP Basics: How to Ramp up Preparedness Now

NIST defines contingency planning as the interim measures to recover information system services after a disruption.

Continuity of operations planning (COOP) is currently used by all federal government organizations to help restore operational IT support for personnel, partners and constituents in the event of an emergency that causes a loss of facilities or computing assets. COOP initiatives mandated by federal oversight authorities require agencies to select functions considered essential to operations. Essential functions consist of the tasks personnel must perform regardless of circumstances. Examples include health care, law enforcement, border patrol, communications and environmental containment.

For many federal organizations, safeguarding electronic assets and data is also considered a critical component of COOP. Agencies must ensure electronic records and resources are backed up and mirrored at a second location in the event data and/or systems are damaged at a primary location. Agencies must also conduct tests and training exercises, to ensure the backup operations can support their needs if networks fail for any reason. This is why most federal agencies continuously seek ways to cost effectively speed recovery, provide enhanced network security, as well as offsite recovery locations. In recent years, COOP and Telework, for example, have been closely connected as a way for federal agencies to allow workers to access applications and information when they can't get to their usual offices -- in the event of a pandemic for example – when workers may be asked to stay home to avoid spreading germs for days or weeks at a time. Some federal organizations are also implementing virtualization solutions to lower costs and speed recovery.

For More Information

It's widely recommend that government organizations strive to prioritize each agency's actual risk and protect the most critical systems and applications. In addition to guidance available (see separate article in this Snapshot report) from the National Institute of Standards and Technology (NIST), there are several recently updated guidance documents available to assist organizations that are seeking more information and assistance. For instance, there's a comprehensive list of COOP-related resources available at: *http://www.fema.gov/government/coop/index.shtm*

Meanwhile, the U.S. Department of Health and Human Services (HHS), along with the Department of Homeland Security, the Office of Personnel Management and the Occupational Safety and Health Administration have all published new guidelines. Federal executives can learn more about what's available at: *http://www.fema.gov/emergency/nims/index.shtm*

The Department of Homeland Security also offers detailed advice in its National Response Framework (NRF), which presents the guiding principles that enable response partners to prepare for, and provide a unified national response to disasters and emergencies. More information is available at: *http://www.fema.gov/emergency/nrf/*

Agency personnel seeking more information can also talk to their management as well as the regional continuity point of contact (POC) responsible for coordination of the organization's COOP activities. For convenience, personnel may call:

- Region I (CT, MA, ME, NH, RI, VT) – (617)832-4798
- Region II (NJ, NY, PR, VI) – (212)680-8504
- Region III (DC, DE, MD, PA, VA, WV) – (215)931-5641
- Region IV (NC, SC, KY, TN, GA, AL, MS, FL) – (770)220-5453
- Region V (MN, WI, IL, IN, MI, OH) – (312)408-5389
- Region VI (LA, AK, OK, TX, NM) – (940)898-5131
- Region VII (IA, KS, MO, NE) – (816)283-7082
- Region VIII (CO, MT, ND, SD, UT, WY) – (303)235-4658
- Region IX (AZ, CA, NV, HI, Guam, Pacific Islands) – (510)627-7009
- Region X (AK, ID, OR, WA) – (425)482-3721
- FEMA HEADQUARTERS (NCR) – (202)646-4282 ▼

People depend on you. All the more reason your systems can never stop.

System crashes, power failures, security breaches and natural disasters. These unplanned events can bring an agency's IT infrastructure to a standstill. Keep your operations up and running with continuity solutions from CDW•G. With extensive government experience, our team of technology specialists can recommend the archiving, backup and disaster recovery strategies to help you achieve your mission. And with total lifecycle support, we make it easy. From assessment and design to implementation and installation, CDW•G has the inside knowledge to protect you from the outside world.

Quantum® SuperLoader™ 3 LTO-5 8 slot

$5299.99

CDWG 2019445

Quantum

APC® Smart-UPS® 3000VA LCD 120V

$992.50

CDWG 1988083

APC by Schneider Electric

Symantec™ Backup Exec™ 2010

Single-user license with one-year Essential Support[1]

$741.13

CDWG 1979649

symantec.

CDW•G

Be unstoppable with CDW·G. 800.767.4239 | CDWG.com/federal

[1] Essential Support includes 24x7 technical phone support and upgrade insurance; call your CDW•G account manager for details. Offer subject to CDW•G's standard terms and conditions of sale, available at CDWG.com. ©2010 CDW Government LLC