



Data Solutions

Full strategic report at:

www.FCW.com/DataSolutions



Inside:

- Achieving Data Center Modernization in Government Operations, s2
- ARRA, Modernization Efforts Drive Greater Energy Efficiency, s4
- Spotlight on Government Drivers and Benefits of Virtualization, s6 • Federal Data Goes Mobile, s7
- Update on Government Continuity of Operations (COOP), s8

Achieving Data Center Modernization in Government Operations

Government organizations must overcome hefty challenges to meet evolving IT mission goals in 2009 as the impact of the ongoing economic crisis, along with wars overseas and an extensive economic stimulus program are complicating their efforts to modernize, consolidate and transform data center operations.

For instance, while a general rule for data center hardware has typically been three to five years between upgrade and/or replacement, in the current economic climate, government IT organizations are extending life cycles and leveraging legacy systems to squeeze more from existing IT assets, particularly servers, storage, and power equipment.

Meanwhile, regardless of the state of the economy, the amount of data to be managed continues to grow exponentially, especially as new types, such as video, continue to gain in popularity. At the same time, the sweeping changes 'stimulated' by the American Recovery and Reinvestment Act of 2009 will likely have the biggest long term impact, making government data centers more capable, effective and energy efficient.

Economic stimulus package appropriations total \$787.2 billion, with key funding initiatives to support technology, science and research, infrastructure improvements, education, energy, healthcare and training. Market research firm IDC estimates ARRA will generate more than \$100 billion in technology spending in the next five years.

Ultimately, for most government IT organizations, the goal remains to provide unified, real-time access to information, as well as visibility agency-wide into data residing on disparate systems, while reducing learning curves and creating a collaborative environment for faster, better decision-making. However, pressures faced by government IT organizations include new political policies requiring alterations in direction/focus, ongoing space constraints, a need for more and better security and continuity of operations, along with greater demand for resource availability and energy efficiency.

The ARRA funding initiative has both helped and hindered IT modernization efforts, industry observers say. On the plus side, by relying heavily on current federal contracts to fulfill ARRA program requirements, the federal government has moved quickly to implement IT modernization within Foreign Services, the State Department and the Social

Security Administration, for examples.

However, for many government organizations, ARRA is testing their ability to adapt to the changing priorities of a new presidential administration, as well as constituent demands for more and better services. When agencies use ARRA to set new operational processes into motion, the workforce, systems, capabilities and reporting systems struggle to keep pace with change.



At a recent conference on the Economic Stimulus program, hosted by 1105 Government Information Group, Mary Davie, assistant commissioner, Office of Assisted Acquisition Services, said the GSA is working with all agencies that ask for help on the reporting requirements for ARRA. Interestingly, federal agencies are also seeking GSA's assistance "in providing general IT and professional services, while they work on projects that allocate stimulus funding," she said.

Successful modernization efforts will likely hinge on how well agencies can bridge the gap between desktop computing, web-based collaboration and enterprise-level applications, according to federal tech industry veteran, Jorge Fuster, founder and principal of VirtualFedTeam, a federal IT staffing resources organization.

To simplify operations, conserve resources, streamline systems management, leverage legacy systems and manage

applications most government IT organizations are putting increased emphasis on strategic planning, which includes:

- Modernizing IT infrastructure to support government requirements;
- Securing information and assets;
- Integration of large and complex agency systems;
- Overcoming organizational and cultural barriers.

The good news, according to federal market research firm INPUT, is that despite the economic downturn, the ARRA program is helping agencies move forward on key IT modernization goals by allocating funding for a wide array of initiatives. Early funding initiatives related to transportation and education are already having a direct impact on state and local government budgets, according to Deniece Peterson, a principal analyst for INPUT in Reston, Va. “As monies are doled out for transportation improvements, for example, that in turn, frees other state and local funding for technology-related initiatives,” she explained.

To deliver services for government personnel, partners and constituents, federal agency leaders must evaluate technologies and services to help modernize operations and achieve compliance with the usual government regulations, along with new policies that strive for greater transparency in ARRA funding initiatives. In general, government IT organizations are working to automate operational processes, increase analytic ‘intelligence,’ manage risks, reduce costs, lower downtime and service interruptions and strengthen security protections that cover government information and resources. In fact, “automation is the driving force behind most IT modernization efforts today,” said Andi Mann, vice president of research for Enterprise Management Associates, Inc., in Boulder, Colo.

There are several disciplines involved in the automation boom, he explained, pointing to tools that can assist in improving performance, availability management, provisioning software, and regular backups. “The goal is to take out the human factor where possible to help data centers both in the public and private sectors to achieve greater efficiency and lower costs,” he explained.

EMA recently surveyed 239 different IT organizations and found that when they invested in data center automation, the average staff cost reduction totaled \$500,000 per year. While reducing management costs is the biggest driver for ongoing data center automation efforts, Mann said, “Reducing the potential for security breaches and enabling IT staff to move away from ‘firefighting’ and on to more strategic IT planning were two key benefits from greater automation.”

Throughout the computer industry, the pendulum has swung toward a general preference for software that’s centrally located, as opposed to programs that run on a

user’s personal machine. The combination of high-speed networks, sophisticated processors and fast, inexpensive servers and disk storage is driving more government computing into data centers. The current climate is also driving the advent of virtualization and has led to much publicity surrounding its technological cousin, cloud computing. Cloud computing is made possible by the proliferation of high-speed Internet connections, cheap, powerful chips and disk drives, and the development of data centers that house hundreds or thousands of computers to quickly serve sophisticated software to legions of users.

By utilizing technologies such as virtualization and using storage equipment that can scale to accommodate future storage needs, customers can avoid expensive rip-and-replace upgrades and extend the life cycles of their existing assets.

Government data center administrators are also stretching storage life cycles, via automated tools that support tiered storage and storage resource management (SRM). Through the addition of advanced SRM tools, for example, agencies can reduce storage costs by simplifying storage administration, and create a more streamlined continuity of operations strategy, along with better reporting on storage usage and energy costs.

Moving forward, the goal for federal agencies will be to create an advanced data center infrastructure that consolidates and simplifies the management and administration of government information to more quickly and efficiently deliver services to users. An open systems approach is crucial, as is a more automation to create the efficient, secure and cost-effective data centers of the future.

Federal IT Operational Advice

According to industry observers, the best way to leverage, protect and modernize government IT assets is to:

- Stretch the life span of IT equipment, using proper maintenance and leveraging newer technologies, such as virtualization.
- Moving parts are subject to wear and tear. Keep air intakes free of dust and debris.
- Find ways to leverage automation in repetitive processes, operations and applications.
- Automation can, for example, be helpful to install regular service packs, upgrades and patches to operating systems, firmware and applications.
- Have a continuous program in place to demonstrate how current applications meet agency needs, and where they fall short.
- Cost savings from automation and deleted applications can be used to fund other ongoing government IT transformation efforts. □

ARRA, Modernization Efforts Drive Greater Energy Efficiency

A heightened awareness of IT power consumption costs, the increasing use of high performance, high-density computing technologies and the impact of the American Recovery and Reinvestment Act are propelling government IT organizations toward greater energy conservation.

And it's a good thing too, as one market research firm has estimated the U.S. government wastes \$1 billion annually on poor desktop power management practices. According to research conducted by Steve Brasen, a principal analyst for Enterprise Management Associates, Inc., in Boulder, Colo., IT practices performed by government agencies (local, state and federal) have notoriously been the most wasteful of any industry demographic group. In the EMA research report entitled, *The True Value of Green IT*, the average weekly power consumption of desktop workstations used by government organizations is 46.31 kilowatt hours (KwH). "This was determined by calculating desktop utilization practices, including how often systems are left operational and how they utilize power saving features like sleep modes and hibernation," Brasen said.

Based on an average national retail price of electricity for the commercial sector of \$11.07/KwH, (compiled by the U.S. Department of Energy, August 2008), the average annual cost to power a single desktop government PC is \$266.58. "With an installed base of 6.7 million deployed workstations, that translates to a whopping \$1.7 billion in annual electrical costs to power these systems," Brasen said.

According to EMA's research, many federal, state and local government organizations would benefit from better system power consumption practices. EMA's research showed that government desktop systems were kept fully 'powered-on' nearly half (48%) of the time during non-work hours, such as evenings and weekends, versus only 19% of the time in high technology organizations. Meanwhile, 29% of government workstations had the power saving features completely disabled, versus only 12% of high technology workstations.

The core of the problem for most government agencies

stems from the financial infrastructure of the organizations. Most government institutions estimate operational costs, including electricity, based on past consumption and any expected growth, Brasen said. This funding is then set aside from the overall budget as an operational necessity. "The process allows very little incentive to reduce costs and streamline operations," Brasen said.

Lacking fiscal incentives to reward reduced power consumption, government agencies require the enactment of regulatory mandates. At the U.S. federal level, the Environment Protection Agency and the Department of Energy are only mandated to identify, report and advise on government power utilization. "It would require congressional legislation to either directly mandate the reduction of federal IT power consumption or to empower the EPA and/or DOE to oversee reductions in energy consumption," Brasen explained.

While the DoE has reported that the federal government is the largest energy consumer in the nation, renewed interest in reducing environmental impacts associated with excessive power consumption is helping to create a climate more conducive to achieving greater IT energy efficiency within government," Brasen said.

Meanwhile the American Recovery and Reinvestment Act of 2009 included several large fiscal projects created to help drive greater energy efficiency in government environments. For instance, opportunities are great for technologies related to the emerging smart grid, which will create a nationwide electrical power system and will largely be reliant on solutions that store, distribute, manage and measure energy consumption. "While there appear to be many energy efficiency opportunities within the overall ARRA initiative, questions remain as to the speed with which federal agencies will be able to adapt and move forward in implementing far-reaching energy reduction improvements," said Deniece Peterson, a principal analyst for INPUT.

That's because after heating, ventilation and air conditioning (HVAC) systems, data centers consume the most power in government buildings. The growth of servers



and storage is also adding to the strain on power and cooling resources. Meanwhile, increasingly network-intensive software and services also consume ever more power.

As older data centers are upgraded and newer ones are built, it's important to ensure that modernized infrastructures are highly energy and space efficient. Since the Energy Independence and Security Act (EISA) was signed into law in 2007, government agencies have been mandated to find new methods to improve energy efficiency. Government IT leaders should consider the power, space and cooling requirements of all data center components, and compare different architectures and systems to ascertain environmental and cost impacts across their data centers.

Other suggestions from industry observers that will help improve energy efficiency include:

- The ability to track resource usage, carbon emissions and efficient utilization of resources, such as power and cooling, are important.
- Strive to implement policies that can help conserve power, reduce cooling costs, maintain availability and support disaster recovery.
- Calculate how much electricity the data center currently uses and document the link between direct IT power utilization and costs avoided.
- Institute a four-year refresh cycle on computers.
- Use only Energy Star[®] rated monitors and computers, as those monitors go to sleep after 10 minutes and CPUs go to sleep after 30 minutes.
- Uninstall equipment that has become technologically obsolete. Industry observers estimate that up to 30 percent of servers in any given data center are no longer in active production, although they continue to consume energy.
- Storage area networks (SANs), improved storage management practices and higher density tape backup subsystems can also help lower energy costs and save space. □

Spotlight on Government Drivers and Benefits of Virtualization

Federal government organizations increasingly are incorporating virtualization to consolidate IT resources, reduce space and power consumption and gain greater agility in launching new applications and services for employees and constituents.

That's because virtualized servers, applications and storage can help reduce data center costs by consolidating servers and increasing utilization from a typical level of 5% to 10%, to as much as 60% to 80%. According to industry estimates, the primary benefits of virtualization technologies include:

- **Reduced downtime** – eliminating planned downtime and preventing or reducing unplanned downtime through the sharing of hardware and automated restart of application servers. Properly implemented, virtualization can enable a dramatic reduction in time to recover following a disaster.
- **Lower costs** – by reducing the need for added hardware and specialized software.
- **Simplified processes** – by removing the complexity of maintaining an exact duplicate of a data center's physical systems for COOP, and streamlining the recovery process.
- **Broader protection** – IT organizations can increase resource availability and ensure more rapid recovery of critical applications via virtualization.

Industry analysts note virtualization technologies play a key role in decreasing power consumption as well. "Virtualization can help government organizations reduce energy and space requirements, often by as much as 50%," said Andi Mann, vice president of research for Enterprise Management Associates, Inc., in Boulder, Colo.

Greater agility is among the biggest virtualization drivers, Mann said. In environments leveraging virtualization, administrators can ramp up new services far more quickly than in traditional software development, he said. The difference is dramatic, according to Mann. "Turnaround for new applications decreases from an average of up to 90 days, to a matter of two to four hours, which gives government IT organizations a real boost in responding quickly to ever-changing operational requirements," he said.

As government IT organizations learn to apply sophisticated management tools, they can also better

optimize virtualization's advantages, Mann said, including greater consolidation, staff savings and even further power reductions. Mann cautioned, however that a reduction in staff requirements may be an elusive goal. That's because while many organizations believe virtualization simplifies IT operations, it actually adds layers of complexity to existing physical computing environments, Mann said. "This, combined with a shortage of knowledgeable virtualization professionals are two of the primary reasons why some organizations haven't broadly invested in such solutions," he explained.

In fact, the primary obstacles to virtualization investments, according to EMA's research, are internal politics, along with difficulties inherent in dealing with multiple departments, as well as getting application owners to 'share' computing resources, Mann said. "The obstacles to virtualization are primarily driven by human issues, based on what survey respondents report," he explained.

Meanwhile, among organizations using virtualization, there has been a strong acceleration of both application and desktop virtualization technologies (up by an average of 25%, as compared to server-based solutions, which are growing at a steady 20% pace.)

In the future, Mann expects to see an increase in the number of IT organizations turning to virtualization services, rather than actual hardware/software-based technological solutions, due to the challenges associated with human issues, along with complexity, the cost of implementation and a general lack of support for applications in a virtual environment. "This may simply be easier to manage as a service, rather than as a stack of technologies that must be supported and centrally controlled," he explained.

One of the biggest challenges public sector organizations face as they plan for data center modernization is how to incorporate virtualization technologies to best leverage legacy systems and applications that are still widely used. Some industry observers claim the growing expense of data center infrastructures will make cloud computing attractive, as agencies could pay a set fee per hour for cloud computing services, rather than investing millions in additional data center construction. □

Federal Data Goes Mobile

Wireless mobility is changing almost all aspects of the way people work nowadays. Smartphones and PDAs are being used not only for voice calls, text messages and managing personal information, but also for tasks typically completed on a computer, including sending and receiving e-mail, browsing the web, storing and modifying documents, delivering presentations and remotely accessing data.

The recent shift in favor of smartphones and PDAs owes at least some of its strength to the presidential administration. Not long ago, Warren Suss, president of Suss Consulting, Inc., Jenkintown, Pa., said in a recent interview that such devices were only available for high-ranking federal officials who had to go way out of their way to justify their use. “Now, the perception is that smartphones and PDAs are productivity tools and a good investment,” he explained.

Increasingly, law enforcement, emergency management and a range of other government functions are being upgraded with wireless capabilities to increase productivity, accuracy and effectiveness. Handheld devices now feature many of the functions of a PC, including e-mail, web browsing, document viewing, music and video, along with mobile communication features such as Wi-Fi, Bluetooth, multiple forms of cellular service and Global Positioning System (GPS) receivers.

Today, the pressure is on to ensure that public and private sector organizations can centrally manage mobile technologies, said Steve Brasen, Principal Analyst, Enterprise Management Associates, Inc., Boulder, Colo. In his opinion, mobile management solutions are critical to government audiences, and must provide three key features, including provisioning (for downloading applications and automating security patches) secure malware protection (to ensure devices are restricted for authorized use only), and maintenance (to keep users productive). “Managing mobile devices can be difficult because there are so many different types available, and each offers its own brand of proprietary technology,” he said.

RIM officials have long maintained that BlackBerry’s own technology offers government a higher degree of security. Brasen maintains that in federal organizations, the ability to control the distribution, inventory and management of these devices is crucial to ensuring secure government operations.

At least for now, security remains a difficult challenge. “Losing a device or having someone pick it up is far greater with a handheld device that anyone can easily walk out of a building,” Brasen explained.

This is why he predicts a wave of solutions that will lock

down handheld devices for use only with specific applications. If a handheld device only functions for one application, it becomes useless for any other purpose. Also, likely to emerge, are solutions that make it easier to recover lost devices. The concept of lo-jack for mobile devices involves using wireless signals to tag (locate) a device and Tag and have it send a signal back that aids in its location. The other key area of concern is data protection, because the use of handheld devices only creates more point of access to government systems and information that are outside the control of agency firewalls. Brasen recommends government data remain encrypted, and that wireless connections must be secured from possible interception, to fully secure smartphones and other handheld devices.

While encryption and security protections may wreak havoc on battery power, that’s considered a small price to pay for greater security, he said. Meanwhile, another growing trend among wireless technology providers involves working with cellular technology providers to access their networks to verify the status of cellular towers and help users identify, for instance, when a cellular tower is down so they can clearly see why email may be temporarily unavailable, Brasen explained.

On the horizon, Brasen expects that there will soon be growing support for heterogeneous technologies to help bridge gaps in managing and supporting both Windows Mobile and BlackBerry devices. Centralized management is an even bigger challenge for Apple, which doesn’t currently allow third party agents to run on its iPhone, making it impossible to centrally manage these devices. “The big question for Apple is, when will the company address this acknowledged situation, by allowing third party agents to run on iPhones?” Brasen asked.

Further out, virtualization is likely to play a key role in “allowing users to run a variety of virtual applications on handheld devices, which will increasingly be used for more ‘laptop-typical’ computing applications in the coming years,” he explained. □

Update on Government Continuity of Operations (COOP)

The ongoing threat of a terrorist attack, pandemic or other natural or manmade disaster has forced a government-wide sharpening of disaster recovery response plans during the last several years.

In mid-June, for example, the Department of Homeland Security (DHS) conducted an exercise to test the readiness and capabilities of federal departments and agencies, coordinating with the White House, to execute their Continuity of Operations (COOP) plans. COOP is 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. The June exercise, known as Eagle Horizon, was a mandatory annual exercise for all executive branch departments and agencies coordinated by DHS through the Federal Emergency Management Agency (FEMA) and its National Continuity Programs (NCP) Directorate.

The exercise “was critical to testing our continuity of operations procedures and ensuring coordination across the federal government in the event of a major emergency,” said DHS Secretary Janet Napolitano, in a prepared statement. “A carefully designed and well-practiced national continuity plan significantly enhances our ability to react swiftly and effectively to any incident we may face.”

In a national emergency, federal departments and agencies may be required to relocate to alternate sites. Eagle Horizon simulates such an event, and triggers a cohesive, overlapping national continuity plan vital to the continued performance of essential government functions. The exercise focused on coordination between federal agencies and tested the Federal Executive Branch Continuity alert, notification and deployment procedures as well as interagency continuity communications. Emergency Relocation Group members were sent by their respective agencies to pre-planned alternate locations and asked to implement COOP procedures.

Continuity plans require agencies to select the functions that are essential to operations. Essential functions are those jobs that personnel must perform regardless of circumstances. Examples of such functions are health care, law enforcement, border patrol, communications and environmental containment.

Safeguarding electronic assets and data is also a critical element of COOP efforts. Agencies must ensure electronic

Emergency Preparedness Advice

These are among the best, most practical steps agencies can take to maintain readiness in the event of emergencies, according to industry IT watchers.

- Rank the order of each agency's applications recovery risk;
- Conduct a gap analysis to align IT management with application recovery risk mitigation priorities;
- Use the gap analysis results to drive 2009 disaster recovery initiatives;
- Address the agency's key pain points;
- Select and track the most appropriate IT disaster recovery continuous improvement metrics;
- Develop a 24/7 support strategy for key processes and applications;
- Invest in process, people and technologies for sustainable continuity of operations.



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 have been closely linked as a



way for federal agencies to allow workers to access applications and information when they can't get to their usual offices. For example, in the event of a pandemic emergency, workers may be asked to stay home to avoid spreading germs for days or weeks at a time.

Technologically speaking, when comes to quickly collecting, compressing (or deduplicating) and transmitting data, Data Domain provides a disk-based storage appliance for backup and disaster recovery that uses a compression algorithm designed to ensure data being transmitted doesn't already exist on a host platform. Technologies to aid in compressing and moving large volumes of data can be extremely important for disaster recovery purposes.

Some federal organizations are also implementing virtualization technologies to lower the cost and dependence on 'one to one' mirroring of data and systems for disaster recovery. Virtualization can help consolidate multiple servers onto one or more physical systems, allowing multiple virtual machines with dissimilar operating systems to concurrently run on the same physical host system. Virtualization can also help agencies achieve COOP goals by allowing IT organizations to 'reuse' older servers at disaster recovery sites, eliminating the need to buy new servers to comply with federal COOP regulations. □

Get more out of storage.

Get inline.



data domain

Optimize Your Backup and Archive Initiatives with High-speed Inline Deduplication Storage

- ▶ Shrink backup windows, reduce operational overhead
- ▶ Increase online data retention for fast restores
- ▶ Automate off-site data replication for secure, tape-free DR
- ▶ Enforce data retention with file-level locking

data domain

#1 IN DEDUPLICATION STORAGE

www.datadomain.com