Data Center Solutions

Full strategic report at:

www FCW.com/DataCenterSolutions

Inside:

Data Center Priorities for 2010

Market researcher INPUT identifies five key technologies that will help federal agencies streamline their operations and meet Administration goals.

As federal IT managers plan ahead, they're looking for technologies to drive down data center costs while boosting productivity, decision making, and customer service levels throughout the organization. According to a recent study by market researcher INPUT, there are five key technologies that have yielded similar benefits for private sector companies and are making their way into federal IT plans for 2010 and be yond. These technologies are:

- Cloud computing
- Virtualization
- Service-oriented architectures
- Open-source software
- Geospatial technologies

Outlined in INPUT's *Federal Industry Report: Emerging Technology Markets in the U.S. Federal Government, 2009-2014* that was published in February, these five technologies address IT-related goals set out by the Obama Administration; cost savings, operational and energy efficiency, information sharing/interoperability, transparency, and agility/flexibility. The study surveyed ninety federal and industry IT professionals in October and November of 2009 who said they expect these five technologies to have a major impact on their environments over the next five years as they move toward data-center consolidation, plug-and-play environments, geographically distributed computing power, and information sharing.

Acknowledging that federal agencies have been deploying these five technologies on a project basis, the INPUT report says that cost pressures and administration mandates will result in wider spread adoption.

"Over the next five years we'll see some fairly rapid adoption of these technologies," says Deniece Peterson, manager of industry analysis at INPUT, who was an author of the study. "While still a fraction of total federal IT spending, we'll see high growth in these areas."

Cloud Computing

One of the key benefits promised by cloud computing –

Adoption Rates of Five Key Data Center Technologies

Survey respondents' stage of adoption:	Cloud Computing	Virtualization	Service-oriented Architecture	Open-source Software	Geospatial Technologies
No plans to implement	24 %	19 %	29 %	33 %	27 %
Learning about it	24 %	5 %	15 %	11 %	3 %
Planning	24 %	16 %	21 %	14 %	19 %
Piloting	8 %	3 %	12 %	3 %	0 %
Already implemented	19 %	54 %	21 %	31 %	35 %
Don't know	1 %	3 %	2 %	8 %	16 %

Source: INPUT's Federal Industry Report: Emerging Technology Markets in the U.S. Federal Government, 2009-2014, a survey of ninety federal agency and industry IT professionals

defined as transferring some or all applications, compute functions, or storage from an organization's data center to a third-party provider – is flexibility, both from the computing model's usage-based payment structure and its self-service provisioning capabilities. Because cloud providers offer their services on a pay-as-you-go basis, federal agencies can contain costs by paying only for what they use, and self-provisioning lets them expand and contract computing resources as needed.

"Over the next five years we'll see some fairly rapid adoption of these technologies."

Deniece Peterson,

manager of industry analysis, INPUT.

One factor that may ease federal agencies' move to cloud computing services is the fact that they can be paid for out of operations and maintenance budgets, which tend to be more accessible to federal IT managers than capital investment funds, says Peterson.

However, there are still challenges regarding cloud computing that federal IT departments must figure out, such as ensuring sufficient security and privacy of data stored in the cloud, how to budget for flexible cloud-computing fees, and what the procurement methods should be.

Virtualization

Virtualization – technology that abstracts computing resources and separates out the operating system so the underlying machine can run multiple applications – reduces hardware, energy, and support costs. By consolidating the number of servers needed to run a data center, the amount of management required is also decreased. While virtualization is becoming easier to implement with more management tools available on the market, federal agencies will still need to grapple with the complexity of virtualizing legacy systems, find funding to reprogram for virtualization, and seek out IT professionals with the necessary skills to run these systems, according to INPUT.

Service-Oriented Architectures (SOAs)

These collections of computing services that communicate and work together to provide functions help agencies reduce integration costs and aid in speeding the development of new applications while encouraging reusability. The challenges organizations face when implementing SOAs include back-end complexity, a lack of unifying standards, and uncertainty regarding security, storage, bandwidth, and capacity planning issues, according to the report.

Open-source software

By shifting more projects to an open-source software base, agencies can reap the benefits of lower licensing fees, more agile application development, and greater code reuse. And, as is the case with cloud computing, open-source software can be funded out of operations and maintenance, rather than capital, budgets, says Peterson. Challenges with this technology include portability issues, ensuring code is free from malware, and support costs.

What could help spur open-source adoption is the fact that leadership in the Department of Defense (DoD) has released guidance encouraging the use of open-source software, and some of its components such as the Navy are already implementing it. "This stamp of approval will formally open the doors to the rest of DoD," reads the INPUT report. "Civilian agencies, which often follow in the footsteps of DoD, will look to DoD as a ... model for determining what to do and what not to do."

Geospatial technology

Traditionally geospatial technology has been used to acquire and manage data that focuses on geographic, temporal, or spatial contexts by agencies such as Defense, Homeland Security, and the Environmental Protection Agency. But there's a new use for this technology that enables agencies to collect, visualize, and map out complex ideas and concepts so they can be easily shared and understood by others, says Peterson. This leads to better business intelligence and improved service delivery. However, agencies will also have to deal with the implementation costs, uncertain return on investments, and the challenges of transparently expanding the volume of data that comes with this technology. ❑

NIEM and the Cloud

The National Information Exchange Model is making inroads among government agencies to facilitate data sharing. But this specification will face a whole new set of challenges in the cloud.

NIEM, the National Information Exchange Model, could become the basis upon which successful data sharing is achieved across federal, state, and local government agencies. This common data standard designed to facilitate critical information sharing in emergency situations, as well as promote data flow during day-to-day operations, promises to give agencies an unprecedented means for sharing data. However, there are still many unknowns regarding how well the data-sharing model will mesh with emerging technologies, specifically cloud computing.

> "If you have data in cloud A that you want to move or copy to cloud B, how do you say 'cloud B'? Most clouds don't have the concept that there is another cloud."
>
> Vint Cerf
> Chief Internet Evangelist, Google

NIEM, the result of a partnership between the U.S. Department of Justice and the Department of Homeland Security in 2005, is designed to enable "information sharing, focusing on information exchanged among organizations as part of their current or intended business practices," according to the NIEM Web site. "The NIEM exchange development methodology results in a common semantic understanding among participating organizations and data formatted in a semantically consistent manner."

The benefits of using NIEM to build strong information-sharing capabilities across agencies will aid first responders and other real-time decision makers – such as officials enforcing security at borders, airports, and seaports; local law enforcement; judicial processors; and correctional officers, the Web site says. NIEM will enable these officials to base their decisions on information that is complete, accurate, and up to date.

Sharing Data in the Cloud

At a NIEM training event in Baltimore last September, Internet pioneer Vint Cerf – who is now the Chief Internet Evangelist at Google – gave a keynote speech that posed a number of questions regarding NIEM and cloud computing. While Cerf offered words of support for the work that federal agencies are doing to implement NIEM, he also warned that cloud computing models may present some specific obstacles to sharing data.

"At the core of what NIEM is trying to do [is] trying to help people take information and make it sharable and therefore more usable," said Cerf. "It is in the cloud computing environments that the NIEM systems are ultimately going to have to work."

While cloud computing in some respects is well suited for sharing data – particularly when it comes to making sure data is up to date, since users collaborating on a project in the cloud can be assured that the information sitting in the cloud is the most current – questions arise regarding how multiple cloud infrastructures will work together.

Missing Vocabulary

"If you have data in cloud A that you want to move or copy to cloud B, how do you say 'cloud B'? Most clouds don't have the concept that there is another cloud … they have this missing vocabulary problem," he told the audience. Cerf offered an example of an organization wanting to move data from one cloud to another, or that began a computation in one cloud, ran out of resources, and wants to complete the computation in another cloud.

"What should a digital object be; what should a cloud expect when one arrives? I think NIEM has a great deal to say about those concepts, but the details still have to be worked out in many respects." Cerf told the audience. "As hard as you have worked on the NIEM ideas for data structures and meta data, about how to interpret things, and the semantics and syntax and everything else … as we start embedding that into the cloud environment we expand some of the challenges and demands being made on the treatment of that data." ❑

Virtualize for the Future

Faced with a budget freeze proposal for federal discretionary spending, agency IT managers are looking to make their technology dollars stretch farther than ever. Virtualization of data-center resources is a step in the right direction.

Standardization, flexibility, and consolidation – these are three ideas that federal IT managers must focus on now more than ever. Following the proposal for a three-year discretionary budget freeze by President Obama during his State of the Union speech in January, agencies are scrambling to figure out what such a spending hold would mean for them. For federal IT departments, it likely will mean a greater dependency on technologies that can be easily standardized on, are flexible enough to adapt to different scenarios and requirements, and can consolidate and utilize existing IT resources.

> "Virtualization is simply a more efficient way to use servers and full data centers."
>
> IDC Government Insights' 2010 State of the Union: Heating Up IT Investments During a Budget Freeze.

"With 2010 funding in place, federal agencies have a chance to work toward migration to new and hopefully more standardized systems that will give them greater flexibility for the future," reads a report by IDC Government Insights entitled 2010 State of the Union: Heating Up IT Investments During a Budget Freeze. "Agencies should spend this year developing long-term migration and consolidation plans, while launching those programs that they are able to get out of the starting gate. Proving cost-cutting concepts on a few high-profile programs can help spark more investments down the road, even in tighter budget times."

Real Benefits

Virtualization of data-center resources has shown to deliver some of the benefits that agencies are looking for today. By using virtualization to separate out applications from the hardware they run on, organizations can make better use of the servers they already have by running multiple applications on them, while at the same time easing server management, reducing energy consumption, and saving floor space. According to virtualization software maker VMware, organizations that implement virtualization typically save between 50 and 70 percent on their overall IT costs.

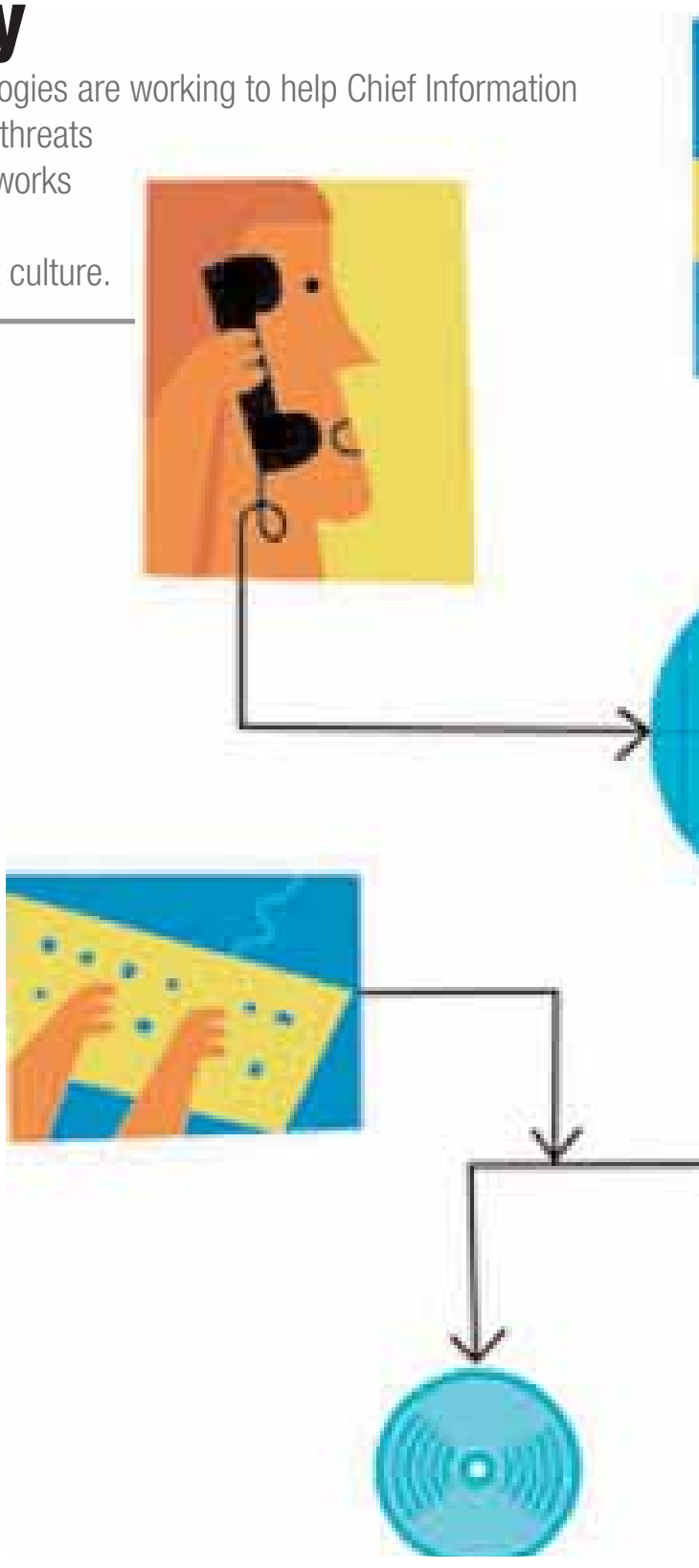
Agencies would be wise to spend money now in order to prepare for future spending freezes, the report continues, so that they don't end up hamstringing operations in the long run. If agencies spend money now on well-thought-out technology upgrades that address current challenges, they can enhance their IT infrastructures with long-term fixes that can weather tighter budgets down the road. In addition to virtualizing data centers, IDC Government Insights recommends that agencies consider Software as a Service, Infrastructure as a Service, customer-relationship management, Web-based services, collaborative interfaces, and IT dashboard technologies to help prepare for leaner times.

Consolidating IT resources through virtualization is not a new concept to federal agencies. The Food and Drug Administration, the Defense Management Contract Agency, and the Environmental Protection Agency are just a few organizations that have implemented virtualization software to consolidate hardware, minimize administration, and reduce maintenance costs. With the possibility of federal budget freezes, agencies should plan to hasten the move away from legacy systems and toward standard platforms that can optimize IT resources, says the IDC Government Insights report.

"Now is the time to get on the IT systems migration path or get caught up in the freeze and risk certain death," reads the report. "Virtualization is simply a more efficient way to use servers and full data centers." ❑

The State of Security

A handful of strategic data-center security technologies are working to help Chief Information Security Officers (CISOs) at federal agencies keep threats at bay. However, their ability to defend agency networks would be improved with changes to organizational structures and the adoption of a risk-management culture.



Federal Chief Information Security Officers (CISO)s are making headway in the battle for cybersecurity, as protection from threats both internal and external becomes a top priority across agency leadership. However, while there are a number of data-center security technologies that CISOs feel are indispensible for their jobs, these executives also face organizational challenges and budgetary limits that keep them from achieving their goals. And because new attacks can spring up at any time, CISOs must constantly scan the threat horizon and be prepared to defend their organizations against the unknown.

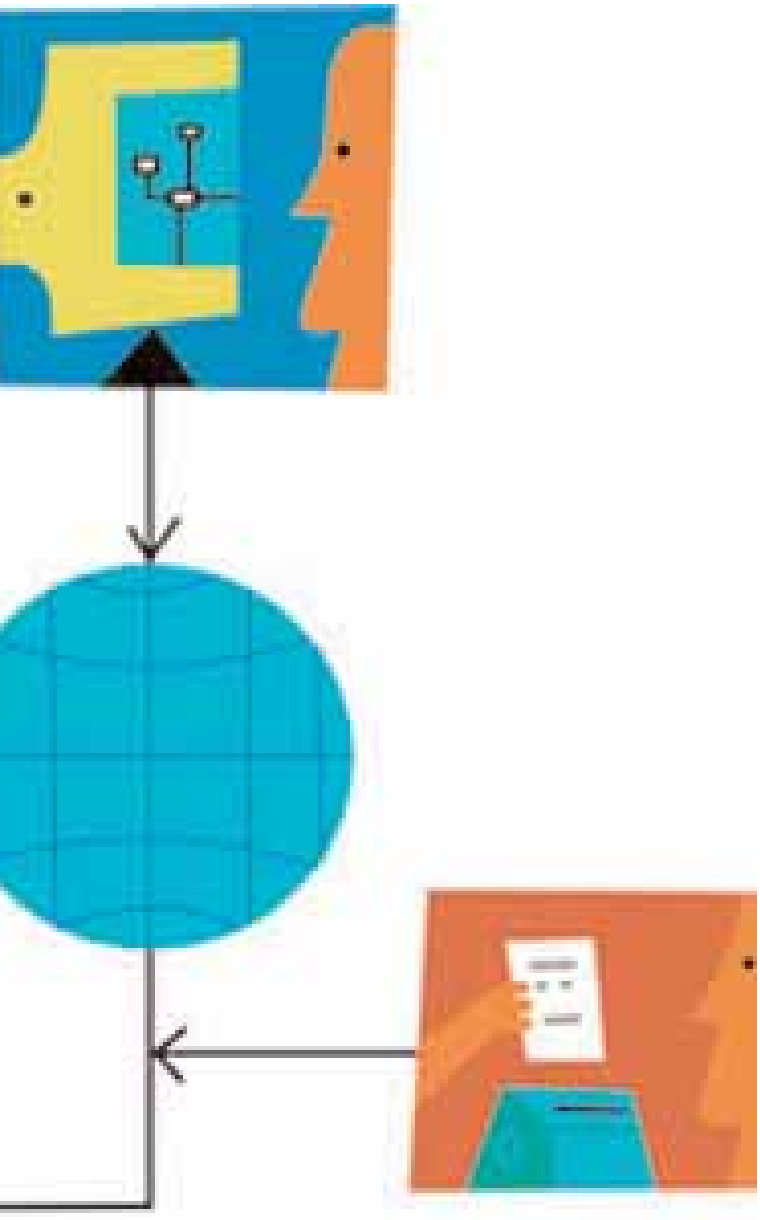
The CISO Perspective

To get a sense for how federal agency CISOs are coping with threats and other security issues, the International Information Systems Security Certification Consortium Inc. (ISC)^2, Government Futures, and Cisco conducted a study in 2009 of forty federal agency and bureau-level CISOs. Called The State of Cybersecurity from the Federal CISO's Perspective, the report summarizes how CISOs feel they are faring in the battle for cybersecurity, and makes some recommendations for improvement.

In general, survey respondents said they are feeling "empowered," since agency management is paying more attention to cybersecurity than in the past.

"The CISOs' responses clearly demonstrate that cybersecurity is evolving in terms of management priority," said W. Hord Tipton, executive director of (ISC)^2. "Although CISOs are still facing organizational challenges, we view it as a positive sign that CISOs feel they are being listened to by senior management and that their recommendations are, for the most part, being considered and implemented."

Still, half of the respondents said while they are making progress to protect their agencies, they're still "not getting ahead of the attackers," according to the survey. The other half answered that they believe they are "turning the



corner" in the battle for cybersecurity.

When it comes to top concerns, 48 percent of federal CISOs said they are most worried by external threats, due to the potential for data loss and exploits. Tied for second place are insider threats and software vulnerabilities, at 26 percent each.

Top Five for Security

As concern over external threats increases, so does the dependency that CISOs place on technologies to help them protect their perimeters, safeguard sensitive information, and prevent unauthorized access to data and resources. According to the survey, CISOs highlighted the top five data-center technologies that are most useful in combating threats:

- Intrusion detection systems/intrusion prevention systems
- Authentication
- Encryption
- Better software
- Quality product testing

Despite the advances in security technology, there are internal issues that CISOs are grappling with in the fight to protect their networks. Improving agency governance is another priority among CISOs, which includes "…getting greater buy-in from agency leadership, eliminating security stove pipes, developing sound metrics, improving IT inventory, and implementing a risk management program," according to the survey. Compliance is another concern for respondents; in particular establishing better relations with the Inspector General in their agencies and achieving certification and accreditation goals, they said.

On the personnel front, CISOs said that retaining key security staff has been easier because of the economic crisis. As respondents look ahead to hiring in the future, they say they will look for candidates with the right experience, communications skills, professional certifications, and security clearances.

CISOs responding to the survey say there are a number of changes that federal agencies could make to how they approach cybersecurity. First, the emphasis should move from compliance reporting – which takes a snapshot of compliance levels at a certain point in time – to risk management and continuous monitoring for threats, since focusing on defending from attacks should take priority over proving compliance. The respondents also said that strict security requirements should be enforced whenever major IT systems are acquired by an agency. ❑

Maximizing Technology ROI

With help from private sector leaders, the Obama Administration has outlined five best practices designed to increase the impact that technology has on federal organizations while keeping costs in check.

In January, President Obama hosted a series of forums at that White House under the heading `Modernizing Government,' where private sector leaders were invited to offer their opinions and suggested best practices to help federal agencies cut costs while improving operational efficiencies and customer service. In one of those meetings, led by Jack Lew, Deputy Secretary for the Department of State, private-sector leaders shared their ideas for how federal government agencies can prioritize technology investments and manage IT budgets to deliver results.

An Agency Perspective

At the start of the meeting, Lew explained to the private-sector leaders some of the challenges that federal agency managers face.

"From an agency perspective, you're focused on getting your work done," he told the group. "You look at a world that doesn't lend itself easily to strategic planning, particularly in an area like IT where decisions are made based on what you know today. And the systems we have, they're probably not implemented for the better part of two years because the funding doesn't come along right away."

Lew added that federal agencies need advice regarding not only how to launch new IT projects, but also how to revamp projects that aren't meeting their defined goals. "How do we get to the point where our strategy drives our systems, as opposed to our systems determining our strategy?" he asked.

Federal Chief Information Officer Vivek Kundra, who also participated in the forum, asked the group to offer their expertise to help federal agencies manage the more than $76 billion worth of information technology projects currently underway in the federal government.

"We'd love to engage in a discussion [about] … what could the government do, and learning from you how you've managed really complex IT projects … and producing the dividends that were promised up front, which seems to be one of the problems in the government," he said.

Defining Best Practices

With input from the private-sector leaders, the group came up with the following five best practices:

1. Demonstrate Need Before Investment: Before purchasing new products and services, agencies should be able to outline a clear purpose for the new technology and show that it aligns with end-user needs;

2. "Right-size" IT Projects for Results: The longest timelines that agencies should develop for their technology projects is twelve to eighteen months. If a project takes longer than that to implement, the return on investment decreases and the products and services chosen run the risk of becoming obsolete. Large-scale projects should be broken into smaller chunks with discreet goals and timelines;

3. Deliver Customer Benefits at Each Project Milestone: In addition to keeping timelines in check, agencies should set well-defined and periodic milestones for each project, and demonstrable customer benefits must be achieved within a year. If it's not clear that the customer benefits can be demonstrated within this timeframe, the agency shouldn't go forward with the project;

4. Minimize Software Customization: Whenever possible, federal agencies should use off-the-shelf software to save on the expense and complexity of writing custom applications;

5. Standardize IT Across the Enterprise: Federal IT managers should work toward standardizing technology across the organization, particularly software and data center infrastructures. Standardization can be hard to achieve, since department-level managers are often interested in technology that suits their teams, so this mandate must come from agency leadership. ❑

Reap the Benefits of Virtual Desktop Infrastructure

Virtualization has had a dramatic effect on the data center, providing cost savings by maximizing hardware purchases and reducing power consumption. Virtual Desktop Infrastructure (VDI) makes it possible to achieve the same savings while managing your PCs. VDI offers:

- Centralized management of all your desktops with easy updates and instant provisioning
- Enhanced security with the ability to lock down images and protect data
- Power savings with thin client VDI
- Near-zero downtime caused by hardware failure

Ready to implement a VDI solution? GovConnection can help with assessments, planning, installation, and ongoing support.

HP LeftHand P4300 4.8TB SAS Starter SAN Solution

- Easy to deploy, scale, and maintain
- Includes (16) 300GB SAS hard drives
- Consolidate multiple storage nodes with Storage Clustering

Smart Buy HP t5730w Thin Client

- AMD Sempron™ 1GHz Processor
- Centralized management and no moving parts means fewer help desk calls, less down time, and greater efficiency

VMware vSphere 4™ Enterprise Plus

Transform your data center into an ultra-efficient cloud computing environment with automated services and uncompromising control.

HP 4GB Virtual Fibre Channel Module

- Simplify SAN fabrics with fewer cables and switches
- Change servers in minutes, not days

Call today to see if you are eligible for special contract pricing or special government and education pricing.

1·800·800·0019
www.govconnection.com

gov is all you need™

GovConnection®
A PC CONNECTION COMPANY