FCW

THE BUSINESS OF FEDERAL TECHNOLOGY

WHAT YOU REALLY NEED TO KNOW ABOUT TECH

From agency heads to acquisition officers — the expertise that's *really* required to make federal IT run

CDW·G CATALOG INSIDE

1105 MEDIA

Trending

OPM: CDM will offer baseline security

The latest analysis of the Office of Personnel Management data breaches comes from OPM itself and involves one of the government's most highly touted cybersecurity programs: Continuous Diagnostics and Mitigation.

When all the security tools enabled by the CDM program are in place, "the government can really have a point at which we can say, 'Yes, we have a firm understanding.... Everybody's now on the same page, reporting the exact same thing,'" Jeff Wagner, OPM's director of security operations, told reporters in August.

The multiphase CDM program offers a system of dashboards that give network managers a clearer view of vulnerabilities. CDM's backers say the program does not thwart big breaches of federal networks but instead is a tool for discovering them.

A series of breaches of OPM databases exposed the information of millions of current and former federal employees, and FCW asked Wagner whether the breaches could have been prevented if all the CDM security tools had been in place. He said access control was a key to the attack because the hackers were able to take advantage of a contractor's credentials, and after all the CDM tools are deployed, government officials can outline additional measures for addressing access control.

The CDM program, whose acquisition vehicle has a $6 billion ceiling, is divided into three phases. The first has given agencies tools to determine what devices are on their networks. The second and current phase focuses on doing a better job of identifying who is on those networks, and security products for identity management and network boundary protection are in the offing. The third phase will delve further into boundary protection and tackle incident response.

The catastrophic breaches of OPM — for which Director of National Intelligence James Clapper has named China as the leading suspect — triggered a maelstrom of outrage on Capitol Hill, including questions about what additional tools federal IT managers need to combat unrelenting threats.

Jim Quinn, lead system engineer for the CDM program at the Department of Homeland Security, told reporters that officials are considering accelerating the program's timeline and potentially issuing task orders for Phase 3 next year. He said, however, that it would be unwise to rush deployment.

Wagner praised officials at DHS and the General Services Administration for trying to speed up CDM's deployment while saying the program can only go so fast.

"Congress and everybody like to say: 'Didn't you do more?'" he said. "How much more can I do? It's one of those things in which [you ask], 'How fast can I go that doesn't get me an [inspector general] flash audit?'"

— *Sean Lyngaas*

> When CDM is in place, "the government can really have a point at which we can say, 'Everybody's now on the same page, reporting the exact same thing.'"
>
> — JEFF WAGNER, OFFICE OF PERSONNEL MANAGEMENT

FCW CALENDAR

9/23 **Defense IT**
David DeVries, DOD's deputy CIO, and DISA Director Lt. Gen. Alan Lynn are among the speakers at Defense Systems' discussion of DOD's Joint Information Environment. Arlington, Va.
http://defensesystems.com/JIE

9/20-25 **Analytics**
Netflix's Kurt Brown is among the big-data experts speaking at TDWI San Diego, which features six days of training on the specific technologies and high-level strategies for managing, modeling and visualizing big data. San Diego.
http://is.gd/FCW_TDWI

9/24 **Customer experience**
ACT-IAC is hosting a half-day summit on "The CX Journey: Understanding Customers and Engaging Employees" to explore best practices, tactics and tools for better CX design. Washington, D.C.
http://is.gd/FCW_cx

Contents

26

MANAGEMENT

16 What you really need to know

Agency heads, acquisition officers and even CIOs don't need to be hard-core techies. Here's the expertise that's really required to make federal IT run.

PROFILE

26 Can Phaedra Chrousos move the needle at GSA?

With a focus on entrepreneurship and customer service, the agency's first chief customer officer is applying private-sector solutions to the sometimes rigid federal bureaucracy

BY BIANCA SPINOSA

The Time is Right to Move to a Hyperconverged Infrastructure

Lowering costs, simplifying IT, better security, improved service and efficiency—federal agencies have been dealing with challenges like these for more than a decade. During that time, they've done their best to meet those challenges.

First, they began virtualizing parts of the datacenter—servers, storage and networking. Virtualization was a valuable step. It introduced much-needed automation into the datacenter, simplified management, and served as an on-ramp for cloud computing. It made the infrastructure more agile and scalable, and automated security and policy management.

However, virtualization isn't enough these days. The federal government continues to ask more of its IT resources. The President's 2016 budget proposal, for example, focuses on improving service delivery and performance. Other mandates require security improvements, increased shared services and collaboration, greater use of the cloud, and even more cost-cutting.

All these requirements mean existing infrastructure needs an overhaul. According to a recent study conducted by Accenture and the Government Business Council, most government leaders believe the current speed of their IT services won't let them achieve their agencies' missions. About half said their infrastructure doesn't provide them with the IT services they need to do their jobs. Other goals for agency IT leaders include implementing data analytics, reducing power and cooling, consolidating applications and data, accelerating IT deployment and reducing risk.

Agencies can solve many of these issues by finding a way to break down traditional datacenter silos. Many also have taken steps by implementing a converged infrastructure, where all the parts—servers, storage, networking—are preconfigured and ready to use.

There are many benefits to convergence, including lower costs, simplified management and greater scalability. Since the systems come preconfigured, though, they can't be customized. Others are moving toward the Software-Defined Data Center (SDDC)—the software version of convergence, where compute, storage, networking and virtualization software are integrated and completely managed via software.

82 PERCENT OF INSTITUTIONS ARE LIKELY TO ADOPT HYPER-CONVERGED INFRASTRUCTURE. —451 RESEARCH

The next step is moving toward a hyperconverged infrastructure, which combines the best of convergence and the SDDC by combining a variety of resources into a single, scalable pool, complete with built-in management tools. Depending on the vendor, these resources might include storage, compute, data protection, networking, a hypervisor, and grid software intelligent enough to auto-discover and add additional nodes to a cluster as needed. With a hyperconverged infrastructure, agencies can scale whatever resource is needed on demand. It's also highly automated, so it's simple to provision and manage, even across datacenters.

WHEN A HYPERCONVERGED INFRASTRUCTURE MAKES SENSE

Whether your agency is looking for efficiency, cost savings or simplicity, a hyperconverged infrastructure can deliver. There are some cases where hyperconvergence truly shines, including:

■ **Efficient VDI deployment:** Hyper-convergence reduces costs and eliminates the inflexible resource provisioning and fragmented infrastructure management that can make VDI deployment complex.

■ **Flexibility:** Run multiple enterprise applications on a single platform with predictable and fast performance in much less space, without performance bottlenecks.

■ **Improved test and development environment:** With direct access to high-performance environments and datasets, IT and software developers can set up complete test environments in minutes and cut QA cycles by as much as half.

■ **Effective remote and branch office management:** By consolidating branch office servers and storage onto a hyperconverged platform, agencies can more easily manage all sites.

■ **Backup and management:** Better backup and disaster recovery through local, remote and cloud-based backups, synchronous and asynchronous replication-based disaster recovery and centralized management.

■ **An easy path to the cloud:** Agencies can deploy secure private clouds quickly and scale on demand.

CONVERGENCE VS. HYPERCONVERGENCE: WHAT'S THE DIFFERENCE?

If you're confused about the difference between converged and hyperconverged infrastructure, you're not alone. While the terms can be confusing, there's a simple way to understand the difference by comparing what each brings to the datacenter.

GameChanger

GAME CHANGING TECHNOLOGY TO MEET AGENCY MISSIONS

In a nutshell, the converged infrastructure is a more hardware-focused approach to simplifying the datacenter. All components—storage, compute and networking—are fully integrated, but able to be separated and work independently.

The hyperconverged infrastructure is a software-defined approach to the datacenter. The components more fully integrated. There also tend to be more components—besides the classic compute, storage and networking. The infrastructure may include components like WAN optimization, data compression and storage virtualization. Performance and management functions like caching, pooling and capacity optimization are built-in. The chart below clearly explains the differences.

"HYPERCONVERGED SYSTEMS WILL BECOME THE NEW STANDARD FOR INFRASTRUCTURE-AS-A-SERVICE DEPLOYMENTS"
—REPORT FROM FORRESTER RESEARCH, MARCH, 2015

CLOUD MADE EASY WITH HYPERCONVERGED INFRASTRUCTURE

The Cloud First mandate has made it clear federal agencies must move at least some of their workloads to the cloud. In some cases, it can be difficult to make that leap. It means figuring out what technology to use, how it will integrate with the rest of the IT infrastructure, and how to create the most efficient and safe cloud scenario. It's even more difficult when the applications and data involved are sensitive and require a secure private cloud environment.

A hyperconverged infrastructure reduces or eliminates many of those challenges. Because a hyperconverged infrastructure contains everything necessary to stand up a cloud, it's easy to deploy a secure private cloud in just a few hours. It's also simpler to start small and scale to hundreds of nodes or more and back again as needed. It simplifies connecting to public cloud providers like Microsoft Azure or Amazon S3.

For private clouds, some vendors now offer "cloud-in-a-box" solutions to help IT organizations stand up private clouds quickly. These solutions include all the requisite compute, storage and networking tools, as well as a management console. This console lets agencies fully control where data resides and who has access to specific data sets.

Because hyperconverged infrastructures support both public and private clouds, they can be a particularly useful in cases where some applications and data must remain on-premises. Other agencies can take advantage of the public cloud. That's the situation with most agencies. IDC Government reports the federal government will spend as much as $3.4 billion next year on cloud solutions. A healthy portion of that will be spent on hybrid cloud solutions.

	CONVERGED	HYPERCONVERGED
Approach	Hardware-based	Software defined
Components	■ Networking ■ Compute ■ Storage ■ Server virtualization ■ IT infrastructure management software	■ Networking ■ Compute ■ Storage ■ Expanded IT infrastructure mgmt. ■ Server hypervisor
Additional capabilities		■ WAN optimization ■ Storage controller attached to each VM at the hypervisor layer ■ Data deduplication and/or snapshots ■ Built-in virtualization ■ Caching ■ Inline compression ■ Capacity optimization ■ Auto-tiering ■ Primary storage data deduplication
Benefits	■ Prebuilt and supported as a single entity ■ Components can be decoupled if necessary ■ Can be expanded by adding additional building blocks	■ Full visibility and manageability at the VM level ■ Allows for resource pooling and sharing ■ Tighter integration of components through software ■ Policy-based protection and resource allocation at the VM level ■ Greater scalability and resilience ■ Can be customized

GameChanger

GAME CHANGING TECHNOLOGY TO MEET AGENCY MISSIONS

Solidify Datacenter Security

The hyperconverged infrastructure can help federal agencies simplify the process of securing their datacenters.

Shutterstock.com

The federal government remains a compelling target for hackers across the globe. This is clearly evidenced by numerous recent high-profile breaches and many more attacks that are either unsuccessful or not headline-worthy. In the face of these persistent threats, there are still a variety of steps agencies can take to improve their security posture and reduce risks. As everyone knows, there's no silver bullet in IT security. It's a recipe. And each ingredient must play its part for the end result to be successful.

World class datacenter security combines perimeter security, secure applications and infrastructure, and security in the architectural design. Security measures added on after the fact, after these things are built, developed, or architected is more vulnerable. It's simply not native to the infrastructure. For this reason, hyperconverged infrastructure has emerged as a strong bulwark against the persistent threats to the federal government's IT infrastructure.

THE HYPERCONVERGED SOLUTION

Hyperconverged infrastructure is disrupting legacy practices of maintaining compute, storage and storage network infrastructure as three separate tiers. That has always meant three separate tiers to procure, install, configure, manage and secure. Instead of hardening each individual data center component, a hyperconverged infrastructure delivers all of this in one integrated package—a single tier.

Besides the obvious benefits of procuring, housing and refreshing less physical hardware, this creates considerable architectural advantage for those securing federal datacenters. Smaller infrastructure means a smaller attack profile. There are also fewer and more narrow points of access and egress.

While hyperconverged infrastructure provides an inherently higher level of security than legacy datacenter infrastructure, federal agencies must require solutions to meet all basic security standards before committing to an investment. Some agencies assign their most skilled IT engineers to manually secure infrastructure and applications.

However, most datacenters don't have that level of in-house expertise. The result is often a mix of systems that only partially meet security requirements. There may be others where IT staff has to disable certain functions to meet security requirements. When that happens, it becomes the agency's problem to find ways to secure those applications or appliances in ways to meet agency and federal requirements.

That's the wrong equation for today's environment.

"Vendors can't expect their customers to know more about how to secure their products than they do," says Eric Hammersly, security architect at Nutanix, a next-generation datacenter infrastructure company. "Vendors need to start owning the responsibility by building applications and products with security in mind from the ground up, and protecting them on an ongoing basis from open vulnerabilities and zero-day threats that can emerge."

For the most effective protection, choose a solution that secures data at rest through high-level encryption, and one that protects data from unauthorized access when the drives are off-line. The hyperconverged infrastructure solution also should enforce strong two-factor authentication to protect against unauthorized access.

Basic security standards should be built into the solution itself, such as

GameChanger

GAME CHANGING TECHNOLOGY TO MEET AGENCY MISSIONS

PCI DSS, SOX, FIPS 140-2, Common Criteria and Suite B. The solution should provide security-driven analytics, with which security analysts can assess and prevent many infrastructure-related risks. Finally, the infrastructure should be self-healing. It should enable workloads to continue functioning uninterrupted even if some are found to be compromised.

SECURITY IS EVERYONE'S BUSINESS

The burden of securing our nation's IT infrastructure is and must be shared. However, complex infrastructure legacy models place too much of the burden on agency IT teams. They're often forced to cobble together a security position around many different moving parts.

When planning any IT investment, agencies must ensure the system not only satisfies basic criteria of each standard, but is certified up to the level required by the agency or department, such as Suite B Top Secret or FIPS 140-2 Level 2. Furthermore, choose application and infrastructure vendors that are responsibly hardening their own code and can prove they have done so. This puts a fair burden of security on the vendors instead of agency IT resources.

"All vendors should be hardening their own code, and they should publish and fully support their [security] baselines," said Simon Mijolovic, senior security solutions architect at Nutanix. "Solutions should come with thorough documentation that shows how the product was hardened and gives you confidence that the vendor is also supporting that baseline."

Datacenter managers should also expect vendors to quickly react to identified vulnerabilities. That means vendors must take responsibility for identifying and patching vulnerabilities faster than ever. That's more

complicated than it might seem.

It's simpler if an application or product is fully COTS. More often than not though, datacenter applications and appliances are likely a product of several inputs—vendor-written code, open source code, and components from other sources. That

THE BURDEN OF SECURING OUR NATION'S IT INFRASTRUCTURE IS AND MUST BE SHARED.

opens the datacenter to a greater extent of vulnerability from different attack vectors.

Combatting this type of complexity requires a vendor that owns the problem—one that is committed to continually monitor the landscape and develop faster testing and remediation processes.

THE RIGHT INFRASTRUCTURE FOR THE JOB

Nutanix, a leader in the hyperconverged infrastructure market, has designed its solutions with security as a primary focus. Besides the inherent security of its hyperconverged infrastructure offering, Nutanix builds additional security measures into every step of the development process. For example, Nutanix developed its own Security Technical Implementation Guide that incorporates DoD STIG guidelines. These empower enterprise security teams to drastically reduce the time it takes to test code and can reduce the DIACAP/DIARMF accreditation process to less than an hour.

To meet the high-level security requirements of federal agencies, Nutanix platforms comply with FIPS 140-2 Level, NSA Suite B support (to Top Secret), Common Criteria EAL2+

and NIST SP800-131A, among others.

Nutanix' hyperconverged infrastructure encrypts user and application data to a level of FIPS 140-2 Level 2 compliance. It lets security staff lock down access to clusters if a security breach is suspected or if threat levels rise. The solution employs strong

two-factor authentication, including the use of client certificates, to prevent unauthorized administrator log-ins. It also provides data at rest encryption through self-encrypting drives, and meets the data-at-rest encryption requirements for HIPAA, PCI DSS and SOX standards.

Finally, Nutanix' hyperconverged infrastructure solutions provide agencies with security-driven analytics with which security staff can assess and mitigate a range of infrastructure security risks. The system continuously checks the health of virtual machines, nodes and disks in the cluster, and flags any potential issues. It also performs root cause analysis of flagged issues by visually navigating, grouping and filtering resources at the VM, host and disk levels. These capabilities help security staff proactively resolve issues before they become bigger issues.

15,019 .gov and .mil email addresses were on the list of Ashley Madison customers that hackers posted in August

WHAT: "Creating a Balanced Portfolio of Information Technology Metrics," an IBM Center for the Business of Government report by Kevin C. Desouza of Arizona State University

WHY: Real-time data is helping government decision-makers meet their agencies' IT needs, but CIOs would benefit from more effective use of performance metrics, according to the report.

Desouza interviewed 27 federal, state and local government CIOs and concluded that a balanced portfolio of metrics could help agencies track the progress of IT initiatives. Although that approach takes time and money, Desouza said that without such measurements, the conversation in the public sector will usually focus on the times when things don't work.

The report found that CIOs are adept at managing metrics from outsourced IT projects, and they are interested in what other IT departments are doing and the reasoning behind their metrics.

VERBATIM: "We are more likely to hear about IT projects that have 'gone rogue' and failed to deliver on their promises. One possible cause for these problematic IT projects is that the [CIO] community has not done enough to invest in the creation of metrics that capture the performance of IT assets and their contribution to organizational performance."

FULL REPORT:
is.gd/FCW_ITmetrics

Out-of-sight CIO posts new job to LinkedIn

Barry West's unexplained absence from the Federal Deposit Insurance Corp. came to an end in August when he updated his LinkedIn page to reflect his new role as president of Mason Harriman Group.

He had been on leave from FDIC since early June and was out of sight for more than two months before his LinkedIn page was updated in mid-August with information on his new position at Mason Harriman Group, a firm that connects retired CXOs with government and industry.

It's unclear when exactly the update was made or whether West personally made it. He was still listed as CIO on FDIC's website on the morning of Aug. 17, but FDIC spokesperson Barbara Hagenbaugh confirmed that he had resigned effective Aug. 15.

Hagenbaugh has consistently declined to say whether West was on paid administrative leave, despite multiple Federal News Radio reports to that effect.

West has extensive experience in and out of government, having served as executive vice president at SE Solutions and CIO at the Pension Benefit Guaranty Corp., National Weather Service, Federal Emergency Management Agency and Commerce Department. He also served as president of the American Council for Technology from 2003 to 2007. He started at FDIC in December.

Hagenbaugh said Acting CIO Martin Henning, who was doing West's work during his absence, would continue to handle the job while a permanent replacement was sought.

Neither West nor Mason Harriman responded to requests for comment.

— *Zach Noble*

"I'M SORRY. WE'RE LOOKING FOR SOMEONE WITH CYBERSECURITY SKILLS."

IBM Hybrid Cloud:

If you have to choose between freedom and security, don't.

There's a new way to cloud. With the IBM hybrid cloud, more flexibility doesn't mean less control. You're free to mix and match public and private cloud environments to run the services and apps you need while maintaining security across all your systems. Learn more at ibm.com/madewithibm

Smarter clouds are made with IBM.

334,000 people were affected by the breach of the IRS' "Get Transcript" application — nearly three times the number originally thought

DOD sets up cyber workforce council

Deputy Defense Secretary Robert Work has set up an intra-department council to manage cyber workforce issues at the Defense Department.

In an Aug. 11 directive, he tasked the council with ensuring that the Pentagon takes a holistic, "total force management" perspective to filling the department's cyber workforce needs with civilian, military and contracting personnel. The goal is to avoid duplication and omissions in the cyber-related skillsets demanded by DOD officials.

The new council will include members of the offices of the DOD CIO, undersecretary of Defense for personnel and readiness, undersecretary of Defense for policy, undersecretary of Defense for intelligence and director of the National Security Agency.

The broadly worded directive also "unifies the overall cyberspace workforce and establishes specific workforce elements."

The updated policy is in keeping with Work's and other officials' emphasis on building a technically sound DOD cyber workforce of some 6,000 employees. The directive comes on the heels of a breach of the Joint Chiefs of Staff's unclassified email network by hackers allegedly linked to Russia.

The absence of decryption played a significant role in that hack, a former intelligence official familiar with the network told FCW. The Russian hackers believed to be behind the breach took advantage of encrypted traffic that the Joint Chiefs of Staff was not decrypting and inspecting, the official added.

— *Sean Lyngaas*

GSA @usgsa

Here's a perfect example of how we're improving customer service all the time. http://fcw.com/articles/2015/08/11/phaedra-chrousos-profile.aspx … @FCWnow

7:00 AM - 12 Aug 2015

FOIA Resource Center @foiaresource

Good PR does not equal legally adequate public service @usgsa @FCWnow @PSChrousos @jimgarrettson

11:06 AM - 12 Aug 2015

Phaedra Chrousos @PSChrousos

@foiaresource @usgsa @FCWnow @jimgarrettson Very true!

4:23 PM - 18 Aug 2015

Join the conversation

FCW uses Twitter to break news, field questions and ask our own.
Learn more at Twitter.com/FCWnow.

Who's Fed 100-worthy?

FCW will soon begin accepting nominations for the 2016 Federal 100 awards. And it's never too early to start thinking about who deserves the federal IT community's most prestigious recognition.

The Federal 100s, of course, spotlight individuals who are having an outsized impact on federal IT. Nominees can come from federal agencies, the private sector, academia or the nonprofit world.

Our judges weigh each nomination carefully and factor in the nominators and the story they tell. Ultimately, though, it boils down to the nominee's positive impact on federal IT, with special emphasis on these three elements:

• **This is an individual award.** Teams are important, too, but we're looking for the women and men who power that collaboration.

• **Winners go above and beyond, whatever their level or rank.** A fancy job title is not required, and doing one's job well is not enough.

• **Results matter.** Exceptional effort is necessary but not sufficient. There must be clear impact in the past 12 months.

So gather your information and supporting nominators, and be ready when nominations open in late October. Make sure we know about all the worthy women and men in federal IT.

— *Troy K. Schneider*
tschneider@fcw.com
@troyschneider

Commentary | DAVID WENNERGREN

DAVID WENNERGREN is senior vice president of technology at the Professional Services Council.

Ideas for the next president

It's not too early to start thinking about how to help the upcoming administration define its priorities for improving federal IT

Although it's still a year away, the next presidential election will be upon us before we know it. And with so many issues needing attention, a set of recommendations on a federal technology agenda would help the next administration hit the ground running.

It's important to see through the haze of heated rhetoric and focus on three questions:

1. What current initiatives should be continued? Too often, ongoing efforts from the prior administration languish or are discarded because they weren't invented here.

2. What current initiatives or policies should be terminated? The road of federal IT initiatives is paved with many well-intentioned efforts at portfolio management that never actually retire legacy systems. Similarly, practices that create drag on the rapid acquisition of effective IT solutions must be discarded.

3. What new initiatives and actions should be embraced? We need to bring speed, innovation and commercial best practices to government. We can no longer afford to function in an environment in which the platforms, apps and managed services available in the commercial marketplace are not the norm in the federal government.

There is no shortage of transition studies and reports in progress around town, and the Professional Services Council is in the midst of developing its own priorities for the executive and legislative branches to help set the course for the next four years.

Here are just a few ideas I'd like to throw into the mix:

• **Things to keep on the bus:** The Obama administration's push for the use of cloud computing is helping agencies move to consumption-based buying of IT solutions. Continued portfolio management efforts will be crucial to undertake

> Continued portfolio management efforts will be crucial to undertake IT modernization and retire legacy systems.

IT modernization and actually retire legacy systems that are no longer secure or cost-effective so that we can stop spending 75 percent of IT budgets on sustaining the old rather than creating the new. And far too many cybersecurity mandates are still works in progress that must be completed now.

• **Things to throw off the bus:** Current IT acquisition practices take too long and preclude adoption of best practices. The over-reliance on lowest price technically acceptable and underuse of statements of objectives, managed services and alternative proposals must be addressed. Also in my sights are point-in-time certifications and paperwork when continuous evaluation would deliver better results.

• **New activities to undertake:** We need to make IT acquisition reform a reality and demand more use of Federal Acquisition Regulation Part 12, managed services and performance-based contracting. We also need a national imperative on cybersecurity that addresses liability and information sharing. Agencies must complete current cybersecurity efforts such as personal identity verification cards, Trusted Internet Connections and Einstein, patching and encryption, and then move on to embrace new cybersecurity best practices and create a world of secure information sharing. DHS needs the authority to take action when agencies don't meet deadlines. And we must improve the ability of government to attract and retain a tech-savvy workforce.

In "The Wisdom of Crowds," James Surowiecki noted that "diversity, independence and decentralization…improve dramatically the way organizations make decisions and think about the future." So let your voice be heard. To offer your ideas, go to **www.pscouncil.org** and click on "Call for Initiatives for the Next Presidential Administration."

Together we can help the next administration encourage the government to partner with industry, rapidly adopt best practices, foster a culture of innovation and ensure that technology enables more effective mission results. ■

Commentary | KRIS VAN RIPER AND DYLAN MOSES

KRIS VAN RIPER is the government practice leader and **DYLAN MOSES** is a research analyst at CEB.
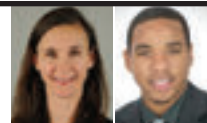
Roadmapping: A key tool for FITARA compliance

A technology roadmap can help agencies reap the benefits FITARA has to offer. Here are the four stages of a successful effort.

The Federal Information Technology Acquisition Reform Act requires that federal CIOs reorganize their IT departments so that those leaders will be accountable and responsible for all IT-related decisions made across their agencies. Although the changes remain a concern for many, FITARA provides government CIOs with the opportunity to develop a clearer picture of their IT portfolios.

If taken as an opportunity, the law could be a catalyst for more effective IT investing and portfolio management by consolidating duplicative systems, retiring legacy assets and ultimately driving federal agencies into a new era of IT efficiency.

To truly capture the benefits that the new law brings, CIOs must have visibility into current assets and must plan for technology changes that signal new investment needs and divestiture requirements. To support those collective objectives, the most successful organizations are using roadmaps to identify the current state, drive fact-based decisions and convey execution plans.

Roadmaps can also help agencies comply with the Office of Management and Budget's mandates for FITARA — in particular, the creation and disclosure of a strategic plan to ensure compliance (which was due Aug. 15) and a strategy for implementing that plan (due Dec. 31). All reporting agencies and their components should have submitted an assessment and an implementation plan by now.

CEB research has found that although roadmaps have the potential to be highly effective communication tools, 70 percent of IT executives are dissatisfied with their organization's current efforts. Respondents cite poor visualization, data quality and cross-silo collaboration as challenges to creating effective roadmaps.

Many organizations struggle to strike the right balance between comprehensiveness and maintenance, and leading organizations

> Federal IT leaders can navigate the complexity of their portfolios better with a concerted roadmapping effort.

use longer time horizons judiciously because they understand that overinvesting in detailed, long-term roadmaps might be a wasted effort in light of the pace of change.

Our work with hundreds of teams in developing roadmaps has revealed four critical stages for establishing a successful roadmapping program:

1. Properly scope roadmap objectives. Roadmaps that are developed without clear priorities and goals in mind will often fail to deliver value quickly enough to the IT portfolio. Instead, leading organizations determine the desired outcomes and identify relevant stakeholders before creating roadmaps.

2. Coordinate roadmap development. Poor or uncoordinated processes result in inefficiencies, bad data and slower time to benefit in roadmap creation. Federal IT organizations can ensure an efficient development process by setting standards for quality measurements, roadmapping processes and segmenting roadmap ownership.

3. Maintain and update roadmaps. Even the best-planned roadmaps face challenges such as changes in business priorities, advancements in technology and inefficient performance management techniques. Leading organizations avoid those problems by anticipating new demands and monitoring the roadmap's status.

4. Share roadmaps with stakeholders. One common mistake is presenting a roadmap without context for the greater organization, thus losing stakeholder buy-in. Federal IT organizations should make artifacts available to different audiences to ensure stakeholder adoption and use.

FITARA's implementation will require focus and rigor, but federal IT leaders can navigate the complexity of their portfolios better with a concerted roadmapping effort. Even if your organization is not subject to FITARA, investing in better roadmaps is an opportunity to improve IT governance and decision-making. ■

SCOTT FRENCH is vice president of government at Panasonic System Communications Co. of North America.

How will FITARA affect government mobility?

The new law empowers CIOs to fully integrate mobile technology into the federal workplace — and transform employee productivity

Earlier this year, a group of federal CIOs met with their counterparts from several of the country's largest corporations, including Coca-Cola and Exxon Mobil. The purpose of the meeting hit close to home for both sets of attendees: how to manage IT investments and how to measure and communicate the important role those investments play in improving organizations' efficiency.

It's exciting to see this collaboration and knowledge sharing between the public and private sectors, especially against the backdrop of ongoing efforts to implement the Federal IT Acquisition Reform Act. As one of the most far-reaching federal IT reforms in decades, the law increases the authority and responsibility of agency CIOs in transforming the way the government acquires and uses IT resources.

By expanding the roles of agency-level CIOs in IT decision-making, FITARA empowers them to ensure that technology investments are cost-effective and provide value toward achieving organizational missions and goals.

One topic that almost certainly came up during the public/private CIO discussions was mobility. In the business world, mobile devices have become standard tools for improving employees' productivity and efficiency. Yet adoption in government has traditionally been slower, in part because of the acquisition and management challenges that FITARA seeks to address. For government mobility, FITARA might prove to be the watershed moment we've been waiting for.

One of the most fascinating aspects of FITARA is the theory behind it. Streamlining IT investments to eliminate financial waste and increase productivity is a long-standing goal in government. But it

---

> CIOs are ready to manage the change necessary to bring the government fully into the cloud-first, mobile-first, data-driven era.

---

might be the first time that elected leaders have chosen to address it by empowering the people who are closest to the problem and understand it best.

Agency CIOs know exactly what needs to happen in their organizations and are ready to manage the change necessary to bring the government fully into the cloud-first, mobile-first, data-driven era. As they settle into their newly enhanced roles, mobility is surely at or near the top of those CIOs' to-do lists.

Mobile technology has been shown to significantly improve productivity and enable time and cost savings in a broad range of industries because it allows employees to complete more work from the field and make better decisions through access to real-time data and constant communication.

AOL Government's research has shown that federal managers expect the same benefits. About half of those surveyed said government employees could redeploy at least 7 hours per week toward more productive work if fully enabled for mobility, and 19 percent said they could redeploy more than 12 hours per week. That's an astounding 30 percent productivity increase in the traditional workweek.

Although the benefits of increased mobility are clear, large-scale deployments of new technology in the federal government have been slow. And they have often happened in the form of piecemeal rollouts of new devices as add-ons to the current IT landscape. Instead, mobile technology should be deployed strategically and in a holistic fashion because it has the potential to disrupt old systems and workflows and revolutionize operations and organizations.

That type of transformational change is hard, but if anyone has the ability to make it happen, it's the CIO, especially with the new authority granted by FITARA.

We are only beginning to understand the impact the law will have on government operations. It's a safe bet, however, that agency CIOs will take advantage of their newly expanded roles to harness the power of mobility for their organizations, employees and the public. ■

WHAT YOU REALLY NEED TO KNOW

Agency heads, acquisition officers and even CIOs don't need to be hard-core techies. Here's the expertise that's really required to make federal IT run.

CIOs: 'A strategic partner, not a coder-in-chief'

BY ADAM MAZMANIAN

Government technology leaders are facing new demands from inside and outside their organizations. The rapid consumerization of technology is creating an appetite among the public for easy-to-use apps for accessing government services, and tech-savvy senior officials are increasingly interested in using new IT tools to deliver those services.

In addition, Congress has empowered agency-level CIOs to take more control of technology spending and hiring and to take a seat at the table with the top mission-delivery executives.

So what do CIOs have to know to do the job? Do they need to be able to assemble their own boxes and networks? Write code? Haggle for the best price for software and services? Be a cybersecurity wonk?

And how far down in the weeds does a CIO need to get? Is there such a thing as a CIO who knows too much about technology?

'Not a coder-in-chief'

"I don't think you should actually be coding as a CIO," David Bray told FCW. The youthful CIO of the Federal Communications Commission comes to technology management from a geekier background than most. He has worked as a programmer and a network engineer, and he tinkers with tech on his own time. He recently used the Android OS to design a peer-to-peer mesh network, with some success.

But for Bray, the real secret to being a successful CIO is merging an ability to engage in top-level strategy with an ability to let talented individuals excel at their jobs.

"The best leaders recognize that they have blind spots," he said. "They make themselves open to other people. It would be hubris to think you know everything. You'll never be able to keep up with it. The best thing that a CIO needs to bring in terms of talent and skills is really how to set a compelling vision and attract sufficient talent as well as recruit talent already on the team to achieve that vision."

Paul Brubaker, who as a Senate staffer helped draft the Clinger-Cohen Act that codified the agency CIO role, said a successful CIO needs to see the big picture when it comes to the organization's lines of business.

"The reason why CIOs haven't been invited to the top table is that they typically represent some narrow element of IT governance, which is seen as playing in the administrative weeds, not adding value to the mission," said Brubaker, who served as deputy CIO at the Defense Department and is now director of federal government business at AirWatch by VMware.

Some modicum of technical experience and ability is important, but not essential, he added.

"You're looking for a strategic partner, not a coder-in-chief," Brubaker said.

Focus on the user

Sonny Hashmi, former CIO at the General Services Administration and now managing director for government at cloud collaboration firm Box, sees an urgent need for a new breed of CIO.

"I think CIOs need to be a lot more tech savvy than they are," he said.

Because large organizations are bogged down in compliance-based tasks, thinking about how technology can drive the future of agencies is frequently farmed out to the growing ranks of chief data officers, chief technology officers, chief innovation officers or even expert cadres such as GSA's 18F (an organization Hashmi helped establish) or the U.S Digital Service.

"My view is [that] the CIO should be doing all of that strategic thinking," Hashmi said. "The reason these new roles emerge is not having the right top leadership."

Although CIO shops need to run networks, manage security and do other essential tasks, CIOs should find trusted partners among the senior staff to manage those tasks so that they can spend 80 percent of their time focusing on the larger strategic innovation challenges and educating senior mission staff on what IT can do, he said.

A CIO candidate who has years of experience running help desks, maintaining networks or managing security might not be "adding differentiated capability to the organization," Hashmi added.

He also emphasized the need to hire CIOs who know how to make the user experience a top priority. In the public and private sectors, "large organizations that run on legacy systems are UX-challenged," he said. In the private sector, "if your app is not easy to use, consumers will not use your service.... It's very simple."

More and more people are using technology to connect with government, which means the government is in the midst of transitioning to an environment in which data and technology don't just support services, they are the services. If those new services are going to be developed and launched successfully, CIO shops need leaders for whom the user experience is a core capability, Hashmi said.

Still room to get your hands dirty

As chief innovation officer at the Defense Intelligence Agency, Dan Doney is part of the growing ranks of C-level technology advisers who work alongside CIOs at agencies. When it comes to evaluating opportunities, Doney said, hands-on experience is a big plus, particularly with cloud-based technology.

"If you are a senior IT manager in the government and you have not actually used the cloud for yourself — you've not released an application into the cloud, you've not done development in the cloud — you're doing yourself a great disservice," Doney said at a recent event in Washington. "You need to experience it yourself so you have a gut sense of what cloud is capable of doing for you. Unfortunately, many of our senior leaders have not had that kind of experience, and it's impacting their confidence."

Ultimately, a CIO must wear many hats. Brubaker likened the role to the classic Renaissance person with a range of interests, talents and skills. And it's becoming more and more obvious that the ability to keep systems running is just the beginning. ■

Agency heads:
It takes more tech than you think

BY ZACH NOBLE

Do agency leaders need to know more about the inner workings of IT to do their jobs effectively and safeguard national secrets? For many experts, the answer is yes.

Tech is now "part of the fabric of everybody's lives," said Montana Williams, senior manager of ISACA's Cybersecurity Practices.

When the recent Office of Personnel Management breaches triggered a national debate about cybersecurity, National Review's Jim Geraghty lashed out at Katherine Archuleta, the OPM director who resigned in the wake
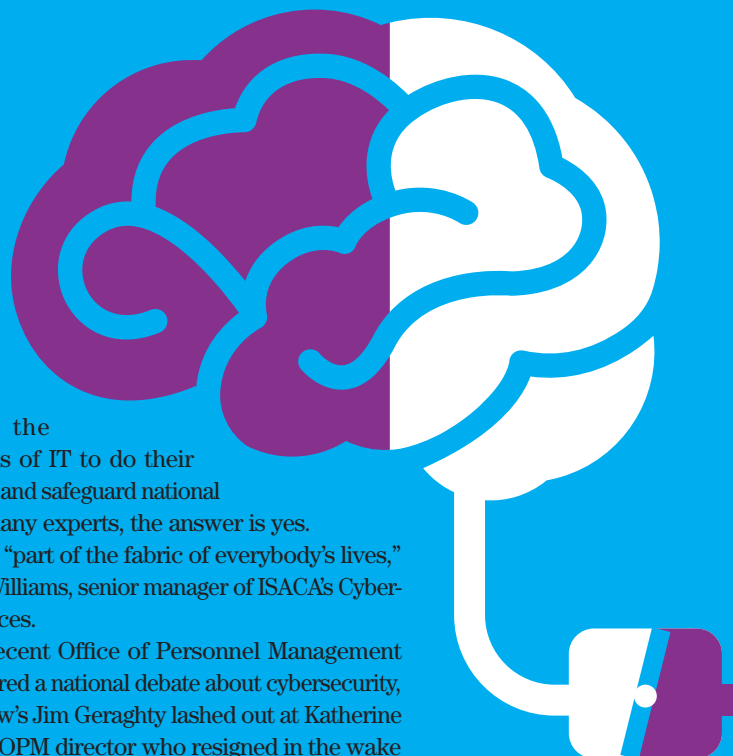
MOBILITY AND SECURITY: ON THE CUTTING EDGE

Every year, more federal employees use mobile devices to collaborate with coworkers, engage with citizens, collect and transmit data, and remain productive while out of the office. According to Mobile Work Exchange, 90 percent of government employees use mobile devices today, and that number is expected to rise even further over time.

While the benefits of mobility to federal agencies are clear, security issues are always a concern. Hacking and malware is a persistent worry, and for good reason. According to a mobile security study from the Government Accountability Office, the number of variants of malware aimed at mobile devices had risen by about 185 percent in the past year.

User behavior also can cause problems. A study by Ponemon Institute found that two-thirds of respondents from a variety of organizations have either frequently, or sometimes, downloaded and used mobile apps that aren't specifically approved by the organization, and only 19 percent

made sure the apps didn't have viruses or malware. A study by Mobile Work Exchange found that about one-third of government employees use public Wi-Fi connections, 25 percent don't set passwords, and six percent have lost or misplaced their mobile device.

Agencies have made great strides in securing mobility by implementing

HACKING AND MALWARE IS A PERSISTENT WORRY, AND FOR GOOD REASON.

technologies and policies around Mobile Device Management (MDM), Mobile Application Management (MAM), and Data Loss Prevention.

But it's simply not enough, though federal regulators are doing what they can. In 2013, the Federal CIO Council issued guidance to help agencies secure mobile devices. The Federal Mobile Security Baseline provides a minimum set of security controls for mobile devices, while the Mobile Security

Reference Architecture, developed by the Department of Homeland Security in collaboration with dozens of agencies, lays out the architectural components required to provide secure mobile services.

Achieving the highest level of mobile security requires even more stringent and specific standards and controls, and they

are on the way. For example, NIST has updated FIPS 201-2, a standard for Personal Identification Verification cards, to allow smart identity card holders to access secure computer networks from mobile devices. The technology goes hand-in-hand with NIST's SP 800-157 for Derived PIV Credentials, which allows users to use mobile devices for secure communications.

THE MOBILE SECURITY CONUNDRUM: BYOD EDITION

According to a recent report commissioned by the National Academy of Public Administration, nearly half of senior federal government employees are using their own personal mobile devices for business purposes. That's not surprising; the Bring Your Own Device (BYOD) movement is slowly but surely becoming part of the federal culture.

While the benefits of BYOD are well-known—they improve productivity and employee satisfaction—there is little doubt that allowing them in the workplace makes mobile security more complicated. Because personal and government data reside on the same device, the loss of a device is a significant security risk. And if employees download apps for personal use that are connected to malware or have viruses, they can affect government data.

Shutterstock.com

GameChanger
GAME CHANGING TECHNOLOGY TO MEET AGENCY MISSIONS

For most agencies, the benefits of BYOD outweigh the risks, providing that certain technologies and policies are implemented and enforced. At the very least, these should include encrypting data in transit and at rest, enforcing access controls that prevent unauthorized devices from accessing government data, enforcing authentication and password protocols, and developing a list of approved apps that employees can download without worry.

One of the best ways to do that is by implementing an approved MDM system, which helps organizations manage and push policies, applications and configurations, and keep track of devices, often by installing a software client on mobile devices. MDM allows agencies to do a "selective wipe"—removing only specific applications or data—in case the device is lost or compromised in any way. MAM is another important solution; it secures applications and data and provides access to apps for specific groups of users based on their needs or roles within the organization.

Other important steps agencies should take include using the newest firewall technology to block users' personal apps from accessing agency data; implementing Network Access Control solutions; and installing Security Information and Event Management systems, which enable IT staff to see security alerts generated by mobile threat detection solutions.

Finally, agencies should strongly consider adding mobile authentication solutions, which help validate the identification of users before they can access sensitive resources. With this solution installed, the device remains secure even if lost or stolen, because others who try to use it won't be able to access critical information.

FOCUSING YOUR MOBILE DEVICE POLICY ON SECURITY
There are many critical parts to an effective mobile device policy, and most of them are related to security in some way. To develop a comprehensive

policy, start by reading NIST publications 800-124 and 800-164.

Here are some important issues to address in mobile device policies:

USING A HARDWARE-BASED SECURITY TECHNIQUE CREATES A PROTECTED ENVIRONMENT FOR CRYPTOGRAPHIC FUNCTIONS THAT IS NEVER EXPOSED AND CAN'T BE HACKED.

Acceptable Use
- Acceptable agency use
- Acceptable personal use
- Prohibited activities
- Permitted access to agency resources
- Backup and file sharing/ synchronization rules
- Blacklisted applications

Data Application/Ownership
- Specify ownership of information and data
- Consequences of unauthorized use, duplication or access

Required Security Requirements
- Device provisioning and configuration, including installation of MDM client
- Password protection and policy
- Device locking policy
- Unacceptable device actions, such as jailbroken or "rooted" devices
- Employee access limits
- Conditions for remote wipe

THE CASE FOR HARDWARE-BASED MOBILE SECURITY
Software-based mobile security techniques encryption, antitheft and antivirus apps, and MDM software have been around for a long time, and they can be quite effective. But when agencies require the highest levels of security such as FIPS 140-2 Level 3 or higher,

or LOA 4—the OMB's highest level of e-assurance—software techniques can't measure up. That's because even though these techniques provide protection, they can be hacked or compromised, and in rare cases, turned off by users. In addition, the mobile operating itself can be vulnerable to attacks.

When top levels of authentication are required, experts recommend a hardware-based approach. Using a hardware-based security technique creates a protected environment for cryptographic functions that is never exposed and can't be hacked. A hardware-based secure element isolates credentials from potential attacks. Because it is self-contained, it can't be compromised.

The National Institute of Standards and Technology agrees. In its latest guidance, NIST urges government organizations to use hardware-based mobile security when the highest level of mobile security is called for. NIST said in its guidance that a software-derived credential could reach "high confidence" but not "very high confidence", according to the OMB identity assurance scale.

With an eye toward making progress in the field, Google recently introduced Vault, a hardware device in the form factor of a MicroSD card. This device, still in development, will encrypt sensitive data rest and allow end-to-end protection of streaming data. It runs its own secure operating system, near-field communications and antenna, and provides 4 GB of isolated storage for the most sensitive data.

GameChanger
GAME CHANGING TECHNOLOGY TO MEET AGENCY MISSIONS

Taking Mobile Secure Communications to the Next Level

When it comes to secure communications, the federal government's requirements are crystal clear—the vast majority of emails, documents, and other types of communication shared with others must be fully secure and encrypted.

For years, agencies have been doing what they can to comply. Notebooks and PCs are outfitted with PKI-based digital signing and encryption technology, letting them comply with the FIPS 140-2 standard for cryptographic modules. In some cases, agencies install VPN tokens on notebooks, which let employees access agency systems securely from remote locations. Agencies also have added readers for smartcards and Personal Identity Verification (PIV) cards to PCs and notebooks for physical access control.

While these methods work well for notebooks and PCs, they don't work well at all for mobile devices. That has become increasingly important; mobile device usage among federal employees has skyrocketed, and many of them are owned by the employees themselves. It is difficult enough to ensure that mobile devices comply with FIPS 140-2 Level 2, but companying with FIPS 140-2 Level 3 or Identity Level of Assurance (LOA) 4 requirements traditionally have been impossible.

There is no good way, for example, to integrate smart card readers for authentication into commercial mobile devices. NIST addressed this issue in recent guidance (SP 800-157), which promotes the idea of the derived PIV credential—an alternative token that can be deployed directly on mobile devices. In its guidance, NIST explains that derived PIV credentials requiring hardware-based secure elements are the best way to meet the challenge of securely authenticating mobile devices.

SECURE MICROSD

GO-Trust Technology is the first company to develop a microSD secure element—basically, an encrypted chip in a microSD form factor. SDencrypter, its flagship product, is a secure microSD with full in-chip hardware-based authentication and encryption/decryption.

SDencrypter and its component-only counterpart JetSmart are certified at FIPS 140-2 Level 3 for identity-based authentication, and they are the only secure microSD products that meet and exceed all technical and security requirements of NIST's SP SP800-157 guidance on derived PIV credentials raising the Identity Level of Assurance to LOA-4.

"This is especially beneficial to government agencies where a lot of employees use their own devices, because it provides a level of security that commercial products typically don't offer," said GO-Trust CEO Darren Lee.

Typically, an agency will purchase the microSD and install it on employees' mobile devices. That way, agencies have complete control over the security, and can deactivate the chip if necessary. The devices have proven to be an inexpensive and extremely effective way to ensure security up to a very high level.

There are many ways that agencies can use the technology to improve mobile security and comply with stringent security regulations. One government agency, for example, installed the microSD cards in some of its employees' mobile tablets, enabling them to digitally sign and encrypt email from whatever location they happened to be. Another agency wanted to replace some of its employees' notebooks with mobile phones while still letting them log into the agency's VPN server. The notebooks had been outfitted with VPN tokens for authorization, but there wasn't any easy way to do that with mobile phones. It accomplished the task by integrating GO-Trust's microSD card with the VPN client. Employees can now securely log into the VPN server just as they did with the notebooks.

There are many other uses for secure microSD cards throughout the federal government. For example, today's communication needs extend far beyond email to voice, chat and text. Building on its secure microSD technology, GO-Trust offers military-grade secure communications options for protecting all of these forms of communication. It works by encrypting encrypted peer-to-peer voice, chat and text communication, as well as enabling participants to share encrypted files with each other.

Over time, federal requirements for security will only become more stringent.

"I wouldn't be surprised if the federal government eventually required all mobile communication to be fully secure and encrypted," Lee said. "We're ready for that now."

of the breaches. He said her performance was part of "a troubling pattern of incompetent management from Obama appointees selected more for their political loyalty than for their expertise, skill or leadership abilities."

Geraghty highlighted Archuleta's lack of an IT or cybersecurity background and claimed she did not appear to have "any expertise in the vitally important human resources and record-keeping functions OPM is supposed to serve."

But she's no outlier. At the 24 agencies governed by the Chief Financial Officers Act, most agency heads have legal, political and/or public administration backgrounds.

There are a few exceptions: Secretary of Energy Ernest Moniz has a background in physics and has served on technology and security commissions; Secretary of Defense Ashton Carter has a background in technology, physics and security; and National Science Foundation Director France Córdova has had extensive scientific training.

In light of the OPM breach, should the old conventional wisdom — that a good leader knows how to lead people but not necessarily how to do those people's jobs — go out the window when it comes to cybersecurity?

It's still about people

At the end of the day, leadership and management skills are still the key.

"Surround yourself with the right people who have the right technical skills, and ask the right questions" was Williams' prescription for agency heads. "Be willing to hold people accountable." Leaders need to "understand [cybersecurity and IT] at the basic level," he added, but they don't need an extensive cybersecurity background. "Large hospitals are not run by doctors," he said by way of an analogy.

Patrick Malone, executive-in-residence at American University's Department of Public Administration and Policy, said, "I haven't ever seen any [federal employees] complain, 'Dammit, I wish my boss knew more about some Windows 10 update.' What people are crying about is their agency's culture."

According to Malone, feds say they need a culture of "compassion, trust, learning, collaboration and caring."

Good leadership might also be a key to attracting and retaining cybersecurity pros. Those skills are in short supply nationwide, and an approaching spike in the numbers of feds eligible for retirement threatens to widen the government's existing cybersecurity skills gap.

Some observers say one of the mistakes that undermined OPM was putting cybsersecurity in the hands of program office employees who did not have the relevant background.

"Soft skills" — though Malone said he is no fan of the dismissive connotations of that adjective — unlock "the real magic

"If you create the right environment, the tech skill will come."

PATRICK MALONE
AMERICAN UNIVERSITY

of leadership": attracting the right talent, encouraging them to give their best and retaining them.

"If you create the right environment, the tech skill will come," Malone said. "The only way we're going to get the technical talent — and the only way they'll stay — is if leaders make them want to stay. Otherwise, you're going to lose them to IBM, lose them to Apple."

Know the risks

Gregory Wilshusen, director of information security issues at the Government Accountability Office, said agency heads need to have a core understanding of what kinds of sensitive information their agency collects, how it's protected, the damage that would be done if the information is compromised, and who controls and interacts with the agency's systems in the cloud.

"Just because you start to migrate systems to the cloud doesn't mean you're absolved of responsibility," he said.

In the future, it shouldn't be a requirement that agency heads have deep IT knowledge. If they do, "that would be a bonus but not the determining factor," Wilshusen added.

So would OPM have done a better job of detecting and responding to the breaches if a tech-savvy leader had been in charge?

Williams said yes, adding that someone who understood the risks would have immediately cut off KeyPoint Government Solutions' system access when it became clear that the contractor had been hacked.

But Malone said the leader's role is to foster an open environment, not necessarily understand all the technology. In such an environment, an agency employee who had a solution to the problem would have felt comfortable bringing it up, he added.

Wilshusen said the public administrators and lawyers who currently lead agencies are probably capable of picking up the tech knowledge they need as they work, and they're likely doing so now.

"I would imagine there's a lot more on-the-job training after what happened to Secretary Archuleta," he said.

Catherine Lotrionte went further, however. "Even if you work at the Department of Agriculture, you need to understand securing data," said Lotrionte, who directs Georgetown University's Institute for Law, Science and Global Security. "You need to have a security-minded person running every single organization or at the top level, even if you have nothing to do with national security secrets."

"Unfortunately, most of these people do not," she added. "That's what they said — the OPM director didn't think of security. Are you nuts?" ■

Acquisition: Knowing enough to ask the right questions

BY SEAN LYNGAAS AND MARK ROCKWELL

The acquisition system — the means by which the federal government buys billions of dollars of IT goods and services annually — is a popular whipping boy for lawmakers, officials and analysts. It is characterized as a long, bureaucratic process that is further complicated by the 1,000-plus pages of the Federal Acquisition Regulation.

"The system is complicated, but you can definitely achieve success within that system," said Joe Jordan, former administrator of the Office of Federal Procurement Policy and now CEO of FedBid. As maze-like as the FAR might seem, he added, "the vast majority of what's in that book is just common sense."

Furthermore, one doesn't need to be an IT guru to become a federal program manager in charge of buying IT, Jordan said. An apprenticeship under an experienced supervisor and some IT training can suffice.

David Wennergren, who was assistant deputy chief management officer at the Defense Department from 2010 to 2013, said a program manager needs a baseline level of knowledge of commercial IT best practices to succeed. He added that he is concerned about the "dearth of new blood" in the IT government workforce. Half the contracting workforce has fewer than 10 years' experience, and a quarter has less than five years' experience, according to Wennergren, who is now senior vice president of technology at the Professional Services Council.

"So you have a contracting workforce that maybe hasn't built up the confidence to try all the flexibilities the acquisition rules allow," he said.

As encouraging as the General Services Administration's 18F and the White House's U.S. Digital Service are, there are nowhere near enough federal technology professionals for the government to do all of its IT development in-house, so IT-savvy acquisition experts will be essential, Wennergren added.

He and Jordan agreed, however, that contracting offices' risk aversion is a far greater impediment to success than a lack of IT know-how.

Asking the right questions

Federal contracting officers might not need to be able to moonlight as IT specialists, but they must
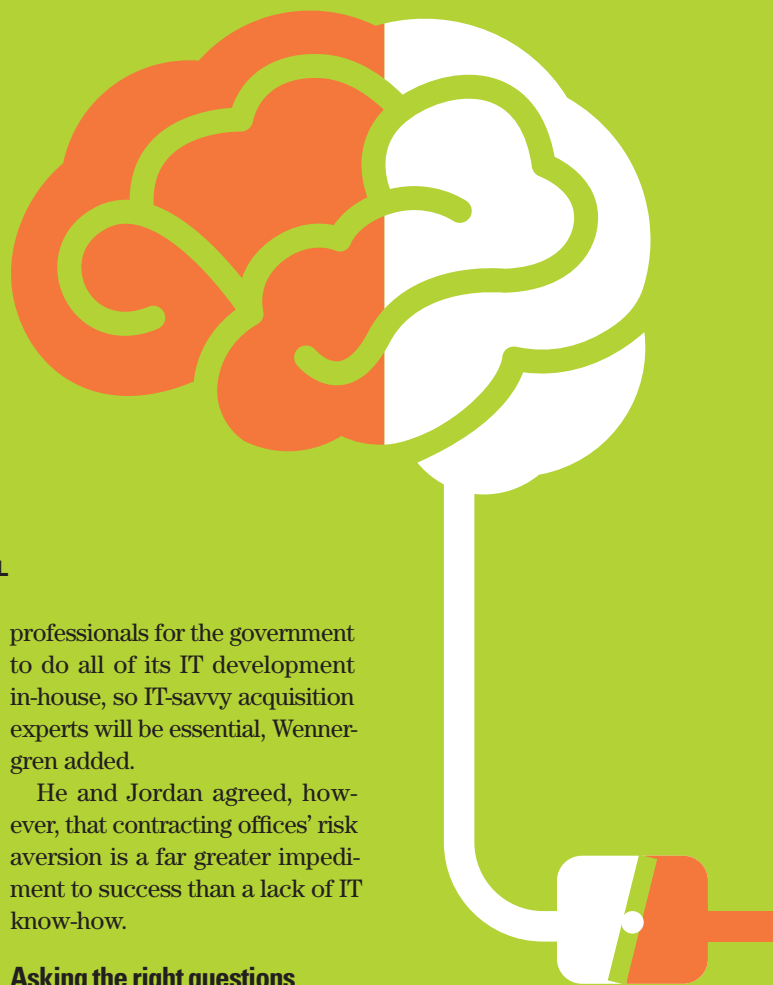

> "The system is complicated, but you can definitely achieve success within that system."
>
> JOE JORDAN, FEDBID

be able to ask federal contractors the right questions.

"With a federal IT budget that's worth $80 billion, there's no way" the government can get into the nitty-gritty details of all those IT system and service procurements, Wennergren said.

Furthermore, the government is struggling to keep up with galloping IT advances that progress so rapidly they can vex the companies that come up with them, and that pace isn't likely to let up.

Therefore, the government must find a way to adapt.

Wennergren said agencies should rely on contractors for product-level expertise, and federal contracting officers should focus on knowing how and whom to ask for effective IT solutions without going into technical specifications. "Too often, government organizations don't ask for the right things," he added.

The government has been injecting IT savvy into its acquisition and education processes — through the U.S. Digital Service's activities, 18F's blanket purchase agreement for agile services and OFPP's effort with the Federal Acquisition Institute to incorporate more IT-specific training into the Federal Acquisition Certification in Contracting.

Although he said he approved of most of those efforts, Wennergren added that they are not attempts to keep up with specific technologies and instead are intended to change the conversation about IT on a number of levels, including the ability of federal contracting officers to ask the right kinds of questions and think in a less rigid way about how to implement IT projects.

"The prize to be gained from 18F will be federal agencies that understand how to ask for" what they want in terms of end results rather than specific products and narrow specifications, he said.

Federal contractors, meanwhile, must develop a more holistic view of the IT environment at the agencies they hope to serve and have the technical knowledge necessary to understand how their products and services can address those needs.

Wennergren said cloud computing contracts offer a good example of how the technical nuts and bolts behind the managed service are mostly left up to the vendors while federal contracting officers focus on the business and management details.

"In most cases, the underlying technology solution is left in the hands of technical experts," he said. ■

Auditors and regulators: Time to hire more IT grunts?

BY ZACH NOBLE

Regulators and auditors have long been management analysts and accountants. But in a world where technology permeates everything — and presents new risks — should IT proficiency now be a priority for overseers?

It becomes a matter of asking: "Do the watchers have a flashlight that works?" NASA Inspector General Paul Martin said.

It turns out those flashlights can be few and far between. Inspectors with IT proficiency

are in short supply in both industry and government.

In the financial sector, for instance, four primary agencies are responsible for examining tens of thousands of institutions, as the Government Accountability Office detailed in a July report.

Although NBC News quoted Dmitri Alperovitch, co-founder of computer security company CrowdStrike, as saying that hackers could wreak "absolute havoc on the world's financial system for years" by altering electronic bank records, there are only a handful of IT-proficient regulators.

Among the findings in GAO's recent report:
• The Federal Deposit Insurance Corp. has 60 "premium IT examiners" to review more than 4,000 financial institutions.
• The Office of the Comptroller of the Currency has 100 IT specialist examiners to monitor 1,500 institutions.

fessional, how can you audit cybersecurity?"

Among the skills regulators and auditors should have is "detailed knowledge of the operating systems and the technology in operation" at the agencies or institutions they're monitoring, said Gregory Wilshusen, GAO's director of information security issues.

"They have to understand security policies and proce-

• The National Credit Union Administration has roughly 50 IT specialists for the 6,200 credit unions it monitors.
• The Federal Reserve System has some 85 IT examiners for the 5,500 institutions under its watch.

GAO auditors said a generalist examiner who has some IT training often reviews the cybersecurity situation at small and midsize banks, which means those institutions are receiving less-than-optimal analysis and advice.

A similar scarcity persists in IG offices. At NASA, Martin said, there are 80 auditors in the IG's office, but only five of them have IT expertise.

"They are very difficult to retain," Martin said of IT-proficient auditors. "We tend to poach from each other in the IG community."

The lack of expertise hinders thorough reviews. "I think every agency has no doubt dozens of IT audits or reviews that should be done" but aren't due to a lack of tech-savvy auditors, he added.

What auditors should know

Martin has criticized the checklist nature of Federal Information Security Management Act reports in the past, noting that FISMA "doesn't get down onto the ground" to deeply assess security.

"You don't want to have a bus driver be the flight examiner for a Boeing 747 pilot just because he can follow a checklist," said Montana Williams, senior manager of ISACA's Cybersecurity Practices. "If you're not a cybersecurity pro-

dures and how they are implemented, and they have to understand technical security controls to be able to judge, 'Are they implemented and operating as intended?'" he added.

Those skills can be difficult to pick up on the fly, which is why some experts advocate looking for people who have an IT background.

"I've found the best IT auditors are former IT grunts," notes Mack, an IT auditor and author of the ITauditSecurity blog. The blog keeps a running tally of the skills IT auditors should have, from basic typing to understanding permissions and knowing how networks, applications and databases interact.

However, Williams and Martin both said that even IT-proficient auditors need continuous training to stay sharp. Williams plugged the Cybersecurity Nexus training program he runs at ISACA. Martin said IGs need to find specialized training for their auditors because the Council of the Inspectors General on Integrity and Efficiency's training program does not offer the necessary cybersecurity courses.

Martin added that tech can be a boon, not just a burden, for regulators and auditors, and he cited the analytics work done by the National Science Foundation's IG as an example.

In the meantime, experts advise making the most of the resources you have.

"We matrix our teams," said Martin, explaining that one IT pro can support a bigger team of reviewers to make audits more effective. ■

MOVING THE NEEDLE AT GSA

With a focus on entrepreneurship and customer service, Phaedra Chrousos is applying private-sector solutions to the sometimes-rigid federal bureaucracy

BY BIANCA SPINOSA

Profile: Phaedra Chrousos

As the first chief customer officer at the General Services Administration, Phaedra Chrousos is infusing some entrepreneurial know-how into an agency that is in the process of reinventing itself.

The CCO position is not just new to GSA. It's new to the federal government, which has rarely been accused of being a bastion of customer service.

Chrousos joined GSA from the private sector in June 2014. She had already co-founded two New York City-based start-ups when then-GSA Administrator Dan Tangherlini was introduced to her through the Partnership for Public Service.

"It was about choosing a hypothesis we both had that a dedicated, empowered team around the customer could actually move the needle at GSA when it came to the way that customers think of the agency," Chrousos told FCW.

Greg Godbout worked with Chrousos on customer service projects for about a year during his tenure as executive director of GSA's 18F. "She's an experienced business owner and an experienced entrepreneur," said Godbout, who's now CTO at the Environmental Protection Agency. "Government needs more entrepreneurs, people who can think outside the box."

'No stone unturned'

Chrousos took on a second set of responsibilities in January when she was named associate administrator of GSA's Office of Citizen Services and Innovative Technologies. She now oversees 18F, but Godbout recalled an earlier interaction when Chrousos was a customer and her team needed software for an important project.

"She left no stone unturned," he said. "That's the type of tenacity you need to figure out ways to get things done.... 18F is that way. It was fun for me to watch her doing that in another office in a different capacity but totally related to driving better services for the American people."

GSA manages 9,000 buildings for the government around the country, so the bulk of the agency's customers are other federal agencies. One of the first things Chrousos did as the new CCO was survey more than 1 million of GSA's tenants.

"It was the first time we had actually surveyed every single tenant of ours," Chrousos said.

The agency followed up with focus groups and then developed action plans for building-related measures GSA plans to implement this year.

'The right person at the right time'

GSA's other main customer base, of course, is contracting officers. To better understand that audience, Chrousos' 230-person team of developers, designers and tech innovators sifted through data, deployed surveys and conducted more than 200 interviews to shape customer journey maps. After the team collected the data, it put the information into the hands of decision-makers.

When it comes to improving the customer experience, Chrousos said she's found that one of the biggest challenges is often a lack of information, not a resistant agency culture.

"Everyone was really excited about the customer," she said. "They were in the government because they were altruistic. They were in the government to do great things, but they just didn't have anything beyond anecdotal evidence to get the job done."

When Tangherlini recruited Chrousos, he was in the midst of trying to reform the agency after a 2012 scandal involving lavish conference spending. He told FCW that Chrousos was "the right person at the right time" to help rejuvenate the agency and bring a fresh perspective.

"The cool thing about taking on someone like Phaedra into this work, she was going to ask substantial questions and existential questions," Tangherlini said. "She was going to bring some of this current thinking to government."

Chrousos honed that thinking by building digital businesses in the private sector. She co-founded and served as chief operating officer of Daily Secret — a digital media company that focuses on city-specific email newsletters — and she oversaw the launch of 37 editions in 21 countries. Before that, she had co-founded HealthLeap, an online service to help physicians with appointment booking, and earlier still, she worked for the Boston Consulting Group.

She studied economics and sociology at Georgetown University and holds graduate degrees from the London School of Economics and Columbia University. She said she was drawn to government work because it fueled her sense of mission. But it has also proven to be rewarding in other ways.

"I've actually found it to be really fun as well," she said. "It's hard and difficult and important, but it's also a lot of fun. My colleagues are very smart. They're all here to do great things and to make a difference, and it's a wonderful environment to be in."

'Naiveté about the government helps'

Chrousos is leading 18F at a time of tremendous growth. The digital innovation hub was launched in March 2014 with five people and has now grown to about 110. By 2017, Chrousos said, the staff is projected to grow to 300.

"We feel like the appetite for our work is tremendous," said Chrousos, adding that 18F's intake pipeline is 100 projects deep.

To keep pace, 18F has developed a blanket purchase agreement for agile development services that aims to connect agencies with vendors that can provide iterative software development, user-centered design and DevOps.

"That was our way to scale," Chrousos said. "We realized we couldn't grow fast enough, so the only thing we could do was partner up with the private sector to work together on the new project."

18F's rapid growth is coupled with a new demographic of

> **We realized we couldn't grow fast enough, so the only thing we could do was partner up with the private sector to work together on the new project.**

government workers. The hub has earned the reputation of recruiting mostly youthful, tech-savvy Silicon Valley types more likely to be at home in an RV in Google's parking lot than working for a bureaucratic federal agency.

"I think people think of us as a bunch of kids," said Chrousos, who is in her mid-30s. "It's kind of a misconception that they're all young and new to government."

She noted that some of 18F's key early employees came from other agencies and that most are senior engineers and senior designers.

The majority of 18F employees, though, hail from outside government, and Chrousos said they bring a fresh perspective. "When you first come in, naiveté about the government helps because you believe you can change anything," she added.

18F is able to bring in those new perspectives significantly faster than most other government agencies thanks to special hiring authority, but there's a limit to how long those employees can stay — usually two to four years. Yet Chrousos predicted that built-in churn would also pay dividends.

She points to the Defense Advanced Research Projects Agency as an example. Created in 1958 to drive the development of emerging technologies for the military, DARPA limits key staff to five-year terms and "turned out to be one of the most innovative places in government," she said.

Godbout went even further by saying the only way to effect change is to pair workers from outside government with innovators who are already working at agencies.

"There's always going to be friction," he said. "There's no way to avoid that. Let's bring in these methodologies and these new people, but how do we pair them with the innovators who are already here who actually already have some really good ideas and have tried things? And that's how you scale quickly."

Chrousos "has been doing that same sort of playbook," Godbout added.

What's next?

Chrousos played down the friction factor. "There's no bad blood between the old guard and the new guard," she said. "I think it's less black and white [than] people think it is." And ultimately, she noted, "good work speaks for itself."

In the short term, Chrousos said she hopes 18F's good work can meet agency needs, create ripple effects and "make agencies more agile and more open and more cognizant of the end user." Further down the road, however, her goals are more transformative.

"In the very long term...I hope that 18F is no longer needed in government and that every agency has a digital service team," she said. "At the end of the day, 18F is a platform to bring in smart people in areas where the government has a dearth of that talent. If in 20 years the government needs something it doesn't have, I'm hoping 18F is that platform." ■

IT insecurity and the need for better management

Effective implementation of FITARA is the government's best hope to address decades of mismanagement and make IT systems more secure

BY RICHARD A. SPIRES

In my previous column, I described the three primary root causes that have led to the massive data breaches and compromises of core mission IT systems at multiple federal agencies. The first root cause is the government's lack of the use of IT management best practices — a problem that goes back to the 1990s.

In that column, I stated that the best cybersecurity defense is the result of managing your IT infrastructure and software applications well.

Yet the government's highly distributed approach to IT management has led to such complexity that for many agencies, maintaining a sea of vastly different systems in an ocean of differing IT infrastructures makes it impossible to properly secure such an IT environment.

Since at least the late 1990s, some leaders in government have realized that the highly distributed approach to IT management has significant downsides, but entrenched interests made it exceptionally difficult to effect the necessary changes. For instance, a number of laws have been passed that attempted to address IT management practices. Most notably, the Clinger-Cohen Act of 1996 mandated a strong agency

> **Clinger-Cohen is viewed largely as failed legislation in the federal IT community because in reality, no agency CIO has the authority granted by the act.**

CIO who could begin to rationalize IT within that agency.

Yet Clinger-Cohen is viewed largely as failed legislation in the federal IT community because in reality, no agency CIO has the authority granted by the act. Components, bureaus and program offices have generally resisted efforts to bring more oversight and discipline to IT management and operations, under the theory that it impedes mission and business progress.

The government does have another opportunity to address IT management weaknesses, however. In December 2014, Congress passed and the president signed the Federal IT Acquisition Reform Act, which was included in the fiscal 2015 National Defense Authorization Act.

FITARA is meant to address the systemic problems in managing IT effectively at agencies — and although there are a number of provisions, the bill's main intent is to empower agency CIOs to address those problems.

Foremost among these problems are duplication of IT infrastructure and systems, lack of adherence to best practices in IT acquisition, and implementation of proper procedures to ensure IT security is prop-

erly addressed throughout an agency's IT organization and infrastructure.

To make sure FITARA does not suffer the same fate as Clinger-Cohen, a successful rollout is critical. I am pleased to see the approach the Office of Management and Budget and U.S. CIO Tony Scott are taking to support the act. In developing its final guidance to help agencies implement FITARA, OMB sought significant outside input, including insight from former government CIOs, chief financial officers, chief acquisition officers, chief human capital officers and chief operating officers. OMB also sought public comment on the draft guidance, which will improve content, understanding and buy-in over the long term.

Yet a significant change-management component is required to transform decades of behavior, and this will take leadership and sustained commitment. Accountability for properly implementing FITARA must start with the White House, and then rest with OMB and the agencies. In particular, OMB must help ensure that agency CIOs have the capability to perform their jobs and the support of agency leaders so that CIOs can drive the required change to effectively implement FITARA.

Further, agency leaders must be supportive of their CIOs, especially at agencies that operate in a federated environment (this is particularly an issue in the Cabinet-level departments). Congress can support those efforts by demanding aggressive implementation of FITARA by agencies, development of measures for assessing FITARA's impact and transparency in reporting ongoing progress while also highlighting obstacles that need to be overcome.

There is much confusion regarding IT security and the best way to protect data and systems. No single product or service offers complete protection, and in my experience, if an agency does not implement IT management best practices, many of the security tools are ineffective. Those practices are foundational to success, and effective implementation of FITARA is the government's best hope to address decades of mismanagement.

My final column in this three-part series will cover steps agencies should be taking to rapidly improve their IT security posture, and I will provide recommendations related to the acquisition of IT security solutions. ■

Richard A. Spires has been in the IT field for more than 30 years, with eight years in federal government service. Most recently, he served as CIO at the Department of Homeland Security. He is now CEO of Resilient Network Systems.

The Federal IT Acquisition Summit

October 20, 2015 | Washington Hilton, Washington, DC

Participating Agencies

SEWP V

NITAAC — OMB Authorized GWACs for IT Acquisition

Featured Speakers From

ARMY CHESS — COMPUTER HARDWARE, ENTERPRISE SOFTWARE AND SOLUTIONS

This second event in the Federal IT Acquisition Summit series provides government IT decision makers with even more contract-specific training opportunities. A must-attend for the acquisition and government IT buying community!

TRAINING OPPORTUNITIES :

ARMY CHESS: ITES-3 & ADMC-3
GSA: DPA
DHS
NIH-NITAAC: CIO-CS
NASA SEWP V

FEATURED PANEL SESSIONS:

FITARA
Cybersecurity: CDM & Beyond
GSA: Alliant (incl. Alliant 2 update)
Cloud: Cloud Changes Everything

Free for Government & Military Attendees

FCW   GCN   Washington Technology   DEFENSE SYSTEMS   Federal SOUP

For Sponsorship Opportunities Contact – Stacy Money: smoney@1105media.com

http://FCW.com/FIAS

FCW Index

People

Agencies/Organizations

Advertisers

These indexes are provided as an additional service. The publisher does not assume any liability for errors or omissions.

To advertise in FCW, please contact Dan LaBianca at dlabianca@1105media.com. FCW's media kit is available at 1105publicsector.com.

PUBLIC SECTOR MEDIA GROUP

CORPORATE HEADQUARTERS
9201 Oakdale Ave., Suite 101
Chatsworth, CA 91311
www.1105media.com

$18,113,000,000,000

The unpleasant outlook for fiscal 2016 funding

Not a single appropriations bill for fiscal 2016 has yet been signed into law. The House has passed six; the White House has issued veto threats for every one.

Without appropriations or a continuing resolution by Sept. 30, federal agencies would shut down for the **13th time** since 1980.

Year	Days
1981	**2 days**
1982	**1 day; 3 days**
1983	**3 days**
1984	**2 days; 1 day**
1986	**1 day**
1987	**1 day**
1990	**5 days**
1995	**5 days**
1995-96	**21 days**
2013	**16 days**

House and Senate leaders have vowed they will not allow a shutdown, but one budget analyst puts the likelihood at

60%
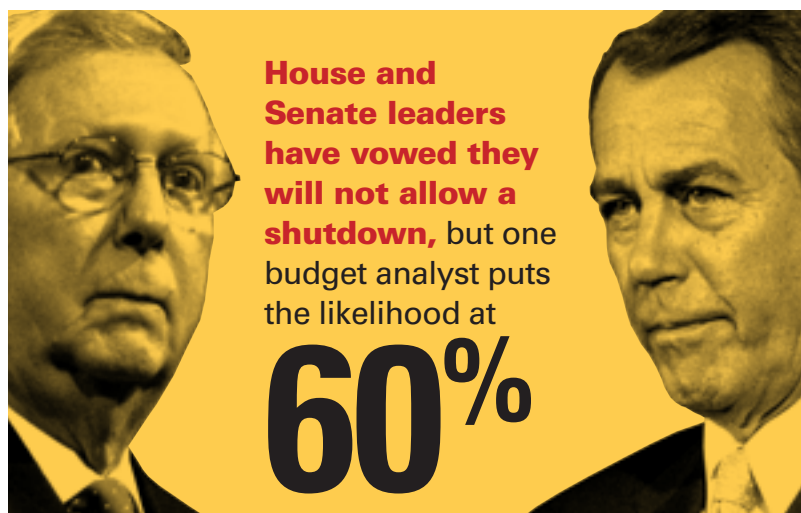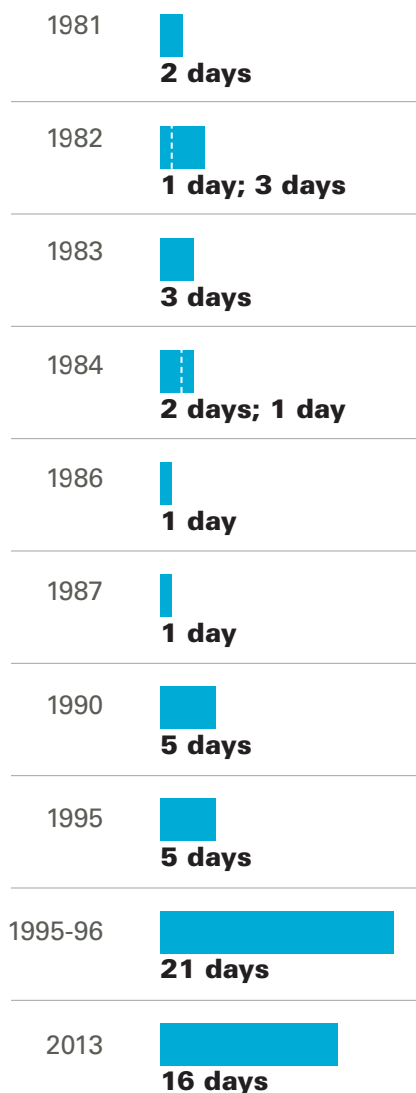
Additionally, the sequester returns on Oct. 1. Barring legislative relief, that means discretionary spending cuts of

$90.4 BILLION:

$36.5 BILLION NON-DEFENSE
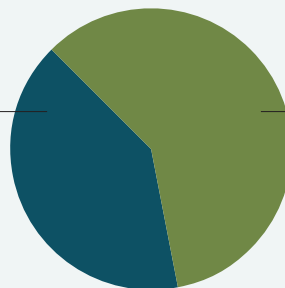
$53.9 BILLION DEFENSE

The current debt ceiling, which could be hit as soon as Oct. 30, would also cause a government shutdown — and problems far more serious than suspended IT projects.

Sources: White House, Treasury Department and Government Accountability Office

"Aggregated and normalized patient data?"
Sergeant James just feels better.

HealthShare transforms care by sharing health information.

To deliver the high quality care veterans deserve, doctors inside and outside the VA need to see a comprehensive patient record.

Using InterSystems HealthShare®, everyone can get the results they need. Patients get the safe, quality care they need to feel better. Doctors and nurses get the information they need, when, where, and how they need it, to make the best care decisions.

"Aggregated and normalized patient data"? That's one of many HealthShare capabilities for solving your toughest healthcare IT challenges.

Learn more at: **InterSystems.com/Federal1CC**

INTERSYSTEMS®

Better Care. Connected Care. **HealthShare.**

CDW·G

FederalGovernment
Solutions

The latest technology solutions for people who get IT | September 2015

010101010101
0010   0010
1001   1001010101010101
0010   0010
1001   1001

CYBER SECURITY
and CDW·G

and NOW YOU'RE NEUTRALIZING THREATS.

CDW·G
PEOPLE WHO GET IT

WIN THE WAR AGAINST CYBERCRIME

WITH ADVANCED TECHNOLOGY PROTECTION.

Federal government organizations are feeling the cyberheat. Cyberattacks are increasingly sophisticated. Insider threats continue to rise, while third–party vendors expose your agency to ever–greater compromise. Massive quantities of complex data, mobile services and devices — along with the use of cloud and outsourced services — are amplifying risk, and making security all the more challenging. Tougher regulations are forcing government organizations to further tighten data security controls.

UNDER PRESIDENTIAL EXECUTIVE ORDER 13636,

the National Institute of Standards and Technology was directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure.
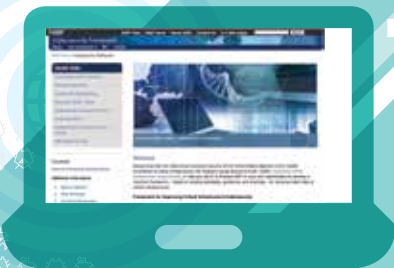
To learn more about the framework and for current updates, visit

nist.gov/cyberframework

DEFEND YOUR DATA

Protecting your agency against reputational losses gets more challenging by the day in a world where cybercriminals are incessantly testing your defenses. CDW·G's account managers and security solution architects can help make sure your IT operations are locked down against digital threats. From mobile security to defense–in–depth, CDW·G can zero in on your vulnerabilities and help you:

· Access, identify and eliminate security faults
· Lock down data and perimeters
· Maximize mobile security

CATEGORIES

INDUSTRY TRENDS
CYBERSECURITY

THE THREAT LANDSCAPE IS EVOLVING

Is your cybersecurity protection keeping up?

Internal and external cyberthreats are getting more and more sophisticated, and so should your cybersecurity defense. Are your agencies' technologies, processes and practices ready to meet the challenge?

Take a look at the cyber landscape and see if they're up to the task.

IT'S A CYBER JUNGLE OUT THERE

THREATS ARE EVERYWHERE...

1 million
Nearly one million new threats are released each day.[1]

1 in every 392 emails contains a
phishing attempt.[2]

EVEN IN YOUR OWN BACKYARD
25,556

The number of data breach events in the federal government in 2013 that involved personally identifiable information, up from 10,481 in 2009.[3]

BEWARE OF INSIDER THREATS
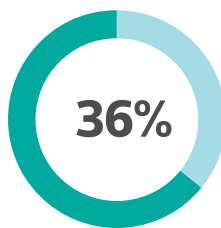
36% of breaches were a result of inadvertent misuse of data by employees.[4]

66% of security breaches go undiscovered for months.[6]

THE HIGH PRICE OF CYBERCRIME

The cost of a data breach averages
$200
PER RECORD[5]

CDW·G can help you fortify your defenses and keep your organization safe. Learn more at CDWG.com/security

Sources: [1]symantec.com, "Internet Security Threat Report," 2015 [2]Symantec Corporation, *2014 Internet Security Report*, April 2014 [3]Gao.gov, "Federal Agencies Need to Enhance Responses to Data Breaches," April 2014 [4]cuna.org, "Assess Internal Threats to Your Network," October 3, 2014 [5]cfo.com, "Calculating the Colossal Cost of a Data Breach," March 24, 2015 [6]Ponemon Research Report, *The Risk of an Uncertain Security Strategy*, November 2013

SIX WAYS TO IMPROVE COLLABORATION ACROSS YOUR AGENCY

Cloud collaboration tools offer a tremendous range of benefits for small organizations. While such tools can function independently, they'll also build upon one another cooperatively.
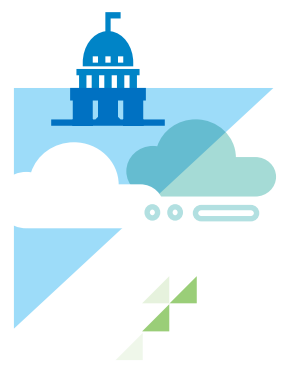
Fast, Secure Data Sharing

Put an end to file version sprawl or workers putting sensitive data on nonsecure devices. Collaborative file management means simultaneous access and a safe workflow while only paying for the storage capacity you need.

Scalable Video Presentation and Conferencing

Whether you only need a manageable way for two workers to chat face-to-face remotely or you want to deliver a live product announcement to thousands around the world, video collaboration can help you convey information without specialized conference rooms.

Cloud-Based VoIP

IP telephony delivers the traditional benefits of phone calling, only with far more feature flexibility and without many of the legacy infrastructure costs.

Centralized, Location-Independent Project Management

Once projects live in the cloud, managers can control and direct them from any compatible device anywhere.

Presence and IM

Recoup minutes every hour by knowing each worker's state of availability and whether more in-depth communication is needed before time is needlessly wasted. Simultaneously, keep your messages secure with sanctioned, enterprise-class IM rather than public options.

Searchable Group Pages and Sites

Establish virtual homes for workgroup projects. This keeps content and communication centralized while providing an easy, efficient way to search through project-related materials.

Learn more about cloud productivity at CDWG.com/cloud

CDWG.com/microsoft
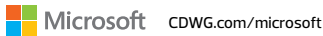
Office

Microsoft® Office Pro Plus 2013
The new way to work together
Open License Government[1]
CDW 2894629
$**402**.98

The new Office provides productivity and collaboration for organizations. Enjoy virtually anywhere access to familiar Office applications, with email, calendar, video conferencing, and most up-to-date documents across nearly all your devices — from PCs to smartphones to tablets.

- Work from virtually anywhere with access to your latest documents and files
- Work together, easily using Office applications with email, shared calendar, document sharing and HD video conferencing
- New features in Excel® and PowerPoint® allow you to easily analyze your data and hold effective presentations

---

CDWG.com/ibm

Premier
Business
Partner
IBM®

Team with CDW·G to build your solution; get exceptional licensing and services to help ensure success
IBM SmartCloud® for Social Business
Collaboration services through web browsers, on mobile devices and on Windows®, Mac® and Linux® desktops
CALL FOR PRICING

IBM SmartCloud® for Social Business is available with no need to buy, build or support your own server infrastructure. Unlimited guest access means you can extend your collaboration outside your organization without additional fees. And since clouds don't exist in vacuums, IBM SmartCloud infrastructure supports integrating with your existing desktop and back-end systems and retaining your existing data.

Adobe
CDWG.com/creativecloud

Adobe® Creative Cloud® for teams
Built to accelerate your business
Per User for a 12-month subscription — multiple platforms
CDW 3415594
$**583**.53

Work wonders.

Step up from Creative Suite® to the 2015 release of Creative Cloud® and drive powerful results across your team.

Get exceptional creative apps and services and everything else your organization needs to efficiently create amazing content and collaborate freely across desktop and mobile.

Google™ CDWG.com/google

Google™ Apps

Google Apps for Government
Web-based email, calendar and documents that let you focus on your mission
CDW 3528136
CALL FOR PRICING

With modern email and collaboration applications that make your workers more productive, your agency can dedicate more time to your critical mission of serving the public.

- Reduce licensing costs, infrastructure costs and increase staff productivity
- Stay connected from anywhere — on your Android™, iPhone®, Blackberry® and Windows® phone
- Security first — work is always backed up, own and control data, increased security and reliability, strong encryption and authentication
- Work smarter — work together in real time, search and share, work together across distance, work together across organizations
- Invisible IT that just works — no more patches, new features as soon as they're ready, no hardware or client software, 24/7 customer support

---

[1]Purchase five licenses OR one processor license to qualify for the Microsoft Open License Government program; media must be purchased separately; call your CDW·G account manager for details

5

Cloud Security

Cloud-based security puts effective data protection within reach — even if you don't have adequate IT staff at your fingertips. Hosted and managed by an external provider, this robust security option automatically updates to help ensure users have the most current protection. Without a full-fledged program to run, it places less stress on your machines, and without software deploy, it can be rolled out in a timely and cost-effective manner. Our experts can help you find the solution that meets your needs.

VARONIS

Varonis® DatAnywhere®
The cloud file-sharing experience with your existing infrastructure
CALL FOR PRICING

Varonis® DatAnywhere® gives IT the ability to provide an alternative to cloud-based file-sharing solutions that is secure, easy to use, and a fraction of the cost of shipping your data to the cloud.

• Create a secure private cloud experience using your existing file-sharing infrastructure
• Keep your data on your file servers
• Keep your existing permissions (e.g., NTFS and Active Directory®)
• Provide secure, enterprise-capable file synchronization, mobile access and third-party file sharing

---

KASPERSKY   CDWG.com/kaspersky

See for yourself how Kaspersky can secure your environment — physical, mobile and virtual — call your CDW·G account manager for a web demo
Kaspersky® Endpoint Security for Business — Advanced
Boosting IT security and efficiency across your organization

One Node With one-year subscription license
CDW 2951621
$**53**.86

Kaspersky Advanced tier delivers the protection and management solution your organization needs to enforce IT policy, keep users free from malware, prevent data loss, and enhance IT efficiency.

---

imprivata OneSign®

Software solution-based architecture
Imprivata® OneSign®
Identity and password proliferation under control
CALL FOR PRICING

Imprivata® OneSign® is an identity and access management platform that integrates user authentication, user access, password management and aggregated audit data in one secure and easy-to-manage appliance.

• Streamline access through strong authentication
• Enhance end-user productivity
• Quickly deploy without interfering with existing IT infrastructure

Cloud Storage

There are many types of clouds to support your growing storage needs, including public, private, hybrid and community. Cloud storage is available as a service, product or solution that can be used for building or delivering other information services. CDW·G has experts on hand to help guide you to the storage solution that makes sense for your organization and your budget.

VEEAM IT JUST WORKS!™ CDWG.com/veeam

Veeam® Backup & Replication™ v8
Delivering Availability for the Modern Data Center™
CALL FOR PRICING

Veeam® Backup & Replication™ provides fast, flexible and reliable recovery of virtualized applications and data.

- Brings backup and replication together in a single solution
- Increases the value of backup and reinvents data protection for VMware vSphere® and Microsoft® Hyper-V® virtual environments
- Veeam is much more than just backup — it leverages virtualization, storage and cloud technologies
- Delivers recovery time and point objectives (RTPO™) of less than fifteen minutes for all applications and data
- Provides capabilities in high-speed recovery, data loss avoidance, verified protection, leveraged data and complete visibility

✦VISION SOLUTIONS CDWG.com/doubletake

Double-Take® Availability™ by Vision Solutions®
Real-time protection for Windows®, Linux® and IBM® servers
CALL FOR PRICING AND LICENSING OPTIONS

- Supports any combination of physical, virtual and cloud servers
- Protects your organization with anything-to-anything real-time, byte-level replication
- Provides comprehensive high availability and disaster recovery with near-zero downtime
- IT flexibility — server, storage, application and hypervisor agnostic
- Enables easy, full-server failover in minutes, not hours

Acronis CDWG.com/acronis

Acronis® Backup Service
A complete, cost-effective and easy-to-manage hybrid local and cloud backup solution
CALL FOR PRICING

Acronis® Backup Service protects everything — physical servers, virtual servers and PCs — with backup to your local or network storage and to Acronis' secure offsite data centers. With a few simple clicks, you can back up and restore anything — individual files, disks or entire systems — in minutes.

Using the intuitive web interface, your IT team can:

- Streamline implementation
- Manage the service directly in the cloud
- Significantly reduce costs
- Significantly reduce IT workload
- Eliminate central management components
- Eliminate dedicated backup servers, cores and cells
- Eliminate the need for VPNs or direct connections

Cloud Collaboration

Cloud computing is changing the way federal agencies deliver and consume IT services. By putting server, storage, compute and networking resources on a virtualized platform, organizations are able to create an agile and efficient pool of on–demand resources. We can help you implement a cloud collaboration plan that includes everything from strategy and design to implementation and ongoing management.

CDWG.com/cisco

Esna Cloudlink for Cisco®
Experience faster, more efficient and effective collaboration
CDW 3084118

$ **29**.99

Esna Cloudlink 5.0 seamlessly integrates Cisco® Collaboration solutions with cloud-based productivity applications such as Google Apps, Salesforce®, Jive®, and IBM SmartCloud® making it easy for you to find, connect and collaborate live with others.

Unified messaging: access and manage voice messages from your email or Jive inbox on desktop and mobile devices. Resolve messages to your contacts to escalate any message to a live voice or video conversation. Bidirectional synchronization between email and Cisco Unity Connection will turn off the message waiting indicator (MWI) on the deskphone.

- See when people are on the phone, their location and with Google Calendar integration, their availability
- Connect with others by clicking on phone numbers or extensions displayed in any cloud application or web page. Dial any number and select the desk phone, softphone or mobile device you want to make the call from
- Chat one–on–one or with a group of people using Jabber® IM through iLink for Cisco. Easily add people to any IM session and share your location right within the chat window

Microsoft
CDWG.com/microsoft

Office 365

Microsoft® Office 365™ Pro Plus
Simplify your IT with up–to–date Office tools and services
Open License Government[1]
CDW 3120376

$ **122**.68

- You can access Office from virtually anywhere, across devices, so everyone in your organization has the freedom and flexibility to be more productive wherever they're working
- It's easy to keep the work flowing when you have tools that make communicating with team members, partners and others a rich and convenient experience
- Comprehensive solutions, such as desktop productivity applications, portals, extranets, external websites, instant messaging (IM), voice conferencing, video conferencing, web conferencing, email and voicemail

CITRIX®
CDWG.com/citrix

CITRIX® GoToMeeting

Citrix® GoToMeeting®
Online meetings made simple
CDW 3289153
CALL FOR PRICING

Citrix® GoToMeeting™ is an easy, fast and secure solution for conducting and attending small–group online meetings with up to 25 attendees. Its innovative, All You Can Meet® flat–fee subscription model enables individuals to use online meetings more often, resulting in increased productivity and a quicker ROI. With GoToMeeting, it's easy to meet naturally online with integrated audio, HD video conferencing and screen sharing.

- Web tools — share your desktop, change presenters, transfer control, chat, draw, highlight, record and more
- Audio — GoToMeeting sets up your conference call for you and provides a free VoIP option
- HD video — the HDFaces® video feature lets up to six attendees to show their webcams in high definition – no special equipment required

CDWG.com/cisco

Cisco® IP Phone 8861
Delivers an advanced, user–friendly experience
CDW 3403695

$**602**.48

- Cisco® Intelligent Proximity integrates select telephony features with your personal mobile devices — USB and Bluetooth® support offer choices in accessories
- Comprehensive and highly secure mission–critical UC features from on–premises and hosted Cisco communications servers
- Share contact lists and call history — move the audio path of active voice and video calls
- Exceptional clarity in voice communications — high–quality, full–duplex, wideband (G.722) audio with echo cancellation for third–party headsets, the handset and speakerphone

AVAYA
The Power of We™

CDWG.com/avaya

Avaya Scopia® XT7100 Video Conferencing Room System
Build relationships and accelerate your productivity with Avaya Scopia Video Collaboration
CDW 3726327

$**8869**.76

- Two simultaneous 1080p/60 fps video channels for live video and content
- 10X optical zoom camera, 4X digital zoom, 40X total
- Dual display support
- Multitouch control via Scopia® Control for Apple® iPad®

Polycom
CDWG.com/polycom

Polycom® VVX® 400 Series Media Phone
High–quality, cost–effective solution to frontline staff handling moderate volume of calls through advanced UC telephony features
CDW 2994777

$**213**.46

- Outstanding voice clarity of Polycom® HD Voice™
- Intuitive larger, color display and easy–to–use line appearances
- Leverage investments — deploy on existing networks and UC systems
- Ready for future expansion modules as your users' needs and organization grows

lifesize.
CDWG.com/lifesize

Lifesize® Icon™ Flex Video Conferencing Kit
If your team wants to use a video collaboration application like Lifesize Cloud in the meeting room, then you need the Lifesize Icon Flex video conference system to bring it to life
CDW 3594039

CALL FOR PRICING

- Click on a name in your directory to initiate a call
- Add call participants with a single click
- Integrate seamlessly into your infrastructure
- Interoperable with third–party systems and solutions

9

plantronics. CDWG.com/plantronics

Plantronics® Voyager™ Edge UC B255 Headset
Audio performance and comfort with intuitive, responsive features and its own portable charging case
CDW 3677423

$**162**.58

- Charging case enables up to 16 hours talk time (up to six hours without case)
- Multiple microphones and signature Plantronics® audio technology eliminate disruptive background noise
- Voice commands and smartphone assistant integration

Plantronics EncorePro™ HW540 Convertible Headset
Flexible headset combines three easily swappable wearing styles in one design
CDW 3506792

$**89**.77

- Exceptional noise cancelling for clearer calls, and increased reliability so conversations can continue without worry
- High-quality audio, a flexible mic with visual positioning guides, soft ear cushions, and durable-yet-lightweight materials for all-day wearing
- Quick Disconnect feature provides walk-away convenience and compatibility with all Plantronics USB, desk phone audio processors and direct connect cables

Jabra® CDWG.com/jabra

Jabra Evolve™ 20 UC Stereo Headset
A professional headset designed for music and voice
CDW 3521186

$**52**.00

Premium noise-cancelling technology gives you peace to work in a noisy, open office; effectively creating a concentration zone around you so you can stay focused.

- Includes a control unit that supports comfortable and easy access to most-used functions
- Ability to answer and close calls directly at the control unit
- Ear cushions are designed to reduce high-frequency sounds

peerless-AV™

Peerless® SR560M
Universal flat-panel TV cart
CDW 1163074

$**490**.76

- Supports screen sizes up to 75"
- Designed to hold flat-panel displays weighing up to 150 lbs. and a maximum of two shelves holding up to 50 lbs. each
- Continuous vertical adjustment for ideal viewing height
- Incremental tilt of -2°, 0° and +5° locks in the ideal viewing angle
- Integrated cable management protects, contains and conceals cables for a clean, professional installation
- Maneuvers on 4" (102 mm) swivel casters, two casters lock
- Customizable with over a dozen accessories

PLANAR
CDWG.com/planar

Planar® PS8250
82" LED–backlit, flat–panel LCD
CDW 3577570
CALL FOR PRICING

Designed for demanding digital signage and commercial applications.

- Includes USB media playback, built–in speakers and a wide array of inputs
- Bezel is logo–free, allowing the spotlight to shine on the content and not on the frame
- Ideal for landscape and portrait orientation
- CustomerFirst™ three–year warranty featuring two–day advance replacement

ViewSonic
the choice of professionals
CDWG.com/viewsonic

ViewSonic® CDE6500–L
65" Full HD LED commercial–grade display
CDW 3355982
$**2299**.99

Features hospitality mode for customized settings.

- 1080p Full HD commercial display for HD multimedia applications
- USB multimedia player for scheduled playback of photos and music
- Mercury–free LED backlight reduces power consumption
- SuperClear® wide viewing angle technology delivers accurate and vivid colors from nearly any angle
- Versatile I/O ports: HDMI™, DVI™, CVBS, YPbPr (YCbCr), VGA and RS232 for easy connection to a variety of equipment

SAMSUNG BUSINESS
CDWG.com/samsung

Samsung® DM40D
40" slim, direct–lit LED display
CDW 3327550
$**784**.00

Delivers 24/7 reliability for continuous operation.

- Sleek industrial design with symmetrical 9.5 mm bezel
- Enhanced SSP system–on–chip (SoC) performance with quad–core processor
- Built–in Wi–Fi® and AllShare® Cast for simple content mirroring from mobile devices
- Max. resolution: up to 1920x1080
- Panel brightness: 450 cd/m²

NEC
CDWG.com/nec

NEC MultiSync® X651UHD
65" LED–backlit Ultra HD LCD panel
CDW 3680937
$**6899**.00

- Amazing imagery delivered by an LED–backlit UHD S–IPS panel
- Enhanced image performance with advanced settings of all relevant visual parameters for full control of brightness, color, gamma and uniformity via Spectraview™ Engine
- Reliable color reproduction with 10–bit color and amazing viewing angles
- Future–proofed with OPS expansion slot
- 24/7 operation with reliable, industrial–grade component for mission–critical operations

THE FUTURE–FORWARD DATA CENTER

When your data center is more streamlined than sprawling, you're able to scale to meet your organization's future demands. With a converged infrastructure solution from CDW·G, you can support increases in network demand and heavier workloads — all inside one reliable and manageable platform.

$5.3 Billion

The total expected savings and cost avoidance from the federal data center consolidation initiative by 2017.[1]

20%

of IT pros listed data center initiatives as their primary focus for 2015.[2]

84% of data centers have had issues with power, space, cooling capacity, assets and uptime that negatively impacted operations.[3]

3X

data center traffic will triple by 2018.[4]

To learn more about optimizing your data center, visit **CDWG.com/datacenter**

Sources: [1]U.S. Government Accountability Office [2]CDW, Surveying Your Network: A CDW Advisory Board Decision–Maker Study, July 2014 [3]idc.com, ''What IT Managers Want from DCIM: Results of IDC's 2013 Datacenter Survey,'' December 2013 [4]cisco.com, ''Global Cloud Index,'' November 2014

CDWG.com/hp

intel inside™ Xeon®

Hard drives sold separately

HP MSA 2040 Storage Array
New high-performance hard drive array
24-bay (SFF SAS), 2U rack, 21.6TB system capacity
CDW 3148667

CALL FOR PRICING

- Uniquely addresses HP ProLiant customers' shared storage and data protection needs
- Reduces TCO while dramatically increasing performance using technologies such as solid-state drives, snap and volume copy and replication
- Positioned to provide an excellent value for organizations needing increasing performance to support initiatives such as consolidation and virtualization
- Delivers performance by leveraging controller architecture with a processor, four ports with 4GB cache per controller and using drive technologies such as SSDs
- Ships standard with 64 snapshots and volume copy enabled for increased data protection

HP DL360 Gen9 Server
Lower IT service costs and service delivery time
CDW 3466978

$1899.99

The HP ProLiant DL360 Gen9 Server is a performance-driven 1U server that you can easily deploy for virtualization, creating databases or for high-performance computing.

- Memory: 8GB std., 384GB max.
- Six-Core Intel® Xeon® E5-2609v3 processor (1.90GHz)
- Hard drive: none ship std.

CDWG.com/citrix

Citrix XenApp®
Deliver applications as a cost-effective, on-demand service to your users, anywhere

CALL FOR PRICING

Citrix XenApp® is a Windows® application delivery system that manages applications in the data center and delivers them as an on-demand service to users anywhere. XenApp® reduces the cost of application management, increases IT responsiveness when delivering an application to distributed users and improves application and data security.

XenApp enables organizations to improve application management by:

- Centralizing applications in the data center to reduce complexity and lower the cost of desktop management by up to 50 percent
- Controlling and encrypting access to data and applications to improve security
- Delivering applications instantly to users anywhere on any device
- Simplifying and automating the process of delivering or updating applications, enabling IT to focus on strategic initiatives

CDWG.com/edgememory

EDGE™ Server Memory Upgrades
Equip your server with additional memory from EDGE
CALL FOR PRICING

- Engineered and specifically designed to meet exact OEM specifications
- 100% individually tested modules

13

EMC and CDW·G

Let us help you optimize your storage system with XtremIO from EMC, a scale-out all-flash array and truly consistent performance offering. It enables application acceleration, total workload consolidation and the predictable and balanced performance you need to keep your data protected, encrypted and always available.

EMC² CDWG.com/emc

EMC® XtremIO™ Enterprise Storage Array
Unlock the full potential of flash and solid-state disk
CDW 3227160
CALL FOR PRICING

- As a scale-out design, this array delivers very high performance levels by creating clusters of multiple X-Bricks
- The consistent method of evenly distributing data across all SSDs for all volumes means that every volume gets the full performance potential of the array
- Load balanced — as clusters grow, data is always balanced across all controllers and SSDs
- Requires no tuning — you don't have to plan for RAID levels, drive groups, stripe sizes, LUN to RAID-group mappings, etc., to achieve maximum performance

EMC VSPEX® BLUE Hyper-Converged Appliance
VSPEX BLUE gives you a single appliance with compute, memory and storage all converged
CDW 3616149
CALL FOR PRICING

- Four nodes of integrated compute and storage, including flash (SSD) and HDD
- VMware EVO:RAIL™ software including VMware® Virtual SAN™ (VSAN)
- 128GB memory per appliance
- 10 Copper Gigabit Ethernet network connectivity
- EMC VSPEX® BLUE Manager provides a system health dashboard and support portal

EMC VNX5600™ Unified Storage Platform
Powerful multi-core optimization
CDW 3097207
CALL FOR PRICING

- Scalable, easy-to-use solution for multiprotocol file and block data services
- Centralized management makes administration simple
- Data efficiency services reduce your capacity requirements up to 50%
- Optimize for virtual applications with VMware and Hyper-V® integration
- Flash optimization delivers high levels of transactional performance with increased bandwidth and low latency
- Built for high availability in mission-critical environments

CDWG.com/cisco
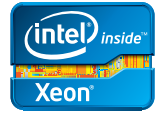
Hard drives sold separately

Cisco® UCS® B200 M3 Blade Server

Delivering performance, versatility and density without compromise

Two Eight–Core Intel® Xeon® E5–2665 processors (2.40GHz)

CDW 3253169

$1495.24

The Cisco UCS® B200 M3 blade server further extends the capabilities of the Cisco Unified Computing System™ portfolio in a half-width blade form factor. The Cisco UCS B200 M3 harnesses the power of the latest Intel® Xeon® E5–2600 series processor family CPUs with up to 768GB of RAM (using 32GB DIMMs), two drives and up to 80Gbs throughput connectivity.

• Memory: 16GB std., 768GB max.

• Up to two optional hot–swappable SFF SAS or SATA bays; 2TB max. storage

Cisco UCS Bundle

Cisco UCS C240 M3 Series Server

High–performance design and internal storage

Quad–Core Intel® Xeon® E5–2609 processor (3.10GHz)

CDW 3186854

$2880.77

The Cisco UCS C240 M3 rack server is a two–socket, two–rack unit (RU), enterprise–class, rack-mount server. The addition of the Intel® Xeon® E5–2600 processor product family delivers an optimal combination of performance, flexibility and efficiency gains.

• Memory 16GB std., 384GB max.

• Hard drive: none ship std.; up to 16 SFF hot–swappable SATA bays available, 24TB max. storage

• Four 1GbE built–in LAN interfaces

CDWG.com/hp

Hard drives sold separately

HP DL380 Gen9 Server

The right compute, for the right workload

Six–Core Intel® Xeon® E5–2609v3 processor (1.90GHz)

CDW 3466969

$1984.02

The HP ProLiant DL380 Gen9 Server delivers the latest performance and expandability in the HP 2P rack portfolio. Reliability, serviceability and near continuous availability, backed by a comprehensive warranty, make it ideal for any server environment.

• Memory: 8GB std., 384GB max.

• Hard drive: none ship std.

Kingston CDWG.com/kingston

Kingston® Server Upgrades

Search for and equip your systems with additional memory from Kingston

CALL FOR PRICING

• 100% individually tested modules

• Patented dynamic server burn–in

• 100% compatible — will not void your system warranty

• Unlimited 24–hour Kingston® technical support

Tripp Lite OMNI1500LCDT

Advanced line-interactive LCD UPS for PCs, network equipment and more
CDW 2885460

CDW·G EXCLUSIVE PRICE

$**156**.60[1]

- 1500VA, 10 outlets, USB/TEL/DSL/Ethernet protection
- Automatic voltage regulation (AVR) corrects brownouts without draining battery power
- LCD continuously reports operating mode and battery charge level, plus additional UPS and site power data
- $250,000 Ultimate Lifetime Insurance

**Tripp Lite SR42UB
SmartRack™ Enclosure**

42U premium enclosure designed for secure, high-density server and networking applications
CDW 858765

CDW·G EXCLUSIVE PRICE

$**896**.74[1]

The SR42UB is packed with features designed to simplify rack equipment installations and maintenance and is compatible with Tripp Lite's extensive range of rackmount accessories, enabling you to customize your solution to meet any requirement.

- Compatible with all EIA-310-D compliant 19" rackmount equipment
- 42U enclosure, 78.5x23.63x43 (HWD), heavy-duty load capacity up to 3000 lbs.
- Locking and removable front and split rear doors; locking, removable split side doors
- Five-year product warranty

25U Rack Enclosure   CDW 858178 $**879**.79

Tripp Lite SU1000RTXLCD2U SmartOnline™ LCD UPS

High-level power protection
CDW 2698655

CDW·G EXCLUSIVE PRICE

$**661**.33[1]

- 1000VA, 900W, six outlets, true online protection, zero transfer time
- LCD control panel with nine selectable screens of UPS and site power data
- USB port, DB9 port, SNMP/web interface and included PowerAlert® software

Tripp Lite 1U Rackmount Console KVM

Control an entire network — in just 1U of rack space
CDW 913496

$**681**.28

- Combines 17" LCD screen, keyboard and touchpad in a 1U rackmount, heavy-duty steel drawer
- Connects to a PS/2 or USB server or KVM switch

1U KVM Rackmount Console, 19" LCD   CDW 1324748 $**683**.28

1U Dual Rail KVM Rack Console, 17" LCD   CDW 2306940 $**1125**.17

Raritan CDWG.com/raritan

Raritan® Dominion® LX
16-port KVM over IP switch
CDW 2544855

$**1192**.00

Dominion® LX is a true next-generation switch with an advanced hardware and software architecture. This innovative design enables new levels of KVM over IP performance, reliability, usability, compatibility and security.

• One remote with BIOS-level access, one local user, up to 16 servers
• Supports PS/2, USB, DVI™, HDMI™ and DP servers
• Universal Virtual Media™ — installs software, transfers files and backs up data remotely
• Absolute Mouse Synchronization™ — reduces installation time

BLACK BOX CDWG.com/blackbox

Black Box® ServSwitch™ Agility DVI, USB and Audio Extenders over IP Kit
Extend signals and do more with digital KVM extension over IP
CDW 2912491

$**1625**.92

• Flexible topology for KVM extension
• Delivers exceptional digital video with no loss
• No-loss compression minimizes bandwidth use while maximizing the user experience

belkin CDWG.com/belkin

Belkin® Fiber Optic Cable
Maximize network speed with higher bandwidth

LC/LC CDW 1042665
LC/ST CDW 1042666
LC/SC CDW 1042669
SC/SC CDW 1042670
ST/ST CDW 1042667
CALL FOR PRICING

Three-meter fiber-optic multimode cables, 62.5/125¨.

Belkin Small Form Factor Pluggable (SFP+) Cables
SFP+ 10Gbps performance

1m CDW 2824209
2m CDW 2824212
3m CDW 2824214
5m CDW 2824217
10m CDW 2824218
CALL FOR PRICING

• Hot-pluggable design
• Fully Cisco® compatible
• Compliant to SFF-8431 standard
• Five-year warranty

VIRTUALIZATION IS KEY

Storage virtualization offers a number of advantages to federal government agencies including improvements in efficiency, costs savings and disaster recovery.

Our solution architects can draw up a virtualization plan tailored to the needs of your organization. In addition to maximizing the efficiency of your physical resources, they'll keep your data center standing through the challenges that lie ahead.

86%
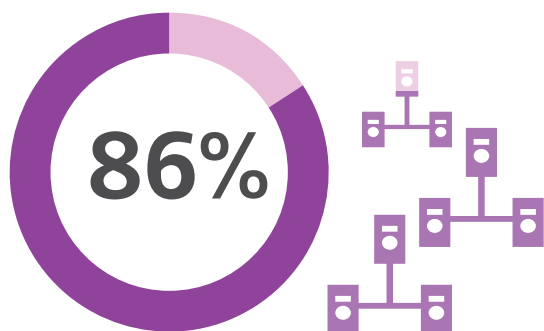
of data centers will be virtualized by 2016.[1]

$48.8 Million

The estimated amount the GSA will save from data center consolidation and cost avoidances between fiscal years 2011 through 2015.[2]

44

THE NUMBER OF MAJOR DISASTERS THE FEDERAL EMERGENCY MANAGEMENT AGENCY DECLARED IN 2014.[3]
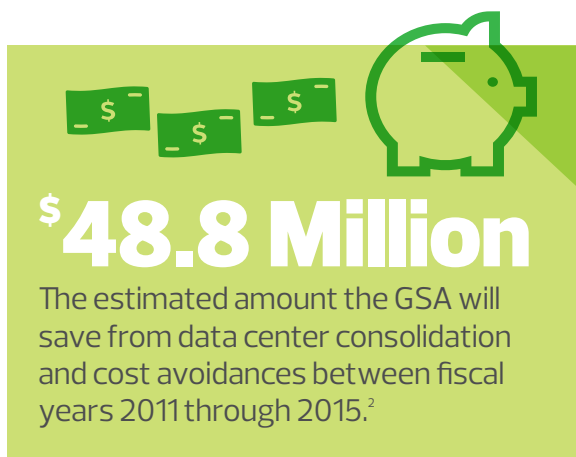
Agencies spend **25 percent of IT budgets solely on storage** — a sobering number considering data is expected to grow 800 percent over the next five years.

See how we can help you get the most out of your data center and your dollars. Visit **CDWG.com/storagevirtualization**

Sources: [1]datacenterjournal.com, "Data Erasure in Virtualized Environments," December 2014 [2]gao.gov, "Data Center Consolidation, Reporting Can Be Improved to Reflect Substantial Savings," September 2014 [3]fedtechmagazine.com, "Big Data Puts Agencies at Storage Crossroads," February, 2015

NetApp
CDWG.com/netapp

NetApp® FlexPod® Solutions
Reduce deployment time, project risk and the cost of IT
CALL FOR PRICING

- Speed deployment of organizational applications
- Get validated designs for VMware®, Microsoft®, Oracle®, SAP® and Citrix® apps
- Deploy the latest all–flash and software–defined data center solutions
- Scale your IT architecture up or out for future growth
- Reduce TCO more than with converged infrastructure alternatives

nimblestorage
CDWG.com/nimble

Nimble Storage CS–Series Adaptive Flash Storage Systems
Flash–optimized from the ground up (CS235 array — high performance)
CDW 3718488
CALL FOR PRICING

- Accelerated performance for higher throughput/IOPS and submillisecond latencies
- Higher storage efficiency — reducing the storage footprint needed by 30 to 75 percent
- Nondisruptive scaling to fit changing application needs through increased performance or capacity, or both
- Maximized data and storage availability with integrated data protection and disaster recovery
- Simplified storage management and reduced day–to–day operational overhead
- Store and protect critical applications such as Microsoft® Exchange, Microsoft SQL Server®, server virtualization, database and virtual desktops

hp
CDWG.com/hp

intel inside™
Xeon®

Hard drives sold separately

HP ProLiant DL180 Gen9 Server
Designed with the right balance of expandability, performance, reliability and manageability
CDW 3466987
$**1355**.59

The HP ProLiant DL180 Gen9 Server delivers an optimized 2U server, all in a new, compact chassis.

- Six–Core Intel® Xeon® E5–2603v3 processor (1.60GHz)
- Memory: 8GB std., 256GB max.
- Hard drive: none ship std.

vmware
CDWG.com/vmware

vmware®

VMware vCloud® Air™ Disaster Recovery
A Recovery as a Service offering by VMware
CALL FOR PRICING AND LICENSING OPTIONS

VMware vCloud® Air™ Disaster Recovery is a new Recovery as a Service solution that introduces native cloud–based disaster recovery capabilities for VMware vSphere® virtual environments. Built on VMware's hypervisor–based replication engine, vSphere® Replication™, and new integration support with vCloud Air Disaster Recovery includes:

- Self–service disaster recovery protection for virtual machines
- Recovery point objectives (RPO) from 15 minutes to 24 hours
- Automated failover testing, planned migrations and recovery
- Elastic cloud compute and storage capacity
- Support for offline data seeding
- Private leased line network option
- Flexible failover testing

Nutanix and CDW·G

The Nutanix Virtual Computing Platform is a web–scale converged infrastructure solution that consolidates the server tier and the storage tier into a single, integrated appliance. It offers a radical reduction in costs, and is easy to deploy and manage.
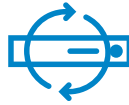
A SINGLE NUTANIX APPLIANCE REPLACES ENTIRE RACKS WORTH OF LEGACY EQUIPMENT.

Source: EurotechComputers, youtube.com/watch?v=fcV8w4oqCCQ, "Nutanix in 2 Minutes," [Video], May 29, 2014

NUTANIX. CDWG.com/nutanix

Nutanix™ NX–1450 Virtual Computing Platform
Converged infrastructure for remote and branch offices
CDW 3075609
CALL FOR PRICING

- Standardize branch office infrastructure to ease IT headaches
- Eliminate SAN storage and simplify IT infrastructure
- Run any VM on a turnkey appliance in less than 30 minutes
- Deliver continuity of operations with built–in replication and backup
- Remotely manage all locations with simplified workflows from a single interface

Nutanix NX–1350   CDW 3075608

Nutanix NX–3450 Virtual Computing Platform
Converged infrastructure for enterprise data centers
CDW 3075628
CALL FOR PRICING

- Provide server and storage in a single 2U appliance
- Run any VM on a turnkey appliance in less than 30 minutes
- Eliminate SAN storage and simplify IT infrastructure
- Deliver up to 80% savings in space and power
- Dual–Port 10GbE and 1x 1GbE RJ45 (IPMI)

arcserve® CDWG.com/arcserve

Arcserve® UDP Recovery Appliance
Unique backup and recovery solution
CDW 3611200
CALL FOR PRICING

- Complete and cost-effective data protection appliance, featuring Assured Recovery
- Simplify disaster recovery activities
- Leverages a combination of SAS and SSD drives for optimized performance
- Unified management console, with simple plan-based data protection policies
- Host-based, agentless backup for vSphere® and Hyper-V®
- Local/remote virtual standby, BMR and tape backup option

Symantec. CDWG.com/symantec

Symantec™ NetBackup™ 7.7
The future of enterprise-class data protection is here
CALL FOR PRICING

Symantec™ NetBackup™ 7.7 reduces the staggering complexity of enterprise data protection, outpaces the relentless growth of the data center, and increases the agility IT needs to transform from traditional cost center to service-oriented enabler. Enterprises trust Symantec.

- Expanded support for cloud storage providers, including Google Nearline, HDS and Cloudian
- Enhanced cloud backup and restore performance
- VMware vSphere® web client and Microsoft® SCVMM plug-ins
- Intelligent policies for Hyper-V® and SQL Server®

SEAGATE CDWG.com/seagate

Seagate® 8-bay Rackmount NAS
Great for backing up PCs in one central location
32TB CDW 3151540
$5384.99

- 1U rack with eight hot-swappable 3.5" drives doubles your storage capacity in the same footprint
- A powerful 2.3GHz Dual-Core Intel® processor delivers incredible file transfer performance of up to 200MBps
- Included Wuala™ cloud service and apps for seamless, secure collaboration and anywhere access from most devices
- Centralized backup for PCs, plus Time Machine® support for Mac® computers

EMC² ISILON CDWG.com/isilon

EMC® Isilon® X400 Scale-out NAS
Flexible and comprehensive storage
36-bay, 4U rack, 144TB system capacity, 10GbE

34.8TB CDW 2910961
CALL FOR PRICING

- Provides the right balance between large capacity and high-performance storage
- Scale-out clustered architecture reaches capacities over 20PB
- Designed for virtualized infrastructure environments, analytics and medical imaging
- SSD technology for file-system metadata and file-based storage workflows
- EMC® Isilon® X-Series significantly accelerates namespace-intensive operations

THE IMPORTANCE OF NETWORK VISIBILITY

Advanced monitoring tools can deliver a dynamic picture of network infrastructures and the devices connected to them.

A recent study by Riverbed revealed that federal IT leaders have far less visibility into their networks than they would like. This lack of visibility makes it much more difficult to identify a variety of problems quickly and accurately. This, in turn, means that problems continue for much longer than they would otherwise, which increases the impact to the agency in terms of costs, lost productivity for employees and other problems.

The good news is that technologies and security architectures can be utilized to increase network visibility, as well as to gain greater control over network reliability, performance and security.

Why IT Departments Lack Network Visibility

Monitoring a network, and the assets connected to that network, used to be a relatively simple matter for most agencies. The organization had one main network, and its key infrastructure components were in a small number of well-secured locations, such as enterprise data centers in federal buildings. Most users had assigned desktop computers, also located within the agency's facilities. And for users with agency-issued notebook computers, remote access

to a small number of IT resources was possible through a single virtual private network (VPN) entry point. Cell-phones did not provide robust data services, so they were irrelevant because they didn't connect to agency networks.

Today, the entire situation has become much more complicated. The networks themselves have become increasingly complex for three main reasons. The first is the shift to cloud-based services. A single agency may use several cloud service providers — for example, to have access to particular applications — but these networks cannot be monitored by the agency's existing tools and techniques. A second reason is the incredible rise of mobility. Users are working from many locations, employing notebooks, smartphones and tablets, and they are demanding — and often getting — access to a wide variety of agency resources from these devices. VPNs are still used for many notebooks, but most mobile devices are accessing agency resources through public-facing servers, and not a VPN. Third, the popularity of bring-your-own-device arrangements, where devices that are not controlled by the agency are allowed to connect to its resources, has greatly increased the complexity of federal networks.
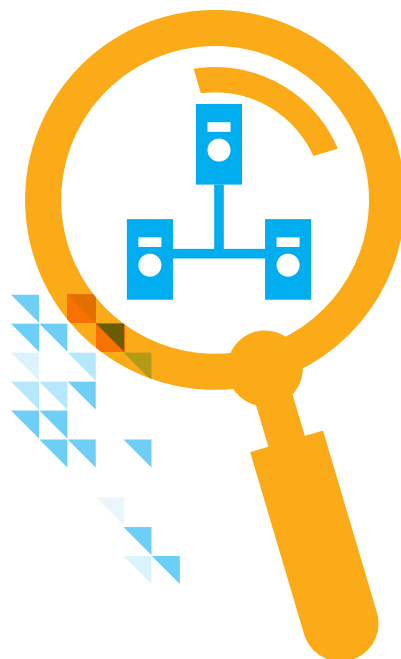
Serious Concerns

The lack of visibility into an agency's networks can lead to significant problems regarding security, performance and reliability. For example:

· Agency IT administrators may be unable to automatically detect many network infrastructure failures and performance problems. This may cause extended disruptions to network, application and data availability.

· The agency may not be able to detect unauthorized devices attached to its networks. Such devices are usually not in compliance with security policies, and they may have already been compromised by attackers.

· The agency may be unable to monitor the contents of traffic passing over its networks. IT administrators may not even know what types of traffic are being carried on the network, let alone the nature of this traffic, whether it is benign, unnecessary or malicious. An attacker could be stealing vast quantities of sensitive data over the agency's own networks undetected.

The benefits of having robust visibility into agency networks logically follow from these problems. The agency can detect failures, performance issues, some

compromises and other adverse situations much more quickly, usually without human intervention. In turn, this enables immediate automated responses, which minimizes the negative effects of these problems.

In terms of cost, increasing network visibility can actually provide substantial savings. A surprising finding of the Riverbed study was that by improving network visibility, downtime for networks and applications can be sharply reduced. The resulting increase in productivity can more than make up for the cost of implementing and operating network visibility–enabling technologies. So, although nearly half of the federal IT leaders surveyed by Riverbed said they do not think that they have enough funding to fix their network visibility problems, it's possible that the solutions would pay for themselves.

Increasing Visibility

Agencies generally cannot fix all of their network visibility problems with a single change. Improving visibility usually requires a combination of new monitoring technologies and adjustments to existing security architectures.

Network monitoring tools and their cloud service–based counterparts provide IT administrators with highly granular and dynamic visibility into their network infrastructure and the devices (such as servers and clients) connected to these networks. The visibility–related capabilities offered by network monitoring tools vary widely, but common features include:

· Automatic identification of network outages and performance reductions, as well as their causes

· Dynamic mapping of the entire network infrastructure, including the identities of all devices on it

· Monitoring of individual applications to identify application performance problems, then determine if each problem is being caused by the application itself or by the underlying network infrastructure

· Estimation of when particular components of the network infrastructure should be upgraded or replaced based on network usage patterns

· Automatic alerts when undesirable conditions are detected

Some network monitoring tools can also automatically correct the problems they find. An agency that does not have an efficient means of acting on identified problems will not benefit as much from improving its network visibility. Such agencies may need to deploy more comprehensive network management tools that have the ability not only to monitor networks and connected devices, but also to automatically perform specific actions when problems occur. These actions could include severing an individual network connection, blocking a bandwidth–consuming denial–of–service attack or reconfiguring a router.

Simply adding network monitoring tools is generally not sufficient to solve

"In terms of cost, increasing network visibility can actually provide substantial savings. A surprising finding of the Riverbed study was that by improving network visibility, downtime for networks and applications can be sharply reduced."

an agency's entire network visibility problem. IT leaders usually have to adjust their security architectures as well. The primary reason for this is to take into consideration the use of encryption to protect the confidentiality of network communications. If these technologies are deployed to standard network locations, such as the edge of the enterprise perimeter, such communications cannot be monitored and analyzed by network monitoring tools, network–based intrusion detection systems or other security technologies that monitor network traffic for suspicious activity. Rather, these technologies must be deployed to locations where the traffic is unencrypted. If the traffic is encrypted from end to end, then host–based versions of these technologies should be used on the sending and receiving hosts instead.

By ensuring that robust network monitoring technologies are deployed to the proper locations within the agency, IT administrators can greatly increase their network visibility, leading to a sharp reduction in the negative effects of outages, performance issues and some network–based attacks. ◼

To learn more about the latest trends and technologies in networking, read CDW's Tech Insights Guide "Gigabit Networking: Connect with the Future."

27%

The percentage of federal technology leaders who said they are able to find the root cause of network performance issues quickly

Source: Riverbed Technology, "The Federal Network Visibility Crisis: Get to Know Your Apps," May 2015

BRINGING SHADOW I.T. INTO THE LIGHT

The right policies and technologies can help agencies gain control over unauthorized IT products and services.

"Shadow IT" sounds scary, and for many agencies, it is. The term refers to when individual users, teams or other entities within an organization acquire IT products and services themselves, without involving the IT department or following organizational policies and procedures. Shadow IT has been around for a long time, but its use has exploded in recent years with the increased adoption of cloud–based Software as a Service (SaaS) applications. These applications can be used on a subscription basis at low cost.

A recent report from Skyhigh Networks reveals some startling numbers. The average public–sector leader believes that his or her organization uses 60 to 70 shadow IT solutions, but in reality the number is 10 times that. Based on this revelation, federal IT leaders must face three important questions:

- Why is shadow IT so commonplace in federal agencies?
- What security concerns arise with shadow IT?
- How can agencies mitigate these concerns?

Reasons for Shadow IT

One of the main reasons that shadow IT has taken root at federal agencies is that users have immediate needs that are not met by the IT department. This may be due to slow agency procurement processes and security requirements that are perceived as being too strict. Cost is another driver of shadow IT. Some users may find it less expensive to directly acquire cloud services instead of going through an agency's IT department. Further, employees are increasingly demanding access to the hardware, operating systems and especially applications that they prefer, instead of accepting tools provided by the IT department. The bring–your–own–device movement is a great example of this.

Security Concerns with Shadow IT

Agency IT leaders have a wide variety of security concerns related to shadow IT. At the most basic level, many IT administrators are unable to determine whether a particular SaaS application is even a possible candidate for the agency to use. For example, an application may be partially or wholly hosted in another country, which could cause a serious compromise of privacy and security. The terms of service of any cloud agreement also can raise significant concerns. A user acquiring a SaaS application is highly unlikely to conduct a formal review of its terms of service, but such a review might determine that the SaaS provider, law enforcement agencies or other parties have the right to monitor and access the users' data, which could lead to security and privacy violations.

A higher–level concern is that shadow IT users are unlikely to conduct a risk assessment before acquiring and using these services. Without assessing risk, IT leaders have no way to determine what vulnerabilities are present and how they should be mitigated to bring risk down to an acceptable level. SaaS providers vary greatly with regard to the strength of their security controls. Some providers assume that users' IT departments will take care of security, so their own security measures are minimal. They may not encrypt data at rest, for example. This allows the SaaS provider to keep prices lower, but it puts users' data at much higher risk of compromise. Users who

58%

The percentage of organizations that have a cloud security awareness training program for users or plan to create one.

Source: Cloud Security Alliance, "Cloud Adoption Practices & Priorities Survey Report," January 2015

acquire shadow IT services are also unlikely to implement the procedural controls necessary to protect data, such as ensuring that when a user leaves the organization, his or her sensitive data stored in shadow IT is scrubbed and the user's access to all shadow IT applications is terminated.

A final security concern with shadow IT regards how agency use of a specific cloud service may be affected by federal regulations. For some regulations, simply storing affected data in a public cloud is a compliance violation, regardless of the security measures in place. More broadly, the use of shadow IT is unlikely to support compliance efforts because shadow IT usage is often unaudited, unmonitored and insufficiently secured.

Mitigating Shadow IT Security Concerns

Users who have a job to do will often go to great lengths to ensure that it gets done, even if this means using shadow IT solutions that violate agency and compliance requirements and put sensitive data at grave risk of compromise. IT departments cannot stop all shadow IT use, so security team members should strive to become trusted advisers to their user community instead of the shadow IT police. This allows the security team to educate users on security policies, procedures, technologies and risks, as well as to guide them in ensuring that their IT acquisitions are properly secured. Increasing security awareness throughout the organization typically increases buy-in to the security program as well. This is not meant to imply that IT departments should take a hands-off approach to shadow IT; on the contrary, it is essential that they be involved in both proactive and reactive ways.

IT departments should identify existing shadow IT SaaS usage through an audit. Tools and services are available that can identify

which cloud services are being used by an agency. Some existing enterprise security technologies, such as next-generation firewalls (NGFWs) and web security gateways, can also identify SaaS usage. Agencies can also acquire cloud-application control systems, which closely monitor all SaaS usage, including details about the applications being utilized and the actions of each user. This allows for granular auditing and access control of SaaS usage throughout the enterprise.

Regardless of the method used, identifying SaaS usage allows the IT department to assess the scope of its shadow IT. The IT department can then act to assess risk for its shadow IT and determine any changes necessary to bring risk to an acceptable level. This may simply involve adding some

"A higher-level concern is that shadow IT users are unlikely to conduct a risk assessment before acquiring and using these services. Without assessing risk, IT leaders have no way to determine what vulnerabilities are present and how they should be mitigated to bring risk down to an acceptable level.

security controls to existing shadow IT. For example, an agency may ensure that before files can be uploaded to a file-sharing service, they are first encrypted. The organization may also use NGFWs, web security gateways or cloud-application control systems to disable the riskiest functions for certain SaaS applications, or to block all use of particular SaaS applications because they cannot be secured sufficiently. Other common security

controls include establishing auditing and security monitoring for SaaS applications so that security incidents and other problems can be identified and handled quickly to minimize damage.

The IT department should be proactive with shadow IT by reducing the need for it. Many shadow IT acquisitions happen because the agency doesn't provide capabilities deemed necessary by the user community, such as advanced collaboration and file-sharing capabilities. Agencies should closely monitor and evaluate new and emerging technologies that may be of value to their user communities. IT leaders should then select one or more SaaS applications that are officially approved to provide these services; this helps to drive users to approved options.

Another way in which the security of shadow IT can be proactively improved is by the acquisition of an enterprise identity and access management solution for SaaS use. Such a solution can enable single sign-on to many SaaS applications. This takes a great password management burden off users and ensures that the individual SaaS passwords behind the scenes are unique, strong and regularly changed. Meanwhile, each user has only a single password to remember, often in conjunction with another authentication measure to provide multifactor authentication.

Before taking any other measures, every agency should have a SaaS usage policy, which establishes what users can and cannot do. Every user should be educated about this policy. Ultimately agencies have to put more trust their employees, but along with this trust comes responsibility. Users must be made aware of the consequences of their actions, as well as the harm that can come to the organization and to users themselves as a result of irresponsible actions that lead to a breach of sensitive data through improper shadow IT usage. ∎

To learn more about cloud security, check out CDW's Cloud Security Technology Insights Guide.

NEXT STEPS FOR WIRELESS NETWORKS

Your wireless infrastructure allows users to take the office with them wherever they go. The wireless network provides staff and guest workers with untethered access to voice, video, data and applications regardless of their physical location.

With the influx of mobile devices and increase in Wi–Fi connections, organizations are already starting to see a paradigm shift to "wireless by default" and "wired by exception."

25%
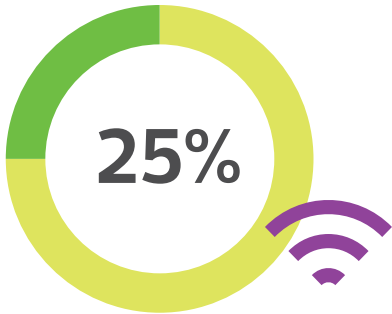
The percentage of installed Wi–Fi access points that are compatible with the new 802.11ac wireless standard.[1]

12%
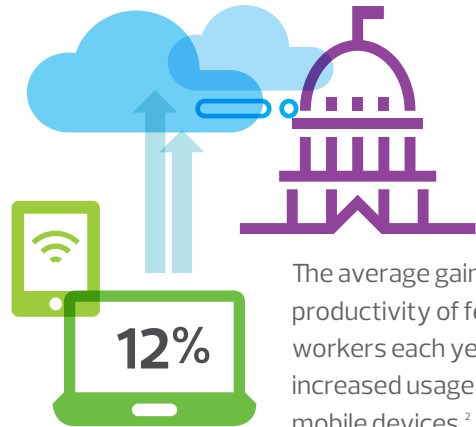
The average gain in productivity of federal workers each year from increased usage of mobile devices.[2]

16%
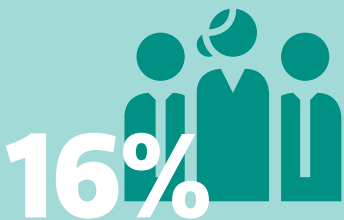
The percentage of IT decision makers who plan to upgrade their wireless infrastructure in the next 12 months.[3]

81%

Growth in wireless data traffic annually.[3]

If you're ready to upgrade your wireless network, we have everything you need to meet your hardware, management and security needs. Learn more at **CDWG.com/network**

Sources: [1]infonetics.com, "WLAN market report," December 2014 [2]dupress.com, "Gov on the Go," February 2013
[3]CDW, *Surveying Your Network: A CDW Advisory Board Decision Maker Study*, July 2014

CDWG.com/cisco

Cisco® Aironet® 1700 Series Access Points
Dual–band APs with 802.11ac
CDW 3499207

$**401**.98

The Aironet® 1700 Series meets the growing requirements of wireless networks by delivering better performance than 802.11n and providing key RF management features for improved wireless experiences. It supports 802.11ac Wave 1 standard capabilities. That includes a theoretical connection rate of up to 867Mbps. The added throughput lets you stay ahead of growing bandwidth requirements.

• More wireless clients associate with the network
• Users tap into bandwidth–heavy multimedia applications
• Mobile workers increasingly use multiple Wi–Fi® devices

CDWG.com/aruba

Aruba® IAP–205 Access Point
Bringing 802.11ac to the masses
CDW 3462003

$**625**.50

Compact and cost–effective wireless APs for maximizing mobile device performance in medium–density environments.

• 802.11ac, 2x2 MIMO, 867Mbps per radio
• Two dual–band radios
• Four integrated omnidirectional antennae or external detachable dual–band antennae
• Installs quickly and easily on any ceiling or wall

CDWG.com/fortinet

Fortinet® FortiGate® 100D with One–year 24/7 FortiCare
Delivers consolidated network security and access
CDW 2900891

$**2829**.90

• High port density for maximum flexibility and scalability
• Application control with identity–based policy enforcement for complete content protection
• Strong authentication options for policy compliance

CDWG.com/netgear

NETGEAR® ProSAFE® Hi–Cap Wireless Controller WC9500
Management without recurring license fees: pay as you grow
CDW 3608484

$**4367**.05

• Highly scalable 10 Gigabit connectivity — supports up to 200 access points and 12,000 concurrent clients per controller
• Enterprise–grade and feature–rich deployment solutions: Layer 2/3 seamless roaming, UFast™ AP discovery, distributed and local forwarding, supports ProSAFE® APs
• Warranty and support: ProSAFE® lifetime hardware warranty, next business day hardware replacement and 24/7 basic hardware technical support

Cisco <u>and</u> CDW·G

**When it comes to networking, it's not just what you know.
It's who you know.**

That's why we partner with industry leaders like Cisco. With technologies spanning the entire networking spectrum, Cisco's Enterprise Networking helps organizations connect seamlessly and securely. And with years of experience in Cisco deployments, CDW·G has the experts and the expertise to make them work for you.

CDWG.com/cisco

Cisco® Catalyst® 3650 Series 24–port Switch
Support BYOD/mobility and offer a variety of performance, security and operational enhancements
CDW 3328742

$**2479**.78

- Optional Cisco® StackWise®–160 technology to provide scalability and resiliency with 160Gbps of stack throughput
- Support for Cisco ONE™ Enterprise Networks Architecture with the UADP ASIC for openness, programmability and investment protection
- Cisco IOS® XE Software support for IPv4 and IPv6 routing and multicast routing
- Modular QoS, Flexible NetFlow (FNF) version 9 and enhanced security features

Cisco ASA 5512–X Adaptive Security Appliance
ASA 5512–X with FirePOWER® Services, 6GE data, AC, 3DES/AES, SSD
CDW 3511958

$**2905**.71

Meet the adaptive, threat–focused next–generation firewall (NGFW) designed for a new era of threat and advanced malware protection.

- Enterprise–class stateful firewall with remote access VPN and advanced clustering for highly secure, high–performance access and high availability to help ensure operational continuity
- Granular Application Visibility and Control (AVC) supports more than 3000 application–layer and risk–based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness
- Provides highly effective threat prevention and full contextual awareness of users, infrastructure, applications and content to detect multivector threats and automate defense response

Cisco Aironet® 2702i Controller
The 2700 series supports high–performing spectrum intelligence
CDW 3322579

$**606**.47

- Offers advanced features
- High–density experience (HDX) delivers outstanding performance in dense BYOD environments
- Integrated 802.11ac radio supports 3x4 MIMO with three spatial streams
- The fourth "receive" antenna provides exceptional performance

riverbed

CDWG.com/riverbed

Riverbed® SteelHead™ CX 570
WAN and application optimization
CDW 3331783
CALL FOR PRICING

An advanced optimization solution that accelerates the transfer of data and applications over your hybrid network.

• Increases application and data transfer performance up to 100x

• Reduces bandwidth utilization by up to 95%

• Accelerates both replication and backup from the branch — or between data centers — by 10x or more

• Delivers application acceleration in nearly any cloud environment

• SteelHead™ CX is available in a variety of form factors/models, including appliances, virtual software and cloud instances

---

hp

CDWG.com/hp

HP 2920–24G–POE+ Switch
Flexibility, scalability and low TCO
CDW 3540922
CALL FOR PRICING

The HP 2920 Switch Series is a managed 10/100/1000 switch that delivers flexibility, scalability and low total cost of ownership with a robust feature set and lifetime warranty.

These switches deliver future–proof unified access and software–defined networking (SDN) capabilities:

• OpenFlow enables an SDN–ready infrastructure and investment protection

• Stacking delivers pay–as–you–grow economics and operational simplicity

• PoE+ delivers 30W per port for access points, cameras and conference phones

• Energy–Efficient Ethernet and HP ASICs lower power consumption

---

CISCO Gold Partner

CDWG.com/cisco

Cisco® ISR 4331
Revolutionizes WAN communications in the enterprise branch
CALL FOR PRICING

With new levels of built–in intelligent network capabilities and convergence, the Cisco® ISR 4331 specifically addresses the growing need for application–aware networking in distributed enterprise sites. These locations tend to have lean IT resources. However, they often also have a growing need for direct communication with both private data centers and public clouds across diverse links, including Multiprotocol Label Switching (MPLS) VPNs and the Internet.

Cisco 4000 Family ISRs provide you with Cisco Intelligent WAN (IWAN) software features and a converged branch infrastructure. Along with exceptional throughput, these capabilities form the building blocks of next–generation branch–office WAN solutions.

---

ca technologies

CDWG.com/ca

ca technologies
®

Monitor up to 30 devices — at no cost; visit CDWG.com/CA to download Unified Infrastructure Management Snap[1]

CA® Unified Infrastructure Management
Get unified coverage of the IT systems and cloud services that matter to your organization

CALL FOR PRICING AND LICENSING OPTIONS FOR MONITORING MORE THAN 30 DEVICES

CA Unified Infrastructure Management is an IT monitoring platform that provides scalable, easy–to–use and resilient monitoring capabilities. CA Unified Infrastructure Management can help enable your organization to proactively monitor on–premises and cloud–based infrastructures — all within a single code base.

Key benefits/results:

• Automatic deployment and speed time to value

• Accelerate problem resolution — and proactively prevent issues

• Easily add additional service offerings, and commit to higher levels of service

• Optimize operational efficiency

---

[1]No–cost download of CA Unified Infrastructure Management Snap for up to 30 devices is offered by CA and subject to the terms provided by CA; offer details can be obtained by going to cdwg.com/ca and clicking on the CA Unified Infrastructure Management Snap banner or calling your CDW·G account manager

29

Adobe and CDW·G

Adobe Acrobat desktop software is now combined with the new Acrobat DC mobile app and Document Cloud services to give users a more efficient way to work from anywhere. Now your organization can build smarter document workflows and help ensure document security across devices.

Adobe

CDWG.com/adobe

Adobe® Acrobat® DC
The complete PDF solution for working anywhere
Multiple platforms
CDW 3663542
$**233**.41

All-new Adobe® Acrobat® DC with Adobe Document Cloud services is the complete PDF workflow solution, combining Acrobat desktop software with the new Acrobat DC mobile app and Document Cloud services to inspire a mobile, connected workforce.

Adobe Photoshop® CC
A whole new experience in digital design
Per User 12–month Subscription

Multiple platforms
CDW 3245460
$**246**.37

Create production-quality designs and other images on your mobile devices as well as your desktop. Get immediate access to all your assets — including Adobe Stock images — from right inside Photoshop®. See how the latest release helps you quickly turn any inspiration into incredible work with great new features for print and graphic design, web and app design, and photography.

CITRIX CDWG.com/citrix

CITRIX
XenMobile

Citrix® XenMobile® MDM
Mobile device management and beyond
CALL FOR PRICING

Citrix® XenMobile® is a comprehensive solution to manage mobile devices, apps and data. Users have single–click access to all of their mobile, SaaS and Windows® apps from a unified app store, including seamlessly integrated email, browser, data sharing and support apps. IT gains control over mobile devices with full configuration, security, provisioning and support capabilities. Flexible deployment options give IT the choice to manage XenMobile in the cloud or on–premises.

- Configure, secure, provision and support mobile devices with MDM
- Mobile app management with a large ecosystem of apps
- Enterprise–class email, browser and document sharing apps
- Multifactor single sign–on

---

airwatch by **vmware** CDWG.com/airwatch

AirWatch® by VMware® Enterprise Mobility Management
Your single solution to control, manage and secure mobile workspace, devices, apps, content, email and browsing
CALL FOR PRICING

AirWatch® by VMware® enables government agencies with advanced data loss prevention capabilities that include blocking access to email, native browsers, applications and content, multifactor authentication, automated compliance engine and noncompliance remediation, network access control, wiping a device of organizational data if a threat is identified, and restricting email forwarding.

To learn more, visit CDWG.com/airwatch

Good

Good

Good Enterprise Mobility Management Suite
Comprehensive mobile device and app management, security and productivity
CALL FOR PRICING

- All–in–one app for users delivers secure email, contacts, calendar, files and browsing for increased productivity
- Simple web–based console for IT enables mobile device management (MDM) and mobile application management (MAM)
- Customizable enterprise app store with consumer–like ratings and reviews
- Cross–platform consistency across iOS, Android™ and Windows®
- Cloud–hosted, on premise or hybrid solutions securely mobilizes your investment in Microsoft® Exchange, Office 365™ and Lync®
- Unlimited devices per user

MaaS360® by IBM CDWG.com/fiberlink

MaaS360®
by IBM

MaaS360® Enterprise Mobility Management
Deploy, secure and support smartphones and tablets
CALL FOR PRICING

MaaS360® by Fiberlink, an IBM® company, delivers a comprehensive enterprise mobility management platform to secure and support users, devices, emails, apps, documents and web access. Recognized as a leader in the Gartner Magic Quadrant for Enterprise Mobility Management (EMM) Suites, MaaS360 allows organizations to fully embrace mobile technology and quickly scale deployments.

31

Maximize Your Productivity

Change how your organization interacts, learns, connects, collaborates and performs with the latest tablets from CDW·G. Our mobility specialists can help you find the devices that meet the needs of your agency.

Learn more about our comprehensive approach to mobility at CDWG.com/mobility

---

SAMSUNG CDWG.com/samsung

Samsung® Galaxy Tab® Active
Toughness and portability
CDW 3520719

$539.99

- Android™ 4.4 (KitKat)
- 16GB flash memory
- Front and rear cameras
- 8" TFT active matrix display
- Resistant to dust and moisture

TOSHIBA CDWG.com/toshiba

(intel)

Toshiba Encore™ WT10
Everything you need for work and play
CDW 3438125

$254.35

- Quad–Core Intel® Atom™ Z3735G processor (1.33GHz)
- Memory: 1GB/32GB SSD
- 10" touch–screen display
- Intel® HD Graphics
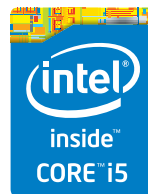- Windows® 8.1

FUJITSU CDWG.com/fujitsu

(intel inside™ CORE™ i5)

Fujitsu LIFEBOOK® T725
The 12.5" LIFEBOOK® T725 is a two–in–one comprising the best of a notebook and a tablet
CDW 3626066

$1339.99

- 5th generation Intel® Core™ i5-5200U processor (2.20GHz)
- Memory: 8GB/500GB hard drive
- 12.5" touch–screen 1366x768 (HD)
- Intel® HD Graphics 5500
- Windows 8 Pro 64–bit/Windows 7 Pro 64–bit downgrade

Authorized Reseller
CDWG.com/apple

Apple® iPad Air® 2
iPhoto®, iMovie®, GarageBand®, Pages®, Numbers®
and Keynote® apps included
CDW 3519198
CALL FOR PRICING

• 9.7–inch LED–backlit display

• A8x chip

• Built–in Wi–Fi® (802.11a/b/g/n/ac)

• Up to 10 hours of battery life¹

• 8MP iSight® camera with 1080p HD video recording

• FaceTime® HD camera

• iOS 8 and iCloud

• Available in space gray or silver

Apple iPad mini™ 3
Touch ID fingerprint sensor
CDW 3519203
CALL FOR PRICING

• 7.9–inch Retina® display (diagonal)

• A7 chip

• 5MP iSight camera

• FaceTime HD camera

• 802.11n Wi–Fi with MIMO

Apple iPad Air 2
iOS 8 and iCloud
CDW 3519196
CALL FOR PRICING

• 9.7–inch LED–backlit display

• A8x chip

• Built–in Wi–Fi (802.11a/b/g/n/ac)

• Up to 10 hours of battery life¹

• 8MP iSight camera with 1080p HD video recording

• FaceTime HD camera

• iPhoto, iMovie, GarageBand, Pages, Numbers
  and Keynote apps included

Apple iPad mini 3
iPhoto, iMovie, GarageBand, Pages, Numbers
and Keynote apps included
CDW 3519194
CALL FOR PRICING

• 7.9–inch LED–backlit display

• A5 chip

• Built–in Wi–Fi (802.11a/b/g/n)

• Up to 10 hours of battery life

• 5MP iSight camera with 1080p HD video recording

• FaceTime HD camera

• iOS 7 and iCloud

• Available in space gray or silver

Microsoft

intel inside™ CORE™ i5

Microsoft® Surface™ 3
Ultraportable, yet highly powerful
CDW 3674365

$**549**.00

- Intel® Core™ Atom™ x7–Z8700 processor (1.60GHz)
- Memory: 4GB RAM/64GB SSD
- 10.8" ClearType Full HD Plus display
- Intel® HD Graphics
- Windows® 8.1 Pro

Microsoft Surface Pro 3
With a 12" display, Surface™ Pro 3 has the power of a notebook in a lightweight, versatile form
CDW 3368322

$**999**.00

- 4th generation Intel® Core™ i5–4300U (1.90GHz)
- Memory: 4GB/128GB SSD
- 12" ClearType® Full HD touch screen
- Intel® HD Graphics 4400
- Windows 8.1 Pro

Kensington®

Kensington® Soft Carrying Case
Protective sleeves for 10" tablets
CDW 2631481

$**11**.99

- Neoprene sleeve protects and cushions your tablet
- Soft fleece lining keeps tablet safe from scratches
- Zippered outer pocket is ideal for carrying accessories
- Easy access through security checkpoints
- Deep stitched accent delivers professional style

GRIFFIN

Griffin Technology® Survivor Escape for Surface Pro 3
Ultrasleek looks with enhanced impact protection for your Microsoft Surface tablet
CDW 3730390

$**39**.99

- Tough TPE surrounds entire Surface tablet (including kickstand), protecting it from bumps and impacts
- Fully–integrated stand protection lets you use the Surface kickstand in all positions
- Enhanced corner protection keeps Surface tablet safe from damage caused by drops
- Sleek, lightweight design fits easily into a messenger bag or backpack to use anywhere

Panasonic <u>and</u> CDW·G

In situations that would damage conventional computers, rugged Toughbook computers keep performing. As a result, users eliminate costly repairs or replacements and avoid wasting time to recover lost work. The bottom–line results are compelling: lower total cost of ownership (TCO) and greater return on investment (ROI) over the computer's useful life.

Find yours at CDWG.com/panasonic

Panasonic TOUGHBOOK CDWG.com/panasonic

intel inside™ CORE™ i5

Panasonic Toughpad® FZ–G1
The fully rugged Toughpad® FZ–G1 tablet
is ideal for field workforces in outdoor scenarios
CDW 3416692

$2417.99

- 4th generation Intel® Core™ i5–4310U processor (2.0GHz)
- Memory: 8GB/128GB SSD
- 10.1" touch–screen display
- Bluetooth®
- Intel® HD Graphics 4400
- Windows® 8.1 Pro 64–bit / Windows 7 64–bit downgrade

Panasonic Toughpad FZ–G1
Engineered to withstand the hard knocks,
drops and spills of real life on the road
CDW 3207687

$2995.99

- 4th generation Intel® Core™ i5–4302Y processor (1.60GHz)
- Memory: 8GB/256GB SSD
- 7" touch–screen display
- Intel® HD Graphics 4200
- Windows 8.1 Pro 64–bit

Panasonic Toughbook® C2
Combine desktop performance with advanced mobility features
CDW 3228941

$2284.99

- 4th generation Intel® Core™ i5–4300U processor
- Memory: 4GB/500GB HDD
- 12.5" touch screen 1366x768 (HD)
- Hands–free ergonomic strap
- Windows 8.1 Pro / Windows 7 Pro downgrade

Mobility Management Portal

Integrate, control and simplify day–to–day administration with our customizable and flexible web–based administrative tool. Our unique portal delivers monthly subscription services that manage security, policy and compliance across your mobile user base.

Learn more at CDWG.com/mobility

SAMSUNG BUSINESS   CDWG.com/samsung

Samsung® ATIV Book 9 Plus 940X3KI
Provides quick boot–up and wake–up for instant accessibility
CDW 3587413
$**1699**.99

- 4th generation Intel® Core™ i7 550U processor (2.40GHz)
- Memory: 8GB/256GB SSD
- Intel® HD Graphics 5500
- 13.3" touch–screen HD LED–backlit display
- Windows® 8.1 64–bit

(intel inside™ CORE™ i7)

FUJITSU   CDWG.com/fujitsu

Fujitsu LIFEBOOK® E734 Tablet PC
Provides an exceptional mix of versatility and mobility
CDW 3677291
$**1039**.99

- 4th generation Intel® Core™ i5–4210M processor (2.60GHz)
- Memory: 4GB/500GB HDD
- Intel® HD Graphics 4600
- 13.3" 1366x768 (HD)
- Windows 8 Pro 64–bit/Windows 7 Pro 64–bit downgrade

(intel inside™ CORE™ i5)

TOSHIBA
Leading Innovation >>>   CDWG.com/toshiba

Toshiba Portégé® Z20T
Designed to be an Ultrabook™ when you need it and a tablet when you want it
CDW 3591540
$**1208**.99

- 5th generation Intel® Core™ M–5Y51 processor
- Memory: 4GB/128GB SSD
- 12.5" touch–screen LED screen
- Intel® HD Graphics
- Windows 8.1 Pro/Windows 7 Pro downgrade

(intel inside™ CORE™ m)

acer CDWG.com/acer

intel inside CORE i5

Acer TravelMate® P645 Dockable Ultrabook™
Keyboard is designed to withstand spills, scratches and more
CDW 3365133

$1009.99

- 4th generation Intel® Core™ i5–4200U processor (1.60GHz)
- Memory: 8GB/128GB SSD
- 14" HD LED–backlit display
- AMD Radeon™ HD 8750M
- Windows® 8.1 Pro 64–bit / 7 Pro 64–bit downgrade

Targus CDWG.com/targus

Targus® Notepac Case
Trade–compliant notebook carrying case
CDW 819383

$39.89

- Padded notebook compartment fits notebooks with screen sizes up to 15.4"
- Luggage strap for easy attachment to rolling travel cases
- Rear slip pocket for extra storage
- Includes workstation area that features disk pockets, business card holder, document pocket

Microsoft® **Hardware** CDWG.com/microsofthardware

Microsoft® Arc™ Touch Mouse
USB wireless optical mouse
CDW 2835956

$55.85

Use it just about anywhere, even on a rough wood surface or carpet, thanks to BlueTrack Technology®.

- Retain wireless control of your computer up to 30 feet away
- Curve it comfortably to get started, then smoothly glide your finger up or down the touch strip
- Responds precisely to the speed of your finger movement, using Haptic feedback (light vibration that signals scrolling speed) to scan through documents or web pages as quickly

EDGE MEMORY CDWG.com/edgememory

Supercharge your PC

EDGE™ Notebook Memory Upgrades
For Acer TravelMate
2GB
CDW 2608083
4GB
CDW 2003848
CALL FOR PRICING

HP Tablets and CDW·G

Help your workforce get more done while they're in the field with the latest HP tablets. Enjoy the versatile design of the HP Pro x2 612 2–in–1 with optional Intel® Core™ i5 and vPro™ performance that converts to a tablet for full speed on the go. Detach the keyboard and work on a large 12.5–inch diagonal Full HD display packed with security features to help protect your device and your organization.

CDWG.com/hp

intel inside™ CORE i5 vPro™

HP Pro x2 612 Tablet
Enjoy the sleek design of the 2–in–1 HP that converts to a tablet for full speed on the go
CDW 3452901
HP SMART BUY
$**1188**.99[1]
- 4th generation Intel® Core™ i5–4302Y vPro™ processor (1.60GHz)
- Memory: 4GB/128GB SSD
- Intel® Dual Band Wireless–AC 7260AN
- 802.11a/b/g/n/ac (2x2) Wi–Fi® and Bluetooth 4.0 combo
- 12.5″ touch–screen display
- Windows® 8.1 64–bit

HP Elite x2 1011 Tablet
Durability comes fully equipped with HP's security and manageability in a 2–in–1 device
CDW 3596011
HP SMART BUY
$**1143**.99[1]
- Intel® Core™ MM–5Y71 vPro™ processor (1.20GHz)
- Memory: 4GB/128GB SSD
- Intel® HD Graphics 5300
- 11.6″ ultraslim LED–backlit touch display
- WIndows 8.1 Pro 64–bit

HP Pro Slate 10 EE Tablet
With access to the latest productivity apps from Google Play running on Android™ 5.0 (Lollipop)
CDW 3678331
HP SMART BUY
$**342**.99[1]
- Intel® Atom™ Z3735F processor (1.33GHz)
- 32GB embedded MultiMediaCard (eMMC)
- Bluetooth® 4.0 LE
- 10.1″ capacitive multitouch screen display
- Battery runtime up to 10 hours

CDWG.com/hp

HP ProBook 440

Built-in security safeguards your HP ProBook against viruses, detects possible corruption

CDW 3595131

HP SMART BUY

$**689**.99 [1]

- 5th generation Intel® Core™ i5-5200U processor (2.20GHz)
- WLAN: 802.11a/b/g/n/ac
- Memory: 4GB/500GB hard drive
- DVD SuperMulti drive
- 14" widescreen LED-backlit HD display
- Windows® 8.1 Pro/Windows 7 Pro 64-bit downgrade
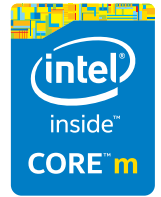
HP Elite x2 1011 2-in-1

Durability comes fully equipped with HP's security and manageability in a 2-in-1 device

CDW 3595999

HP SMART BUY

$**1009**.99 [1]

- Intel® Core™ MM-5Y51 processor (1.10GHz)
- Memory: 4GB/128GB SSD
- Intel® HD Graphics 5300
- 11.6" ultraslim LED-backlit touch display
- WIndows 8.1 Pro 64-bit

intel inside™ CORE™ m

HP UltraSlim Docking Station

Be more productive throughout the day

CDW 3145533

$**159**.00

- Simple one-click, slide-in connectivity
- Get high-speed connectivity to the USB devices you use most with four USB 3.0 ports
- Two DisplayPort® ports and one VGA port

HP EliteDisplay E241i

24" analog/digital/DisplayPort

CDW 3248330

$**266**.32

Combination of a large screen, extra-wide viewing angles and extraordinary comfort.

- Max. resolution: up to 1920x1200
- Panel brightness: 250 cd/m²
- Response time: 8 ms
- Three-year limited warranty

HP Desktops and CDW·G

Increase productivity across your organization by upgrading to the latest desktops from HP. And ensure the transition is a smooth one, by having your desktops custom configured in our state-of-the-art, environmentally controlled, ISO 9001 and ISO 14001 certified configuration center.

CDWG.com/hp

intel inside™
CORE™ i5 vPro™

HP EliteDesk 800

Transform your workplace with Intel® Pro Wireless Display (Intel® Pro WiDi) — a capability within Intel® vPro™ technology enabling users to securely and wirelessly project to conference room screens and displays, no dongles required

CDW 3391086

HP SMART BUY

$713.99[1]

- 4th generation Intel® Core™ i5-4590 vPro™ processor (3.30GHz)
- Memory: 8GB/1TB hard drive
- DVD SuperMulti drive
- Intel® HD Graphics 4600
- Windows® 8.1 Pro/Windows 7 Pro 64-bit downgrade

HP EliteOne 800 23" All-in-One Desktop

Widescreen all-in-one that is built to handle the demands of virtually any environment

CDW 3435515

HP SMART BUY

$1439.99[1]

- 4th generation Intel® Core™ i7-4790S vPro™ processor (3.20GHz)
- Memory: 8GB/1TB hybrid drive
- DVD SuperMulti drive
- Radeon HD 7650A
- Windows 8.1 Pro 64-bit/Windows 7 Pro 64-bit downgrade

HP EliteDesk 705 Mini

New AMD PRO A-Series APUs with HSA technology

CDW 3518162

AMD

HP SMART BUY

$553.99[1]

- AMD A8 PRO-7600B processor (3.10GHz)
- Memory: 4GB/500GB hard drive
- AMD Radeon R5
- Windows 8.1 Pro/Windows 7 Pro 64-bit downgrade

LG *Life's Good*
CDWG.com/lg

LG CBV42–B PCoIP® Zero Client
Secure, high–performance computing with virtually zero maintenance
CDW 3028943

$248.00

- Teradici® TERA2321 processor
- Memory: 512MB
- Gigabit LAN
- Six USB 2.0 ports
- Mounting bracket included
- Stand vertically with a cradle or it can attach to the backside of a monitor for increased space efficiency

LG 23CAV42K–BL
23" zero–client PCoIP TERA2 LED monitor
CDW 2890013

$406.99

Cost–effective, ultrasecure desktop virtualization.

- Utilizes a Teradici® TERA2 chipset and VMware Horizon View™ to deliver a powerful and secure virtual computing solution
- Headphone out with speakers
- Six USB 2.0 inputs to offer variety usage scene
- UPoE ready with optional AUPOE–1 adapter

ASUS IN SEARCH OF INCREDIBLE
CDWG.com/asus

intel inside™ CORE™ i5

ASUS D510MT Mini–Tower PC
Features Windows 8 Pro OS and gives you more of what your organization needs
CDW 3680593

$627.99

- 4th generation Intel® Core™ i5–4460 processor (3.20GHz)
- Memory: 8GB/1TB HHD
- Exclusive ASUS Business Manage — one–stop management and data protection
- Windows® 8.1 Pro/Windows 7 Pro 64–bit downgrade

Lenovo.
CDWG.com/lenovo

intel inside™ CORE™ i5 vPro™

Lenovo ThinkCentre® M93p
Embedded security — built–in peace of mind
CDW 3095872

$729.99

The 4th generation Intel® Core™ vPro™ processor strengthens security and increases productivity across your organization.

- 4th generation Intel® Core™ i5–4570T vPro™ processor (2.90GHz)
- Memory: 4GB/500GB hard drive
- Intel® HD Graphics 4600
- Gigabit LAN
- Windows 8 Pro 64–bit/Windows 7 Pro 64–bit downgrade

HP Printers and CDW·G

Increase productivity and save money across your organization by upgrading to the latest HP printers. CDW·G puts its knowledgeable experts to work for you to recommend, design and implement a printer solution that meets your agency's needs and budget.

CDWG.com/hp

HP Officejet® Pro 6230 ePrinter
Productivity features to keep your organization rolling
CDW 3512797

$**99**.99

- Mfr. print speed: up to 18 ppm black, 10 ppm color
- Print resolution: up to 600x1200 dpi
- Duty cycle: up to 15,000 pages

HP LaserJet® Enterprise M605n
Take productivity to the next level
CDW 3661529

$**999**.00

- Mfr. print speed: up to 55 ppm
- Print resolution: up to 1200x1200 dpi
- Duty cycle: up to 225,000 pages
- Max. media capacity: 3600 sheets
- Hi-Speed USB 2.0 ports (host and device); built-in Gigabit Ethernet 10/100/1000T network port; Hardware Integration Pocket (HIP)

HP Designjet® T520
36" large-format, color inkjet printer
CDW 2827801

$**2850**.00

- Mfr. print speed: up to 35 seconds for D/A1-sized documents
- Print resolution: up to 2400x1200 dpi
- HP Instant Printing — quickly print your HP-GL/2 and PLT files with the simple click of a button
- Separate ink cartridges and printheads at a low price and efficient servicing routines without any need to replace maintenance tanks keep running costs down

HP
CDWG.com/hp

HP Officejet® Pro X451dn
Network–ready color inkjet printer
CDW 2937679
$**224**.99

• Mfr. speed rating: up to 55 ppm, black and color
• Print resolution: up to 1200x1200 dpi black, 2400x1200 dpi color
• High volume printing — up to 4200 pages per month
• 550–sheet capacity

HP Officejet Pro X576dw MFP
Bring the power of the printing press to the desktop with HP PageWide Technology
CDW 2940212
$**399**.99

• Mfr. speed rating: up to 70 ppm, printing and scanning
• Print resolution: up to 1200x1200 dpi optimized
• Duty cycle: up to 75,000 pages per month
• Help workgroups thrive with proactive manageability tools
• Improve workflow — send quick faxes, scan documents to a PC, email and more

HP SUPPLIES

SAVE TIME AND MONEY WITH HP SUPPLIES

Squeeze out printing inefficiencies with CDW·G and HP
CDW•G's partnership with HP gives you access to all of their printing supplies, including standard, multipack and high–capacity cartridges. These purchase options can save you up to 35% per page.

• HP LaserJet multipacks deliver 10% savings by bundling multiple toner cartridges in one package
• HP LaserJet high–capacity toner cartridges print at a lower total cost per page by up to 35% over standard printer cartridges
• The higher yields delivered by each of these upgrade options help you save time through less frequent supply orders

Call your CDW·G account manager today.
800.808.4239

SUPPORT SERVICES

HP Care Pack Services

HP CARE PACK SERVICES

HP Care Pack Services will provide customers support to:

• Maximize productivity
• Mitigate and minimize downtime
• Provide enhanced technical phone support via North American call centers
• Budget predictability with a fixed one–time upfront cost to support and service all incidents
• Customizable support options that fit customers' specific needs
• Reduce in–house IT costs to increase customer ROI

Call your CDW·G account manager today.
800.808.4239

West Point Compatible Supplies

West Point Products has one of the broadest lines of cartridges in the industry — compatible with all major brands of printers, copiers, faxes and MICR. Using West Point products does not void any warranties and West Point has a 100% satisfaction guarantee'. Please contact your account manager and give WPP a try.

Description	Compatibility	CDW	Price
Dell 330–2209 toner	Compatible with printer model 2335DN	2452895	$47.87
HP CF280A toner	Works with: HP M400, M401, and M425 series printers	2940742	$58.84
TN720 toner	Works with: Brother HL–5450DN, HL–5440D, DBC–8150DN and DCP–8110DN printers	3093434	$58.84
HP390A toner	Works with: HP printer models: HP LJ Enterprise 600 M601N, M601DN, M602DN, M602N, M602X, M603DN, M603N, M603XH; LJ Enterprise M4555 MFP, M4555F MFP, M4555FSKM MFP, M4555H MFP – Std.	2712955	$92.76

Canon imageCLASS® MF820Cdn–MF printer

Advanced capabilities deliver impressive, customizable usability while also saving space

CDW 3590161

$1119.00

- Seamlessly navigate through features with the first imageCLASS® color 3.5" customizable touch–panel LCD
- Boost productivity with blazing fast double–sided print and copy speeds — Up to 36 pages per minute
- Limit interruptions with up to three additional 550–sheet cassettes (allows up to 2300 sheets)

Ricoh Aficio® SP C252SF

Color laser multifunction printer

CDW 3337584

$699.00

- Mfr. speed rating: up 21 ppm
- Maximum print resolution: up to 2400x600 dpi
- Versatile connectivity with standard wireless, Ethernet and USB networking
- Support a variety of network environments with PCL and PostScript® 3™ emulation including both Windows® and Macintosh® network environments

CDWG.com/hp

HP Scanjet® Pro 3000 s2 Document Scanner
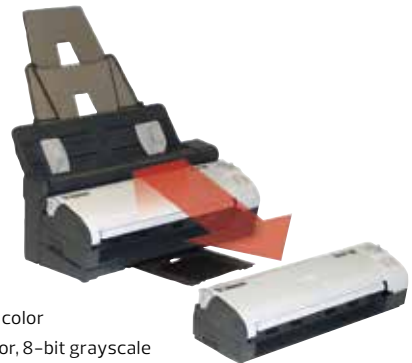Duplex sheetfed scanner
CDW 3017780

$448.87

- Mfr. speed rating: up to 20 ppm, black and color
- Scan resolution: up to 600x600 dpi
- Duty cycle: up to 1000 pages per day
- Media size: up to 8.5"x34"

visioneer CDWG.com/visioneer

Visioneer® Strobe™ 500
Mobile duplex color scanner plus docking station
CDW 1927608

$358.10

- Mfr speed rating: up to 15 ppm, black and color
- Scan resolution: up to 600 dpi, 24-bit color, 8-bit grayscale
- Powered by USB port to scan anywhere
- Scan contracts, forms, receipts, photos, ID cards
- One-year limited warranty

Panasonic CDWG.com/panasonic

Panasonic KV–S1025C–S
Duplex–ready sheetfed color scanner
CDW 2396701

$745.12

- Mfr. speed rating: up to 26 ppm
- Optical scan resolution: up to 600 dpi
- Handles virtually any type of paper and feeds ID cards, including embossed hard cards
- Each image wiped automatically according to government guidelines, leaving a clean memory after each use
- Meets Section 508 accessibility requirements
- Three-year warranty

Logitech® MK345
Wireless keyboard and mouse set
CDW 3607068
$**34**.99

Enjoy the perfect combination of great comfort, modern design, powerful features and extra-long battery life.

- The reliable combo with generous palm rest and comfortable mouse
- Small nano receiver connects both the mouse and keyboard to your computer
- With a full-size keyboard, integrated palm rest and contoured mouse, typing and browsing feels very comfortable
- Low-profile, whisper-quiet keys
- Hand-friendly contoured design for the mouse

Logitech MX Master Mouse
A precision instrument for masters in their craft
CDW 3651497
$**99**.99

Designed to provide an exceptional experience for power users and masters of their craft who want to get more done, more efficiently.

- Contoured to support your hand and wrist in a comfortable, natural position
- Well-positioned buttons and scroll wheels for fine-motion control and a fluid experience
- Automatically shifts between scrolling modes in response to your touch
- Adds easy horizontal navigation and advanced gestures

peerless-AV

Peerless® LCT620A
Desktop monitor arm mount
CDW 2544658
$**106**.72

Supports up to 29" monitors.

- Articulating arm allows monitor to be adjusted to the perfect ergonomic position to help reduce eye, back and neck strain
- Accommodates different monitor weights ranging from 8.4 to 17.8 lbs. (3.8 to 8.1 kg)
- Smooth and effortless arm movement provided by bushings at all pivot points
- Monitor can be positioned anywhere from 0.25" to 18.50" (6 to 470 mm) above the desktop surface measured at the center of the adaptor
- Integrated cable management provides clean, professional installation finish

ViewSonic® VG2239m
22" analog/digital/DisplayPort®
CDW 2762158
$**199**.99

The slim bezel design, coupled with hidden stereo speakers, make this a space saver.

- Max. resolution: up to 1920x1080 Full HD
- Panel brightness: 250cd/m²
- Contrast ratio: DC 20,000,0000:1 (1000:1)
- Fully ergonomic with 90° pivot, height adjust, swivel and tilt
- Three-year parts and labor warranty

ASUS VS228T–P
21.5" analog/digital LED monitor
CDW 3531768
$**113**.71

Optimized for the ideal image and color quality.

- Versatile viewing positions with Smart View technology
- 25° (forward 5°, backward 20°) tilting angle
- Max. resolution: up to 1920x1080
- 50,000,000:1 ASUS smart contrast ratio
- Three-year warranty with ASUS Rapid Replacement

PNY CS1111 SSD
Next generation of Optima SSD
240GB CDW 3633852
$**94**.75

- Easy and cost-effective HDD replacement
- Faster boot times, quicker application launch and better overall system performance
- Excellent power saving for longer battery life

WD

CDWG.com/wd

WD Red® NAS Hard Drive
Designed and tested for small–scale RAID environments

3.5", SATA 600, 64MB cache, 6TB
CDW 3426282
$**279**.99

- Ideal for stand–alone one– to five–bay NAS systems and desktop RAID
- NASware® technology enables seamless integration, robust data protection and optimal performance for systems operating in NAS and RAID environments
- 3D Active Balance Plus™ enhanced dual–plane balance control technology significantly improves the overall drive performance and reliability
- Up to 35% MTBF improvement over standard desktop drives for a more reliable and robust solution
- Energy efficient and lower TCO for always–on 24/7 NAS environments

Intermec by Honeywell

CDWG.com/intermec

Intermec® PM43
Direct thermal printer
CDW 2709543
$**1567**.50

- Ideal for a wide range of applications within the distribution center, warehouse and manufacturing environments
- Advanced and secure network connectivity
- Print resolution: up to 203 dpi

NEC

CDWG.com/nec

NEC NP–PX602WL–WH Projector
6000–lumen advanced professional SSLS installation projector
CDW 3554168

CALL FOR PRICING

Ideal for new applications such as digital signage.

- High brightness, lower power consumption enhance always–on capabilities of laser projection
- Eco–friendly features, minimal maintenance and cost savings
- Seamlessly blend multiple images with integrated edge blending capabilities
- Built–in HDBaseT enables simplified installations with a single cable for video, audio and control signals

SEAGATE

CDWG.com/seagate

Seagate® Backup Plus Slim
Thin, light and easy backup that's good to go

2TB CDW 3224271
$**94**.99

- Features mobile backup using the Seagate® Mobile Backup app
- Protect your data with easy, flexible backups
- Back up from Facebook and Flickr and share to YouTube
- Easy to share files between Windows® and Mac® computers
- USB 3.0 plug–and–play with no bulky power supply adapters

IRONKEY by imation

CDWG.com/ironkey

IronKey™ H350 Basic FIPS Hardware Secure Portable USB 3.0 Hard Drive
Protect data from the outside in

1TB CDW 3712576
$**254**.99

- Lock down sensitive data with FIPS 140–2 Level 3 certified drives protected by AES–XTS 256–bit encryption
- Entire device is FIPS 140–2 Level 3 certified — all components and firmware are protected
- Take advantage of all the performance improvements of USB 3.0 with fast read/write speeds
- Built to survive years of wear and tear, and shielded in a solid, tamper–resistant aluminum enclosure
- Can be upgraded to a managed enterprise drive with IronKey™ enterprise service or server
- Five–year limited warranty

Honeywell

CDWG.com/honeywell

Honeywell Hyperion 1300g Handheld Barcode Scanner
Hassle–free scanning, especially in scan–intensive or light industrial applications
CDW 2504443
$**149**.25

- No moving parts and full impact resistant bumpers
- Fast reading of 13 mil barcodes out to 18˝
- Supports all popular interfaces in one device
- Five–year warranty

47

GET THROUGH I.T. UNSCATHED

CONTRACT PURCHASING and CDW·G

Dealing with complex contract, policy and purchasing requirements is rough. We've been there thousands of times. We know what you're up against, and we know how to get you through it unscathed.

With more than 20 years of experience, we have the tools and the resources you need to fulfill your agency's IT mission — making technology purchasing and procurement a surprisingly smooth process.

To learn more about contract purchasing solutions, visit CDWG.com/contracts or call your dedicated CDW·G account manager at 800.808.4239

CDW·G PEOPLE WHO GET IT