



THE BUSINESS OF FEDERAL TECHNOLOGY

RUGGEDIZED TABLETS MAXIMIZE EFFICIENCY AND LOWER TCO FOR FEDERAL INSPECTIONS.

In today's digital environment, government agencies need dependable computing technology that can be used virtually anywhere. Ruggedized tablets provide highly mobile solutions that can survive extreme conditions that would sideline consumer-grade tablets. And when combined with powerful Intel® processors, these rugged tablets can meet government needs with superior levels of performance and unprecedented embedded security technologies. Together they help protect identities, keep data safe and enable IT departments to realize a lower total cost of ownership and higher operational efficiency.

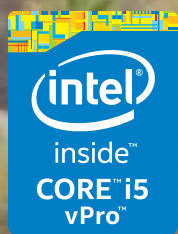
- MIL-STD-810G rated and all-weather IP65 designs
- Daylight-readable, gloved multi touch screens
- Hot-swappable batteries for continuous operation

DOWNLOAD OUR FREE WHITEPAPER TODAY AT

fcw.com/panasonic

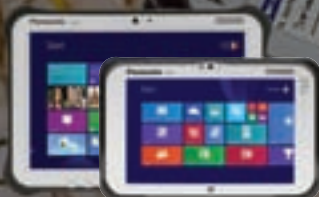
SPONSORED BY
Panasonic





Panasonic

THE FUTURE WILL WORK WITH YOU ANYWHERE.



Panasonic Toughpad® tablets are reliable and powerful mobile computing solutions for federal agencies. Designed to overcome the challenges of nearly any environment, Toughpad tablets can be counted on for both field data collections and as a desktop replacement. And when combined with the Intel® Core™ i5 vPro™ processor, you get higher levels of performance plus enhanced levels of security.

us.panasonic.com/toughpad

TOUGHPAD



THE FUTILITY FACTOR

Acquisition reform efforts are getting serious. But are we missing the bigger issue?

PAGE 18

+ DOD networks and 'the ISIS effect'

PAGE 28

Prepping for the Internet of Things

PAGE 31



The Federal IT Acquisition Summit

Exploring Strategies, Options & Innovations

June 2, 2015

National Press Club, Washington, DC

**EDUCATION &
TRAINING FOR
KEY CONTRACT
VEHICLES**



Joanne Woytek,
NASA SEWP



Robert Coen,
NIH-NITAAC



Mary Davie, GSA

**Free for
Government
& Military
Attendees**

Participating Agencies



For Sponsorship Opportunities Contact

Alyce Morrison: amorrison@1105media.com or Kharry Wolinsky: kwolinsky@1105media.com

For More Information Visit: <http://fcw.com/fias>

VA sees sharp uptick in cyberattacks

The Department of Veterans Affairs is an increasingly popular target for hackers and cyber criminals. Attempts to infiltrate VA networks or ship malware to VA employees and contractors via phishing email messages are growing exponentially, according to data released by the agency.

There were more than 350 million attempts to infiltrate VA networks in March 2015, up from 15 million in November 2014. VA blocked almost 1.2 billion pieces of malware in March, up from 300 million six months ago.

CIO Steph Warren said the department risks being overwhelmed if attacks continue to grow at the current rate. VA has been releasing top-line numbers on cyber infiltration attempts in recent months, so there is a clearer picture of the threats facing VA than those facing other agencies. But Warren told reporters in April that "there is lots and lots of interest, and we are not the only ones seeing this kind of interest."

"We hope there is some appreciation of the level of threat that is coming at these organizations," he added.

VA uses the Einstein network protection system run by the Department of Homeland Security, and Warren

said VA officials were "aggressively taking advantage" of new features being added to the Einstein toolkit.

He also said VA's tech employees are taking a harder line with colleagues who open phishing messages and click on attachments from unknown senders. Doing so typically gets the employee a chat on proper email precautions and cyber hygiene



"Six months ago, I could not have projected that we would be seeing this volume, this intensity of attacks."

— STEPH WARREN, VA

from an IT staffer that includes an explanation of what could happen if a rogue program were permitted to infect the system.

VA's defenses in combination with Einstein have blocked inbound intrusion attempts, but Warren stressed that the volume of attacks presented an urgent threat.

"Six months ago, I could not have projected that we would be seeing this volume, this intensity of attacks," he said.

Meanwhile, VA officials are consid-

ering how they might move some of their data and operations to commercial cloud environments. Warren said Office of Information and Technology staff and representatives from across VA — including the general counsel and Office of Inspector General — are meeting to develop a cloud computing strategy. A previous plan to move VA email to an HP cloud was scut-

tled because VA's OIG objected to the records retention schedules contained in the cloud deal.

Warren said he hoped to develop a plan to move high- and medium-security apps and data to the cloud. "We're not looking for a consensus solution," he said. Instead, he wants to clear potential hurdles to moving to the cloud and address objections as they come up. Warren said he hoped to see a first draft of the cloud strategy within 30 days.

— Adam Mazmanian

FCW CALENDAR

6/2 Acquisition

GSA's Mary Davie, NASA's Joanne Woytek and NIH's Michelle Street are among the many speakers at the Federal IT Acquisition Summit. Washington, D.C.

fcw.com/Events/FIAS/

6/10 Cloud

FedRAMP Director Matthew Goodrich will discuss removing barriers to agency cloud adoption and (ISC)²'s Dan Waddell will explore evolving threats to cloud security. Washington, D.C.

fcw.com/CloudSecurity

RISEINGSTAR AWARDS

NOMINATIONS NOW OPEN

Nominations for the 2015 Rising Star awards are now being accepted. Learn more at fcw.com/2015risingstars.



SPECIAL REPORT

18 Rethinking acquisition

Acquisition reform efforts are everywhere, it seems. But it's important not to lose sight of the big picture.

NS2020: A new take on telecom

BY MARK ROCKWELL

The urgency behind DOD's reform efforts

BY SEAN LYNGAAS

Acquisition after FITARA

BY ADAM MAZMANIAN

Why reforms fall short

BY MICHAEL GARLAND

DEFENSE

28 The 'ISIS effect' on DOD networks

From Kuwait to Honolulu, the war with Islamic State militants is changing how the U.S. military communicates

BY SEAN LYNGAAS

TRENDING

3 SECURITY

VA sees a sharp uptick in cyberattacks

FCW CALENDAR

Where you need to be next

8 ID MANAGEMENT

NIST plays matchmaker on identity verification — and looks for help on a continuous monitoring pilot project

9 EDITOR'S NOTE

Is IT acquisition fixable? Plus, an FCW Insider news roundup.

10 PROCUREMENT

GSA widens its telecom collaboration efforts. And a new report shows a lack of interest in digital government.

DEPARTMENTS

14 COMMENTARY

Ground rules for improving federal cybersecurity

BY DAVE McCLURE

DOD needs a change in acquisition culture

BY AJ CLARK

DOD and Silicon Valley: A marriage made in hell?

BY STEVE KELMAN

31 EXEC TECH

Are agencies really ready for the Internet of Things?

BY ZACH NOBLE

33 FCW INDEX

34 BACK STORY

What comes next for FITARA implementation



Editor-in-Chief Troy K. Schneider

Executive Editor John Bicknell

Managing Editor Terri J. Huck

Senior Staff Writer Adam Mazmanian

Staff Writers Sean Lyngaas, Zach Noble,
Mark Rockwell

Contributing Writers Richard E. Cohen,
Chad Hudnall, John Moore, Sara Lai Stirland

Editorial Fellow Jonathan Lutton

Vice President, Art and Brand Design

Scott Shultz

Creative Director Jeff Langkau

Assistant Art Director Dragutin Cvijanovic

Senior Web Designer Martin Peace

Director, Print Production David Seymour

Print Production Coordinator Lee Alexander

Chief Revenue Officer Dan LaBianca



**Chief Operating Officer and
Public Sector Media Group President**
Henry Allain

Co-President and Chief Content Officer
Anne A. Armstrong

Chief Revenue Officer
Dan LaBianca

Chief Marketing Officer
Carmel McDonagh

Advertising and Sales
Chief Revenue Officer Dan LaBianca
Senior Sales Director, Events Stacy Money
Director of Sales David Tucker
Senior Sales Account Executive Jean Dellarobba
Media Consultants Ted Chase, Bill Cooper, Matt Lally,
Mary Martin, Mary Keenan
Event Sponsorships Alyce Morrison,
Kharry Wolinsky

Art Staff
Vice President, Art and Brand Design Scott Shultz
Creative Director Jeffrey Langkau
Associate Creative Director Scott Rovin
Senior Art Director Deirdre Hoffman
Art Director Joshua Gould
Art Director Michele Singh
Assistant Art Director Dragutin Cvijanovic
Senior Graphic Designer Alan Tao
Graphic Designer Erin Horlacher
Senior Web Designer Martin Peace

Print Production Staff
Director, Print Production David Seymour
Print Production Coordinator Lee Alexander

Online/Digital Media (Technical)
Vice President, Digital Strategy Becky Nagel
Senior Site Administrator Shane Lee
Site Administrator Biswarup Bhattacharjee
Senior Front-End Developer Rodrigo Munoz
Junior Front-End Developer Anya Smolinski
Executive Producer, New Media Michael Domingo
Site Associate James Bowling

Lead Services
Vice President, Lead Services Michele Imgrund
*Senior Director, Audience Development & Data
Procurement* Annette Levee
Director, Custom Assets & Client Services Mallory Bundy
Editorial Director Ed Zintel
Project Manager, Client Services Jake Szlenker, Michele
Long
Project Coordinator, Client Services Olivia Urizar
Manager, Lead Generation Marketing Andrew Spangler
Coordinators, Lead Generation Marketing Naija Bryant,
Jason Pickup, Amber Stephens

Marketing

Chief Marketing Officer Carmel McDonagh
Vice President, Marketing Emily Jacobs
Director, Custom Events Nicole Szabo
Audience Development Manager Becky Fenton
*Senior Director, Audience Development & Data
Procurement* Annette Levee
Custom Editorial Director John Monroe
Senior Manager, Marketing Christopher Morales
Manager, Audience Development Tracy Kerley
Senior Coordinator Casey Stankus

FederalSoup and Washington Technology
General Manager Kristi Dougherty

OTHER PSMG BRANDS

Defense Systems
Editor-in-Chief Kevin McCaney

GCN
Editor-in-Chief Troy K. Schneider
Executive Editor Susan Miller
Print Managing Editor Terri J. Huck
Senior Editor Paul McCloskey
Reporter/Producers Derek Major, Amanda Ziadeh

Washington Technology
Editor-in-Chief Nick Wakeman
Senior Staff Writer Mark Hoover

Federal Soup
Managing Editors Phil Piemonte,
Sherkiya Wedgeworth

THE Journal
Editor-in-Chief Christopher Piehler

Campus Technology
Executive Editor Rhea Kelly



Chief Executive Officer
Rajeev Kapur

Chief Operating Officer
Henry Allain

**Senior Vice President &
Chief Financial Officer**
Richard Vitale

Executive Vice President
Michael J. Valenti

**Vice President, Information Technology
& Application Development**
Erik A. Lindgren

Chairman of the Board
Jeffrey S. Klein

SALES CONTACT INFORMATION

MEDIA CONSULTANTS

Ted Chase
Media Consultant, DC, MD, VA,
OH, Southeast
(703) 944-2188
tchase@1105media.com

Bill Cooper
Media Consultant, Midwest, CA, WA, OR
(650) 961-1760
bcooper@1105media.com

Matt Lally
Media Consultant, Northeast
(973) 600-2749
mlally@1105media.com

Mary Martin
Media Consultant, DC, MD, VA
(703) 222-2977
mmartin@1105media.com

EVENT SPONSORSHIP CONSULTANTS

Stacy Money
(415) 444-6933
smoney@1105media.com

Alyce Morrison
(703) 645-7873
amorrison@1105media.com

Kharry Wolinsky
(703) 300-8525
kwolinsky@1105media.com

MEDIA KITS

Direct your media kit
requests to Serena Barnes, sbarnes@1105media.com

REPRINTS

For single article reprints (in minimum quantities of
250-500), e-prints, plaques and posters contact:

PARS International

Phone: (212) 221-9595
Email: 1105reprints@parsintl.com
Web: magreprints.com/QuickQuote.asp

LIST RENTALS

This publication's subscriber list, as well as other lists
from 1105 Media, Inc., is available for rental. For more
information, please contact our list manager, Merit
Direct. Phone: (914) 368-1000
Email: 1105media@meritdirect.com
Web: meritdirect.com/1105

SUBSCRIPTIONS

We will respond to all customer service inquiries within
48 hours.
Email: FCWmag@1105service.com
Mail: FCW
PO Box 2166
Skokie, IL 60076
Phone: (866) 293-3194 or (847) 763-9560

REACHING THE STAFF

A list of staff e-mail addresses and phone numbers
can be found online at FCW.com.

E-mail: To e-mail any member of the staff, please use
the following form: *FirstinitialLastname@1105media.
com*.

CORPORATE OFFICE

Weekdays 8:30 a.m.-5:30 p.m. PST
Telephone (818) 814-5200; fax (818) 936-0496
9201 Oakdale Avenue, Suite 101
Chatsworth, CA 91311

SNAPSHOT

CYBERSECURITY

Compliance is a Headache for Cloud Adoption

While the hybrid cloud is becoming the preferred choice for organizations who want to move IT to the cloud, actually getting there could prove a headache. Outside of the technical requirements, moving to the cloud and staying compliant with government mandates and guidelines is apparently no easy thing.

In September 2014, the Council of the Inspectors General published its findings of an examination of 77 commercial cloud contracts that federal agencies issued as they transitioned to the cloud. All of them, the council said, lacked the detailed specification recommended in Federal cloud computing guidelines and best practices documentation.

"Additionally," the report said, "59 cloud systems reviewed did not meet the requirements to become compliant with FedRAMP by June 5, 2014, even though the requirement was announced on Dec. 8, 2011."

The report concluded, damningly, that none of the 19 participating agencies the council's review examined had adequate controls in place to manage its cloud service providers and the data that reside within its cloud systems.

Earlier studies had come up with similar findings. In 2013, for example, The Ponemon Institute conducted a survey of more than 4,000 organizations in seven countries and found that just over half of the respondents said they

didn't know exactly what their cloud provider does to protect their data, and only 30 percent said they did. At the same time, respondents still expressed a "marked increase in confidence" about the ability of cloud providers to protect sensitive and confidential data.

FedRAMP (Federal Risk and Authorization Management Program) and FISMA (Federal Information Security Management Act) are the two directives most closely related to cloud adoption by government agencies. OMB set the 2014 deadline for vendor compliance with FedRAMP, which describes a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FISMA compliance, which requires agencies to develop, document and implement information security measures for such things as cloud services, is tested every year.

There are some systemic barriers that stand in the way of cloud initiatives coming into compliance. Even though the OMB has mandated that all cloud systems used by government agencies comply with FedRAMP,

for example, the FedRAMP program management office has no authority to enforce compliance at the agency level.

In order to spur better compliance, the Council of Inspectors General has recommended that the OMB:

- Establish standardized contract clauses that agencies must use when adopting cloud computing technologies;
- Determine how best to enforce FedRAMP compliance; and
- Establish a process and reporting mechanism to ensure Federal agencies require cloud providers to meet the FedRAMP authorization requirements in a timely manner.

This is where managed cloud services can provide the greatest value for agency users, said David Weisbrot, federal cloud business manager at QTS, some of whom may not have the technical resources or expertise to meet the very specific compliance requirements. They can be used to continually watch an intrusion detection system, for example, or collect and archive security logs, all things required to meet FISMA Moderate needs. •

Breaking Through the Security Cloud




For more coverage of cybersecurity issues – including hybrid cloud, identity and access management and encryption and compliance – go to

FCW.com/2015SNAPSHOTCYBERSECURITY



Federal Solutions on a Mega Scale.

FedRAMP Compliant. 24x7x365 Secure.

 **FedRAMP** Whether it's building infrastructure, consolidating data or moving apps to a virtualized platform, QTS delivers what agencies want most: FedRAMP compliance and best-in-class physical and logical security. That's a mega data center that agencies can trust.



Data Centers Powered by People

qtsdatacenters.com

Atlanta-Metro GA | Atlanta-Suwanee GA | Chicago IL | Dallas-Fort Worth TX | Jersey City NJ | Miami FL
Overland Park KS | Princeton NJ | Richmond VA | Sacramento CA | Santa Clara CA | Wichita KS

IN THE IT PIPELINE

WHAT: A National Institute of Standards and Technology “sources sought” notice seeks information on vendors that can help the agency test a proven risk-scoring methodology that would lead to a long-term, real-time continuous monitoring program.

WHY: NIST is looking for a plan, software and technical services for a year-long pilot for five categories of users at the agency: authorizing officials, information system owners, information system security officers, operating unit security officers and security control assessors.

Officials are encouraging large, small and foreign companies to provide information about their abilities.

The notice states that interested companies should have experience with e-governance, risk and compliance tools, preferably RSA Archer, which is the approved vendor solution for the Department of Homeland Security’s Continuous Diagnostics and Mitigation program.

Companies should also have deep knowledge of NIST’s Risk Management Framework and its Cybersecurity Framework. Furthermore, proposed solutions must include security control descriptions, assessment results, risk scoring and drill-down reporting capability.

After the results of the pilot project are analyzed, NIST might conduct a competitive procurement and award a purchase order for a system.

FULL LISTING:
is.gd/FCW_DARPA_BRASS

NIST plays matchmaker on identity verification

A senior official at the National Institute of Standards and Technology said one of his agency’s ongoing projects is to foster a private marketplace for best practices in identity verification.

Security isn’t the only issue at stake, said Michael Garcia, deputy director of the National Strategy for Trusted Identities in Cyberspace (NSTIC). Liability, interoperability and privacy are all factors, and progress is needed in each area “to actually get to a functional, sustainable marketplace,” he said.

The theft of online credentials and the hassle of managing passwords are burdens on consumers. Forty-six percent abandon a website rather than try to reset a password or answer a security question, said Paul Grassi, NSTIC’s senior standards and technology adviser, citing data from Verizon Enterprise Solutions.

Passwords are a “perfect combination of a really bad user experience as well as being terrible at security,” Garcia said.

There is broad interest in improving that user experience, not least from businesses wanting to offer more services online and federal officials concerned about security.

To harness that interest, NIST has funded the creation of the Identity Ecosystem Steering Group, which includes stakeholders that range from Citigroup to the Electronic Frontier Foundation.

By summer’s end, the group will issue a preliminary framework of business rules and interoperability standards for identity verification, Garcia said. The next version of the framework will get more specific, with provisions on accountability mechanisms, risk models and liability arrangements, he added.

“If nothing else, if we do this right, it removes this bilateral need for rooms full of lawyers to get together and spend months trying to figure out whether or not they can work together,” Garcia said.

— Sean Lyngaas

INK TANK



\$100,000+

is the starting salary being offered to 2015's top computer science graduates from schools like Carnegie Mellon University

FCW Insider: People on the move

Al Tarasiuk retired as CIO of the intelligence community on April 28 after more than four years at the helm.

Director of National Intelligence James Clapper credited Tarasiuk with advancing the IC Information Technology Enterprise, an ongoing quest for a single, standards-based IT architecture across intelligence agencies.

President Barack Obama has nominated Vice Adm. **Peter Neffenger** to be the next head of the Transportation Security Administration. Neffenger has served as vice commandant of the Coast Guard since May 2014.

Jimaye Sones, the Defense Information Systems Agency's former comptroller, has accused the agency

of demoting him after he reported accounting practices he believed were potentially illegal.

"I went from comptroller to currently I'm sitting in an 8-by-10 office...and I've been told by [DISA Director Lt. Gen. Ronnie Hawkins] I'm not to communicate, for any business reasons, with the agency while I'm under this so-called detail," Sones told FCW in an exclusive interview.

He said that, starting in the fall of 2012, he began warning DISA's leadership that the agency risked violating the Anti-Deficiency Act, which bars federal employees from spending unappropriated funds. When he reported the issue to the Defense Department CIO's

office, Sones said he was reassigned to lower positions within DISA.

According to Sones' legal team, the DOD inspector general is investigating the alleged financial improprieties, and the U.S. Office of Special Counsel is investigating the claims of retaliation.

Martha Dorris has a new job at the General Services Administration. The longtime GSA leader, who most recently directed the Office of Innovative Technologies, has become director of the Office of Strategic Programs at the Federal Acquisition Service.

Dorris replaces **Maynard Crum**, who had served as acting director and is shifting to a different role at GSA.

— FCW staff

EDITOR'S NOTE

Is IT acquisition fixable?

Acquisition reform is in the air.

That's almost certainly a good thing. What's less encouraging, however, is the sense that virtually everyone involved has a different idea of what that reform should look like.

Is better training the answer as services and complex procurements become the norm? Do agency acquisition officers need to be more accountable to the programs that will ultimately use the IT, or are they too close to the programs already?

What about the acquisition vehicles themselves? Can new structures and approaches improve the buying process, or would a narrowing of the often-overlapping options better serve agencies and their industry partners?

And could it be that those sorts

of questions miss the forest for the trees? After all, there has been plenty of talk in the past year that we don't need fixes but a wholesale reimagining of what we expect from government acquisition.



I don't pretend to have the answers, but this issue of FCW aims to better explore the questions. In the pages that follow, we look at a few of the efforts that are driving the acquisition discussion — at the

Defense Department, the General Services Administration, the Office of Management and Budget and elsewhere.

There's also an important reminder that this conversation is not exactly new: IT acquisition has been a friction point for as long as there has been IT to acquire. Since all previous reform efforts have fallen short to at least some degree,

it's worth asking what can be done to make this go-round different.

On FCW.com, meanwhile, there's plenty more to read and discuss: GSA's hallways, the Office of Federal Procurement Policy's Acquisition 360 initiative, the Department of Health and Human Services' Buyers Club, new versions of SEWP and NetCents, contests and other tools to help woo new firms over the procurement hurdles, and whether the U.S. Digital Service is about sharing expertise or insourcing. It's a rare day that this conversation doesn't advance online.

So add your voice to the discussion. Comment online, reach out to @FCWnow via Twitter or email me directly — and tell us what you think acquisition really needs.

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

CRITICAL READ

WHAT: "Washington Must Work Harder to Spur the Public's Interest in Digital Government," a report from Forrester Research.

WHY: In a survey of more than 4,000 Americans, roughly one-third said they use the mail, the phone or in-person meetings to interact with the government and more than 40 percent use government websites. Beyond that, digital service use was "paltry."

Although most respondents said the federal government should offer more digital services, many don't trust the government with personal information or don't see the value of many digital services. Even tech-obsessed millennials prefer to interact with the government through old-fashioned means.

Quality, not quantity, should guide future digital expansion, the report advises. Kill the unwanted social media accounts, improve the functionality of existing digital services and build a "true federal Web portal" — something more than half of Americans say they want.

VERBATIM: "Just 30 percent of online adults with a cell phone or tablet are interested in federal mobile apps that tailor safety alerts and other government information to the user's location, and only about 40 percent of online customers are interested in either a digital Social Security card or a single-sign-on credential for federal websites."

FULL REPORT:
is.gd/FCW_Forrester

GSA widens telecom collaboration efforts

The General Services Administration has stepped up efforts to encourage industry collaboration in the development of its massive next-generation telecommunications contract.

In late April, the agency convened a public comment session on the Enterprise Infrastructure Solutions (EIS) contract, which will be the foundation of the Network Services 2020 strategy for telecommunications services. The meeting was the first of three aimed at working more closely with industry on the contract.

Fred Haines, EIS program manager in GSA's Office of Network Services Programs, told FCW the initial meeting went well. "From comments received, our industry partners are satisfied with our initial outreach," he said. "Our expectations for the May

28 and June 30 sessions are to dive deeper into industry's comments and recommendations and report back our analysis."

After issuing the EIS draft request for proposals in February, the agency's mid-April comment deadline saw almost 1,600 comments and questions from industry and federal agencies concerning its RFP.

"GSA is committed to make sure the RFP we release this summer is complete and addresses needs of government and industry," Amando Gavino Jr., director of GSA's Office of Network Services Programs, told FCW. "If that means we release the RFP later than July to take more time to analyze input and enhance the document, we will."

— Mark Rockwell



IoT Attack
@iotattack

#NIST official: Internet of Things is indefensible - <http://bit.ly/1GDoD4K> #IoT #security via DARPartners



Reply Retweet Favorite

12:34 PM - 1 May 2015

Join the conversation

FCW uses Twitter to break news, field questions and ask our own.

Learn more at Twitter.com/FCWnow.

5 Things You Need to Ask When Planning for the Hybrid Cloud

Cloud spending is big business for agencies. IDC recently reported that federal spending on cloud technology will top \$9 billion by 2017. But if agencies don't plan carefully and use the right technologies, providers, and integration strategies they may be throwing away money and causing more work than benefit, especially when it comes to the hybrid cloud. There are strategies that agencies and organizations can use to find better success with their cloud implementations. Here are five questions that every agency IT person should ask during a journey to the hybrid cloud:

1. WILL MY HYBRID CLOUD IMPLEMENTATION SCALE AS OUR AGENCY'S NEEDS GROW?

Scalability is one of the main benefits that cloud providers tout, promising that agencies can burst up and down as needs wax and wane. However, just because a provider says they can scale with your agency's needs, doesn't mean they actually will, explains Jeff Kaplan, managing director of THINKstrategies Inc., a firm that specializes in cloud services.

"The best way for someone to evaluate [scalability] is for them to ask a potential provider if they are already supporting organization of a comparable size," he says. "It's easy to say, 'Yes, we will scale,' but they should be able to prove it."

Kaplan suggests that organizations take their current implementation, project how quickly they will grow, and ask the provider for references and proof that they are already working with another organization of that same size growing at the same rate.

2. HOW RELIABLE IS OUR HYBRID CLOUD?

An agency's reliability of its on-premise resources are a given, says Steve Duplessie, founder and senior analyst at Enterprise Strategy Group. What's more important is whether or not the cloud

with hybrid cloud agencies must worry about data not only while it is at rest but also while it is in flight. To understand how safe your data will be, Duplessie says you'll need to make sure the organization is using strong encryption technology such as FIPS 140-2 certified encryption so that data is never exposed to risk.

4. HOW EASY IS IT TO MOVE BETWEEN CLOUDS?

Since agency technology needs evolve over time the cloud provider you use today may not be the same one you

THE CLOUD AT ITS CORE SHOULD MAKE THINGS SIMPLER BUT IT'S BEEN LAID ON TOP OF OLD WORLD TECHNOLOGY.

provider has a good track record as well as procedures and processes in place to not only keep resources up but notify you in the event of service issues. How will they inform you of status and issues?

"Then it's all about availability and protection (backup and DR)," he says.

3. IS OUR HYBRID CLOUD AS SECURE AS IT CAN BE?

Indeed, data security has always been the biggest concern for IT. However,

will use tomorrow. Every agency must make sure that they can simply and quickly take all of their data from one provider to another— and without added cost, say experts. "What happens if you end up hating your provider?" Duplessie asks. Every cloud provider should offer portability, and give your agency a step-by-step process to make that happen.

5. HOW MUCH VISIBILITY AND CONTROL WILL WE HAVE?

The cloud at its core should make things simpler but it's been laid on top of old world technology, says Kaplan, so agencies need management control over not only on-premise but also cloud resources. A good provider will have plenty of tools to this end.

Kaplan suggests asking providers what kind of management control and administrative power you will have over your hybrid cloud environment.



Backup and Recovery in a Hybrid World



The City of Mount Dora, Fla. recently faced a problem. The city's nine departments had outgrown a legacy data backup and recovery system. The organization found a solution in a cloud-based system that not only automated processes, but ensured that—in the event of an outage—city workers would be able to continue to function and no data would be lost.

This story speaks to several characteristics of traditional backup and recovery: It can be very cumbersome and once you've filled a disk or tape, there's nowhere else to grow. In addition, either technology can be a lot to manage and restore. In recent years data growth as well as capacities have increased tremendously, making the challenge of backup even more difficult. The time-to-recovery for a large tape drive can be days or even weeks.

However, with the advent of the cloud, backup and recovery may become easier for some organizations, and cheaper, too, as the burden of buying, maintaining and supporting traditional media is lessened. Agencies can keep the most important and

sensitive data on site and send older or less crucial data into the cloud for short and long term storage. As with traditional storage, though, the old adage remains: You can't set it and forget it. You need to understand not only what you're storing but how your cloud provider is handling that data.

"Even in the cloud things can disappear so you need to know exactly how backup and recovery works—both on-premise and in the cloud," explains Jeff Kaplan, managing director of THINKstrategies Inc., a firm that

IN RECENT YEARS DATA GROWTH AS WELL AS CAPACITIES HAVE INCREASED TREMENDOUSLY, MAKING THE CHALLENGE OF BACKUP EVEN MORE DIFFICULT.

specializes in cloud services. He says that agency IT people need to ask some questions before they transition a single megabyte into the cloud.

For instance, what safeguards are in place to ensure your data is safe during transport as well as when it resides

on the cloud provider's servers? In addition, will your provider be able to scale appropriately? With traditional infrastructure, especially in the government space, it can be hard to figure out how much space you'll end up needing.

Also important, he says, is asking how easily what you're already doing can be aligned and integrated with a cloud backup solution. Most organizations will continue to use their current backup technology, and when the two can work together recovery becomes not only easier, but more efficient. Some agencies may want to add a third option in the form of an appliance that can use technologies like deduplication and compression to reduce the cost of cloud storage and data transport. When you're sending less data to the cloud or more compact data, the agency will see cost savings in the form of less data sitting in the cloud.

In addition, agencies that want to get out of the business of handling backup and recovery may want to see if their provider offers managed services that typically include software, restores, bandwidth and other forms of support.

Finally, agencies should decide if cloud backup and recovery is really

right for them. While it makes sense for most, it may not make sense for every organization, says Kaplan. "The cloud should be a tool to either economize on the physical process or further automate it," he explains. "There's got to be an ROI you can point to before you make a change."

CDW-G Delivers Cloud Skills, Capabilities to Agencies

In the early days of cloud computing, agencies feared the cloud. At the time, there were good reasons. Cloud security was not a given, and the skillset needed to handle such technology simply wasn't there. Today, however, as agencies and organizations adopt cloud strategies, it is becoming clear that so much—from compute to applications to backup and recovery—is not only possible in the cloud but in many cases preferable, especially as regulation and technology catches up to needs.

Last year in particular was a good year for cloud. As of June 2014, agencies can only use cloud services that have been certified under FedRAMP so that any cloud service they choose has been certified to meet all security measures put forth in the Federal Information Security Management Act (FISMA). This is a boon for IT, says Jack Nichols, the Federal Cloud Client Executive for CDW-G. "In addition, the DISA SRG or Security Requirements Guide for cloud services was released in the middle of January so now agencies have a definitive guide for cloud services."

This means agencies can use cloud for any number of applications and services with the confidence that no matter what they choose it will meet the agency's business and technology needs. Still, with so many options, figuring out which technology and where it lives—in the public, private or hybrid cloud—isn't always easy.

That's where CDW-G comes in, says Nichols. The company can help agencies figure out the way forward. "We help them try to determine what in their IT services catalog can or should be best delivered from a cloud provider, whether it's public or private. Then we help them determine what's the best cloud," he explains. "If it is best suited for cloud as the IT delivery mechanism, then which



is the best method or which is the best cloud provider? Is it public or private? If it's public, then which is the best public cloud provider?"

CDW-G has relationships with practically every IT manufacturer so the organization can help agencies scope their requirements and then custom configure and create the products and services that are needed. "We can also bring the capability to audit those and audit them in accordance with either the DISA security requirements guide or the FedRAMP baseline," he says.

For some customers, backup and recovery will be an important addition to their cloud strategy. One option, says Nichols, is software, systems and service company NetApp's SteelStore appliance.

SteelStore, a backup and archive solution, sends data to the cloud, boosting recovery time, cutting costs and reducing risks. The solution, which offers end-to-end security at rest and at flight using FIPS 140-2 certified encryption, uses inline deduplication and compression, reducing

storage costs by up to 90 percent. The SteelStore option also gives agencies more options since the appliance integrates with more than 90 percent of all cloud providers, says Nichols. "NetApp is also famous for ease-of-use," he says.

In the end, says Nichols, working with CDW-G is a matter of comfort and abilities. "Working with cloud services in general can still be uneasy for folks," he says. "The challenges are not just technology-driven but culturally-driven. It takes patience and understanding on both sides. At the end of the day, CDW-G makes the process easier, more efficient and cost-effective."



FOR MORE INFORMATION ON
FEDERAL CLOUD SOLUTIONS
PLEASE VISIT CDWG.COM.



Ground rules for improving federal cybersecurity

In today's complex cybersecurity environment, these three elements form the foundation of agencies' ability to defend networks and data

Big-data analytics are gaining attention in the cyber world, and there is widespread recognition that government agencies must retreat from the current cut-and-paste approach to collecting threat information. Instead, there is real value in automating critical continuous monitoring and focusing more attention on critical analyses.

That shift has given rise to the application of predictive and behavioral analytics to all enterprise and external data in an effort to better evaluate threat potential, thereby increasing the likelihood of detecting attacks before they occur and gathering useful threat and vulnerability intelligence.

However, for many organizations, it is a daunting if not impossible task to prevent all intrusions from occurring. In fact, most testing shows it might be safe to assume a breach has already occurred without any near-real-time detection. Today, data security — at rest, in transit, in use — takes precedence over a systems mentality. Data sharing, created by distributed computing environments and accelerated by the continuing explosion of end-user devices and capabilities introduced by the Internet of Things, has created a very challenging cyber environment.

As a result, organizations must address some basics that form the foundation of future cyber protection success:

1. With the push toward enterprise solutions, **data governance needs critical attention.** Without

it, cybersecurity is handicapped at the outset. At a minimum, agencies must categorize data into master, shared and single use bins. That is essential for building basic business and workflow processes that control proper access, usage, protection and accountability. Business process rules can help identify critical assets and whether those assets are being used in ways that could create damaging vulnerabilities.

There is real value in automating critical continuous monitoring and focusing more attention on critical analyses.

2. We must **focus on data and security architecture and engineering designs** that make it difficult to get access to key assets and limit damage when cyber breaches are successful. As noted, protecting data can be complicated by moving apps to the end user and operating in an Internet of Things world. Data segmentation practices are paramount in a world in which vulnerabilities are a fact of life. Agencies must address a fundamental question: When an attacker gets inside a perimeter, what will that entry allow them to do?

3. Given the unprecedented rise

in advanced persistent threats by internal and external actors, **agencies should incorporate a "current compromise" assessment approach** into core security measures. A good way to think about this is akin to using a hunt versus peck approach to vulnerability scanning and penetration testing. Compromise assessments use egress pattern matching and other techniques that can further isolate and identify the source of a compromise. In essence, you assess entry from an attacker's perspective and use the same likely attack vectors.

Often a reverse, "inside-out" approach is deployed. Administrators say: "Here are my critical assets; let's try to discover all the ways an outsider could get to them and then plug the dike." However, it is more useful to search for business-critical assets and data that adversaries would seek during an actual breach. That method is stealthier than standard penetration testing.

Tools are available that evade and bypass normal system security protections. By emphasizing significant business and operational impacts, the approach is useful for drawing executive management's attention to prioritized security solutions. And it is a bell-ringer for those who doubt whether security vulnerabilities really exist and put their operations at risk.

Keeping a focus on these fundamentals in cybersecurity programs can help strengthen an agency's overall security program and posture. ■



DOD needs a change in acquisition culture

The Pentagon needs a modern, agile acquisition process that can get technology into the field faster — and industry should take the lead

The basic military rifle, the M16, and its derivatives — including the M4 carbine that today's infantry troops use — date back to 1963 and the jungles of Vietnam. Development began in 1949.

USS Nimitz, the Navy's first-of-its-class carrier, was commissioned in 1975. The next carrier, the *Gerald R. Ford*, will join the fleet in 2016 after construction began in 2005. The F-15E, the Air Force's workhorse in Iraq and Afghanistan, goes back to 1984. The development contract for the F-35 was signed in 1996, and the first scheduled deployment will be in 2018.

My point is this: An acquisition process designed for large and unique weapon systems is becoming harder and harder to apply to technologies in the Information Age. The challenges that the Pentagon and Congress face with defense IT acquisition will continue to grow if the system for buying airplanes, ships and rifles is applied.

There is a need for a cultural shift in government procurement and in the defense industry that can allow an informed series of vendors to anticipate needs and shorten the acquisition cycle so the Defense Department doesn't buy mobile and Web applications the way it builds ships and airplanes.

The current acquisition process — see a problem, craft what the required solution looks like, compete the solution, buy the solution, build the solution — is so cumber-

some that it has reversed development from government stimulation to business fomentation. Where once DOD's need drove IT development, which then spun off to commercial use, now we in the software industry build our products as commercial technology.

An acquisition process designed for large and unique weapon systems is becoming harder and harder to apply to technologies in the Information Age.

It's the reason research and development money from Amazon, Samsung, Google and others in the IT world dwarfs that of U.S. defense, and it's the reason commercial capability drives solutions for government need. Is it any wonder that, when the CIA went shopping for cloud computing capability for the intelligence community, it turned to Amazon with a \$600 million, 10-year contract?

We in industry want to align ourselves with a new, modern, agile acquisition process to build things at our own expense so that when government sees technology it can use, it can buy that technology

quickly and get it to the field, where it can save lives.

That approach allows smaller companies with specialized IT capabilities to solve DOD problems now. Warfighters see capabilities that are available commercially and wonder why those capabilities are not adapted to military use in the field, where they can bridge existing capability gaps.

The need for a culture change in defense acquisition was addressed at length in the National Defense Industrial Association's "Pathway to Transformation" report. "NDIA does not believe there is a 'one size fits all' approach that will uniformly deliver the best acquisition outcomes," the report states. "Different kinds of acquisition programs require different kinds of tools, authorities and oversight to ensure integrity in the process."

The report also said: "Culture eats strategy for lunch."

That's only one of the reasons to applaud the confirmation of Ashton Carter as secretary of Defense. Carter led a march toward acquisition reform as undersecretary of Defense for acquisition, technology and logistics in 2010, and his successor in that post, Frank Kendall, has continued that march with his legislative proposals to streamline the complex acquisition process.

It's a blueprint for a culture change, one that both DOD and the defense industry can get behind to reward vision, accountability and reason. ■



DOD and Silicon Valley: A marriage made in hell?

The differences are irreconcilable, but government should still be looking for at least a few flings

With both Defense Secretary Ash Carter and Homeland Security Secretary Jeh Johnson visiting Silicon Valley in April, there has been a fair bit of attention paid to the national security world's attempts to better tap the innovative energy of U.S. high-tech companies.

Yet there are so many challenges to making such a relationship a reality that any sober-minded person might conclude it is a non-starter and shouldn't even be tried.

Silicon Valley is mostly indifferent to government. And to the extent that people might care, most people there are more privacy-oriented and more likely to sympathize with Edward Snowden than with the National Security Agency.

And, of course, salaries in Silicon Valley dwarf those in Washington, and the work environment is much more casual.

So first a case must be made that the government — and the Defense Department in particular — needs Silicon Valley. My good friend Alan Balutis, a longtime fed now working for Cisco, wrote recently that “the reality is that if you open up the way you run the procurements, any of the big systems integrators or service providers or medium-sized firms [along] the Beltway would be every bit as innovative and cutting edge and agile as any other firm elsewhere in the world.”

If that's true, then the push to engage Silicon Valley isn't worth it

because the probability of failure is too great and the benefits are overstated.

But I don't think Alan is right in this case. Although there are many innovative individuals at the big federal contractors, the relative lack of innovation from those companies involves a history longer and deeper than just the procurement system.

The federal contractor world, at a minimum, needs to be shaken up by competition from those outside it.

It involves the whole government environment, which does not often value risk-taking, and the selective recruitment over time of people into contractor jobs that grow out of that environment.

Silicon Valley's record of innovation is so superior to that of government contractors that it's not going to be possible to overcome that gap in the short or perhaps even the medium term.

The federal contractor world, at a minimum, needs to be shaken up by competition from those outside it.

Yet if a marriage between the government and Silicon Valley is unlikely, is there any chance for

at least a few dates? I think there might be.

First, procurement contests to solve government tech problems are a way to both avoid the dysfunctions of federal procurement and attract new players from the private and public sectors. Prizes could be a source of startup capital for young entrepreneurs, who might even use the ideas they develop to start a business.

Second, the millennial generation is notable for its lack of cynicism and positive view toward helping others. Little of that, sadly, now gets expressed in the form of a desire for public service in government. But when Johnson asked Valleyites to “consider a tour of service to your country,” he was on the right track. Government service will not appeal to all of them by any means, but it could resonate with some.

After all, it is amazing how many Valley types the administration has talked into doing a stint in government service lately. There ought to be a concerted effort to involve the Silicon Valley crowd currently in Washington in a discussion of how best to craft an appeal to attract at least a subculture of public service-oriented techies.

Such recruits might serve the government as contractors only sporadically or work inside government only temporarily, but that's much better than their being on the outside altogether. ■

N O M I N A T I O N S D U E J U L Y 2

**SUBMIT
YOUR
NOMINATIONS
TODAY!**

FCW's Rising Star awards program recognizes individuals in the first 10 years of their federal IT careers who have gone above and beyond their official job descriptions.

FCW.com/2015RisingStars



**RISINGSTAR
AWARDS**

Rethinking acquisition

Everywhere one looks, it seems, there's an effort underway to reinvent IT acquisition — from the federal workforce to procurement policies to the fundamental strategic thinking.

In this special report, FCW explores three case studies in particular — and offers an important reminder that the government has been through this exercise before.



NS2020: A new take on telecom

The General Services Administration is working hard to adapt to changing communications needs. Just don't call it a contract.

BY MARK ROCKWELL

For nearly three decades, the General Services Administration has managed a series of overarching contracts for telephone services and other agency communications needs. Just what was covered by those contracts depended on clear definitions of what constitutes telecommunications services.

This time around, however, things aren't nearly as clear-cut — and GSA is approaching the acquisition differently to address the tectonic shift in telecom services.

Potential bidders on the next version of the agency's telecom contract — the \$50 billion, 15-year Enterprise Infrastructure Solutions contract that anchors GSA's Network Services 2020 strategy — are watching hopefully as the agency's ideas take shape. There are some parallels to past efforts, but some key differences as well.

GSA officials have said they expect EIS to draw more — and more diverse — potential contractors than the five telecom carriers that currently provide

services through the Networkx vehicle. They said they expect to attract those nontraditional companies in part because of the new contract's longer life and the fact that it requires fewer mandatory services.

There has been some speculation that Google or other Silicon Valley-oriented technology and communications companies might be interested as prime contractors. Multiple sources told FCW, however, that those kinds of firms would more likely partner with companies that control traditional telecom infrastructure, which the contract allows.

A broader scope

For EIS, GSA is working with industry stakeholders to craft a more flexible and comprehensive way to address advancing telecom services. NS2020 is intended to be the federal government's strategic sourcing center for network-based and network-enabled services. It will not be one big contract, however, but rather a series of vehicles that cover regions

in the U.S. and provide a wider variety of services.

GSA released its much-anticipated request for information for EIS in April 2014 and a draft RFP this past March. Officials scheduled a series of meetings from April to June aimed at soliciting industry feedback. The agency is aiming for a July release of a formal request for proposals, but officials have said they could stretch the final deadline if needed.

Mary Davie, GSA's assistant commissioner for the Office of Integrated Technology Services, which oversees the Networkx and EIS programs, has said her agency hopes EIS will serve at least 30 percent of the \$6 billion annual federal communications market.

She said the aim for NS2020 is to evolve GSA's contracting capabilities as commercial and federal telecom markets move beyond hardware-based networks, owned legacy infrastructure, and even cloud computing and mobile services toward more open and innovative services and technologies. EIS will have



GSA's Mary Davie said the agency's aim for NS2020 is to evolve GSA's contracting capabilities as commercial and federal telecom markets move beyond hardware-based networks.

Rethinking acquisition

a broad scope, including a wide range of commonly procured communications products and services, so that agencies will no longer have to split their enterprise requirements across multiple procurements, she added.

The draft RFP for EIS outlines (over the course of a few hundred pages) the government's wish list for the following:

- Data services
- Voice services
- Contact center services
- Colocated data center services
- Cloud services
- Wireless services
- Commercial satellite communications services
- Managed services, including audio and video teleconferencing

When the massive draft RFP was issued, there were some industry concerns about how NS2020 was taking shape, but carriers see promise in GSA's approach to opening up collaboration and allowing room for evolution.

Learning from past mistakes

Lisa Bruch, CenturyLink Government's vice president of federal sales and marketing, said GSA has proven that it can handle shifting technological and market changes.

In the late 1990s, GSA navigated a dramatically changing telecom market in which long-distance and local telephone companies and services were blending into one another and the shift toward IP-based services began. With Networx predecessor FTS2001, Bruch said, the agency gave itself and bidders room to evolve and unfold new capabilities spurred by the Telecommunications Act of 1996.

Networx, which launched in 2007, further redefined telecom acquisition.

Now with telecom services becoming commoditized and integrated into a whole range of IT systems and capabilities, GSA again is facing a tricky market and technology crossroads, Bruch said. The business principles GSA is pursuing under NS2020, such as acquiring current-generation services for fixed

and wireless and lowering costs using commercial services, have not changed, she added.

"What's shifted is the state of the industry," she said.

"I don't know of any other industry where change is happening at such a rapid pace," said Mike Leff, AT&T Government Solutions' vice president for civilian government business. "Our customers continue to change how they are buying services and solutions, moving more toward a consumption-based model. We are also seeing a shift away from point solutions to end-to-end solutions that can scale. NS2020 and contracts like EIS are well aligned to where industry is headed."

Furthermore, "NS2020 will not only provide the foundational infrastructure and services to include managed networks, Ethernet, virtual private networks and regional telecommunications," but the new contracts "will have the flexibility to address several big megatrends around strategic services, including the convergence of IT and

telecommunications, network, mobility, cloud and the Internet of Things."

EIS also represents an opportunity to learn from Networx's mistakes. Although that vehicle, which expires in 2017, tried to tackle the increasingly unstable nature of what telecom services have become, Bruch said Networx was too detailed in what it offered. With EIS, GSA is taking a looser approach and defining services and technology in less detail — and hopefully, she added, not trying to manage technology development too aggressively.

Leff and Bruch agreed that EIS and NS2020 demonstrate that GSA is moving proactively and collaboratively to address rapidly evolving federal telecom needs. However, Bruch said one of her biggest worries about EIS is that the agency will become too focused on the trees and not see the forest by being too specific in defining everything it wants.

"You don't go to the hardware store when you're buying a house and try to design the kinds of the bolts you will use on the second floor," she said. ■

The urgency behind DOD's reform efforts

Better Buying Power 3.0 has a geostrategic urgency and emphasis on cybersecurity that were missing from previous iterations

BY SEAN LYNKAAS

Changing the way the Defense Department buys weapons and IT has been a decades-long project, but the latest effort contains a strain of desperation.

A chorus of Pentagon officials, from Secretary Ashton Carter on down, has lamented that DOD risks losing its technological edge to potential adversaries such as Russia and China. That existential crisis is exacerbated by the new era



Frank Kendall, undersecretary of Defense for acquisition, technology and logistics, has embarked on a third iteration of acquisition “improvement” through a program called Better Buying Power.

of relatively tight and uncertain defense spending triggered by the Budget Control Act of 2011.

Frank Kendall, undersecretary of Defense for acquisition, technology and logistics, is an engineer by training. He has been chipping away at the acquisition bureaucracy gradually. He has told reporters that the phrase “acquisition reform” bothers him because it implies an overhaul of the system rather than the incremental improvements he has been making.

And so the Pentagon’s top acquisition official has embarked on a third iteration of acquisition “improvement” (henceforth called “reform” in this article, perhaps to Kendall’s chagrin) through a program called Better Buying Power.

BBP 1.0, released in 2010, focused on improving business practices, while 2.0, which came in 2012, emphasized better decision-making. But 3.0 has a geostrategic urgency that was absent in previous versions.

A white paper on BBP 3.0 released by Kendall’s office notes a “remarkable leveling of the state of technology in the world, where commercial technologies with military applications such as advanced computing technologies, microelectronics, sophisticated sensors and many advanced materials are now widely available.” Protecting proprietary information has grown more difficult, “a fact that potential adversaries are doing their best to exploit,” the paper states.

The implication is that the fate of the

United States as a world power is intertwined with the BBP odyssey.

Unlike its predecessors, the new guidance is preoccupied with cybersecurity. It calls for Defense Department CIO Terry Halvorsen and other top Pentagon officials to add a new section to DOD’s acquisition manual detailing program managers’ responsibilities for cybersecurity.

BBP 3.0 is taking effect as Carter, who previously had Kendall’s job, settles in at the Pentagon’s helm. Acquisition reform advocates hope Carter’s technocratic touch will make now the time for meaningful change after years of half-measures.

Yin and yang

Rep. Mac Thornberry (R-Texas), chairman of the House Armed Services Committee, has expressed similar optimism and has said it is partly because his Senate counterpart, Sen. John McCain (R-Ariz.), supports his reform agenda. Thornberry has made defense acquisition reform a legislative priority and has worked closely with Kendall.

Thornberry added that he hopes the stars are aligned this time around. “We can’t waste this opportunity,” he said in announcing acquisition legislation in March.

Kendall and Thornberry are the yin and the yang of meaningful acquisition reform. If the Pentagon’s acquisition machine is to become more attuned to the Digital Age, both men will have

to drive change.

Thornberry’s bill, on which Kendall’s office gave input, would remove obstacles to top military officials working on acquisition issues and require private-sector acquisition training for DOD personnel. It would also require DOD acquisition programs to come with written strategies that identify appropriate contract types and risk-mitigation tools.

Kendall largely welcomed the legislation but with at least two big caveats. He said he was wary of the overinvolvement of service chiefs in the acquisition process. He was also skeptical of the bill’s “dual-track” career path for military officers involving both combat and acquisition experience.

Those are significant but perhaps surmountable differences in Kendall’s and Thornberry’s approaches to the issue.

Avoiding ‘Groundhog Day’

There is a certain cynicism among longtime observers about the ability of anyone to tame the defense acquisition bureaucracy. As Tom Sisti, a senior director and chief legislative counsel at SAP America and a former adviser on acquisition in the Senate, put it last year, “We seem to be in a kind of procurement ‘Groundhog Day’ where we recycle through a lot of the same recommendations.”

An inexperienced government workforce and inadequate use of commercial technologies that were conceived outside

Rethinking acquisition

the traditional defense base are chronic problems that have loomed over the latest round of acquisition reform. Those challenges will outlast the tenures of Kendall and Thornberry, but the men's legacies

will likely be judged on how well their policies tackled such systemic issues.

Regardless of whether BBP 3.0 or any new law has a lasting impact on the defense acquisition system, the future

promises more work. Thornberry has said he has a database with more than 1,000 suggestions for acquisition reform that lawmakers will "continue to mine for years to come." ■

Acquisition after FITARA

OMB's implementation guidance gives agency CIOs new power — and increased accountability

BY ADAM MAZMANIAN

There are new rules of the road for federal agency IT acquisitions, and the bottom line appears to be that the CIO job is about to get a lot more powerful and potentially a lot more interesting.

On April 30, the Office of Management and Budget released proposed guidance for implementing the Federal IT Acquisition Reform Act, which was signed into law in December 2014.

As interpreted by OMB, the law not only strengthens the authority of agency-level CIOs over their agency and component CIO colleagues, but it gives them a role in determining how agencies will deploy IT to run government programs.

CIOs are directed to be involved in the pre-budget submission stage for

IT for specific federal programs and agency enterprise IT. CIOs are also tasked with reviewing and approving the IT portion of agency budget submissions. And they are authorized to define how their agencies' IT capital planning and project management are performed and to define metrics for reporting their progress.

Agencies must submit plans to OMB for how all that work will be accomplished according to a "common baseline." Each agency will have a chance to fine-tune OMB's interpretation of FITARA to give CIOs greater or lesser participation in planning and decision-making.

OMB also sought to allay fears that gridlock could result from having all IT roads lead to the CIO's office.

"This was an initial primary concern of many CIOs and agency executives," the guidance states. "In response, we created the CIO assignment plan to allow the CIO to assign, in a rules-based manner, certain responsibilities to other people in their department. This keeps the accountability with the CIO but allows each agency to realistically meet the law's requirements while minimizing the chance for bottlenecks."

Under FITARA, the agency CIO is now in charge of hiring component IT leaders, whether they are called CIOs or some other title. Agency-level CIOs also have a leadership role in the ongoing evaluation of technology leaders and are responsible for compiling and publishing a list of all the agency's CIOs.



"The proposal represents an important milestone in transforming FITARA from the letter of the law on paper to the reality in practice across the federal government."

REP. GERRY CONNOLLY (D-VA.)

The guidance touches on other areas of FITARA's legislative language, including strategic sourcing, data center consolidation, governmentwide software purchasing and IT acquisition cadres. But because those elements were so closely modeled on existing Obama administration initiatives, there wasn't much in the way of new material. Updates in areas that require fine-tuning to comply with FITARA will be released before the end of fiscal 2015.

One of the law's key architects is pleased with OMB's efforts.

"The proposal represents an important milestone in transforming FITARA from the letter of the law on paper to the reality in practice across the federal government," Rep. Gerry Connolly (D-Va.) told FCW. "Importantly, the draft guidance recognizes that effectively implementing enhanced CIO authorities requires that reforms be carried out across the entirety of an agency's C-suite leadership."

Connolly also stressed the importance of CIOs using the new powers they've been given.

"I look forward to working closely with the FITARA implementation team to further refine and enhance this proposal, particularly with respect to ensuring that agency CIOs utilize the full authority under FITARA to ensure that they have the right component agency CIOs in place now," he said.

Federal CIO Tony Scott said at a May 1 conference that the guidance is not so much about ramping up CIO authority as it is about rationalizing agency processes to accommodate the integral role that technology plays in government operations.

"There's nothing you can do, no business decision you can make that doesn't have some huge technology implication or impact," he said.

The window for public feedback on the draft guidance closed May 30, and OMB promised to review and incorporate suggestions, "as appropriate, to develop final guidance in the coming weeks." ■

Why reforms fall short

After two decades of good intentions, it's time for an enterprise strategy for IT acquisition and management

BY MICHAEL GARLAND

The Obama administration's early Office of Management and Budget initiatives and the Federal IT Acquisition Reform Act now being implemented all have been well-intentioned, but none has offered an over-arching IT strategy.

One of the main reasons that the Clinger-Cohen Act failed to rein in waste, and why all the intervening reform efforts have had only limited impact, is the absence of an enterprise organizational design for IT acquisition and management. There are guidelines, regulations and initiatives, but there is no centralized, integrated strategy supported by a corresponding organizational structure. The government has been intensely fragmented when it comes to IT acquisition.

Read in a vacuum, the pre-2015 OMB initiatives, many of which were memorialized by FITARA, are hard to criticize. Yet these well-meaning and hand-crafted initiatives have been trapped within a dysfunctional structure. The "25-Point Implementation Plan to Reform Federal IT Management" of 2010 was less a strategy than a tactical assault. It articulated 25 concrete steps to try to achieve particular short-term outcomes.

Likewise, 2012's effort, "Digital Government: Building a 21st Century Platform to Better Serve the American People," addressed the need to ensure

that the systems managing public data were designed to maximize the public's ability to use the data. Again, it was a component of a strategy, not an acquisition design.

Since Clinger-Cohen, most of the initiatives have been tantamount to designing beautiful windows and doors for a house that sits on a faulty foundation.

Government is not really an enterprise

At the core of the strategy vacuum is the oft-ignored reality that the government does not operate like a conventional enterprise. Rather, the government "manages" its IT like a holding company with a portfolio of many disparate assets. The current structural approach is to treat the agencies as independent entities with the ability to determine their own IT paths, guided by maxims such as "cloud first" and coupled with oversight at the budgetary level from OMB.

That approach lacks cohesion and inhibits the ability to develop and exploit best practices. It has been an ad hoc structure devoid of an enterprise strategy. The fragmentation also hinders the ability to develop valued expertise or deploy any of the various continuous improvement methodologies that have been so useful for the private sector.

The less-than-stellar results we've

Rethinking acquisition



At the core of the strategy vacuum is the oft-ignored reality that the government does not operate like a conventional enterprise. Rather, the government “manages” its IT like a holding company with a portfolio of many disparate assets.

MICHAEL GARLAND

seen, unfortunately, are exactly what one would expect from the government's current fragmented organizational structure. Imagine Walmart funding individual IT investments to be run independently and in parallel by its inventory, finance, sales, marketing and human resources departments — and then being surprised to learn they all chose different software systems to do similar things.

Clinger-Cohen inadvertently supported that approach, as have all the intervening initiatives and attempts at reform. All the efforts have stayed within the four walls of the dysfunctional fragmented structure and, therefore, have failed to produce significant improvements.

Back in 1996, centralized command and control lost its appeal with the Brooks Act's repeal because there was an impression that the General Services Administration's centralized IT procurement authority was a box-checking exercise that added no value. But the experience of the Brooks Act should not be dispositive. There was no aligned strategy under that law, and the same lack of alignment continues to plague the government's IT estate today.

When it comes to IT, the government would be wise to move beyond the holding company mentality. The citizenry has much at stake. It has a right to expect the success of the entire “enterprise” portfolio, not just that select individual agencies or sub-agencies can economically deploy IT.

William Cohen's iconic words, first published in the “Computer Chaos” report in 1994, still resonate: “Weak oversight...[has] led to the American taxpayers not getting their money's worth [on IT expenditures]. Effective management and control over such a significant portion of the budget is seriously lacking, and the federal government's problems with buying computers [are] widespread.”

Then-Commerce Department CIO Roger Baker's 2002 assessment, shared at the hearings leading up to the E-Government Act, is also still relevant. “There is no cohesive strategy, there are too many points of control...caused by ad hoc infrastructure,” Baker said. “We need somebody with the charter to look at federal government IT as an enterprise issue.”

A glimmer of hope?

On Dec. 4, 2014, Office of Federal Procurement Policy Administrator Anne Rung issued a memo calling for, among other things, enterprisewide vendor management. In that memo, Rung wrote: “Relationships with vendors are still managed individually across thousands of procurement units, which makes it challenging for both the acquisition workforce and the vendor community to drive improved outcomes. Mirroring other governments and industry, who manage industry relationships as a single enterprise, OFPP will, within 90 days of the date of this memorandum, develop a plan to recruit the federal government's first vendor manager

for top IT commercial contractors.”

That is a promising start! Since then, OMB and GSA have publicly announced a plan to deploy category management disciplines across IT product lines in order to better serve the entire government. This top-down strategy, if well executed, could put in place the first building blocks for a centralized view of the government's IT estate. It's also consistent with Congress' intuitive desire, represented in the early FITARA drafts and hearings, to put it all back together — to gain more centralized control — and to develop an enterprise IT strategy that results in an organizational structure for improved outcomes.

Let's keep our collective fingers crossed that this renewed interest in a governmentwide, enterprise approach to IT — including industry best practices such as category management — continues to gain momentum. If it truly takes hold, then transformative enterprise-oriented change could finally occur. ■

Michael Garland is a former vice president at BearingPoint Technology Procurement Services and senior vice president at Siemens Enterprise Communications, and is currently under contract with the federal government supporting IT acquisition modernization. This essay is excerpted from “Reforming IT Acquisition Reform,” Garland's thesis for a master of laws degree in government procurement at George Washington University Law School.

Federal Agencies, Cautiously, Target IT Shared Services

Shared services, in which organizations get common business and office services from a third party provider, has been a regular private sector and state and local government practice for years. The federal government has languished in its use of shared services, but the push is on to change that.

Beginning with the Federal IT Shared Services Strategy, released by the Office of Management and Budget (OMB) in May 2012, agency chief information officers are now expected to follow a “Shared First” approach to IT service delivery. Next generation shared services are one of the essential tools agencies will need “to successfully accomplish their missions in the face of tight resources and rising customer needs,” then federal CIO Steven VanRoekel said when the strategy was published.

That’s not debated, and there are clear signs that the move to shared services is accelerating throughout government. How to get there without disrupting agency functions, however, is still a concern.

A recent survey of agency chief financial officers by the Partnership for Public Service found that many have implemented select shared services initiatives, but “are not viewing widespread implementation as their priority, due in part to past experiences with shared services and the challenges of sustaining long-term transformation efforts.”

The Shared Services Strategy outlines three general categories of IT intra-agency shared services, to be delivered by designated

agency providers:

- Commodity, such as web site and content management, infrastructure and asset management, and email, help desk and collaboration.
- Support, such as records, human resources and financial management.
- Mission, such as performance management, geospatial IT, and federal health architecture.

As well as a direct savings in IT costs and the people needed to provide these kind of services in-house, the Shared First approach is designed to support the OMB’s PortfolioStat process, an annual evidence-based review of an agency’s IT investment that aims to identify those that are not “well aligned” with agency missions or business

been relatively easy to implement. Many agencies have already moved to such things as Google Apps for email, for example, and, increasingly, electronic archiving, records management, help desk and collaboration functions are outsourced to service providers.

Other parts need more help to put in place. In March 2013, the OMB issued a memo directing federal agencies “with limited exceptions” to use a shared service for future modernization of their core accounting and financial systems. The Treasury Department was given the job of evaluating how well agency proposals met this guidance, and to work with agencies and service providers to improve the way those

MOVING THE MORE COMPLEX AGENCY FUNCTIONS TO SHARED SERVICES HAS SHOWN MIXED SUCCESS.

functions, and can be cut back to free up funds for other purposes. It also leverages the use of strategic sourcing to help agencies get the lowest prices possible for their IT.

In May 2014, four agencies—Agriculture’s National Finance Center, Interior’s Interior Business Center, Transportation’s Enterprise Services Center and Treasury’s Administrative Resource Center—were named as Federal Shared Service Providers (FSSPs) for core accounting and other purposes. Agencies are expected to consider these providers when looking for these shared services, before looking to other providers.

Some of the Shared First vision has

financial services are delivered.

Moving the more complex agency functions to shared services has shown mixed success. In March 2015, for example, Health and Human Services (HHS) said it was halting the planned 2016 move of its human resources services to the Agriculture Department’s National Finance Center because of technical complexities and other issues. It might instead opt to go with a private sector services provider.

Ned Holland, assistant secretary for administration at HHS, said at a conference hosted by the Partnership for Public Service that a part of the problem with FSSPs was that they didn’t have the funding to make the kind of



improvements, such as software upgrades, needed to meet their customers' requirements. Under federal rules, they can't spend money until they have a signed contract in hand.

In its survey of federal CFOs, the partnership also identified other reasons why agencies are cautious about wholesale use shared services. They hesitate to transition vital agency functions without a clearer idea of the cost benefits, for example, as well as the need for more information about the performance of FSSPs. For that matter, many of the CFOs said they needed a clear idea about their agency's own performance and costs in order to build a business case for the move. Strategic workforce planning should also be integrated into decision-making on shared services.

In an October 2014 study by the Association of Government Accountants (AGA), two-thirds of the government executives surveyed said they have concerns about the quality of shared

services offered, while one-third eyed loss of control and cost management. Nevertheless, the AGA said, "Slightly more (were) confident than not that the move to shared service providers would make agency and government-wide operations more efficient."

Some agencies are already building expertise on shared services. HHS has a goal to "maximize the economic, architectural and operational value" of its shared services across the department and elsewhere, through the more than 50 services and products it offers. Likewise, the Treasury offers a range of services to both internal and external customers through its Shared Services Program, similar to those offered by its companion FSSPs.

Other agencies have for some time offered shared services closely tied to their core expertise. The National Oceanic and Atmospheric Administration (NOAA), for example, provides weather data and models to other agencies and to the private

sector. The Veterans Administration shares medical information services to the Defense Department, and is looking at how to expand shared services internally to help with its own business processes.

As one of the short-term goals for shared services, OMB said it will explore opportunities to actively expand the Shared First mandate beyond financial services to other administrative functions, and also more closely engage the larger government departments to see if they can share their internal shared services.

In an interview with Federal News Radio, OMB Controller Dave Mader said he expected between six and 10 agencies to move to shared service providers over the next three years. The question now is if the four FSSPs will be able to meet that demand, or if a commercial provider also needs to be added to the list.

"That analysis we are undertaking this fiscal year," he said.

A Quick Guide to Implementing Shared Services

Government organizations that want to implement IT shared services need to consider a range of issues, both technological and cultural, including a way for potential users to size up competing service offerings from providers.

The OMB's Federal Information Technology Shared Services Strategy, published in May 2012, is the basis for the government's current push to expand the use of shared services in agencies, as a way to both cut the costs of IT acquisition and improve the effectiveness of IT.

As a part of that, the OMB lists a number of things as critical for the success of any agency implementation of shared services, including "robust connectivity and agile cloud computing" as the primary technical elements. Along with that go such things as business process re-engineering, cultural change to overcome "loss of control" issues, and a buy-in by agency executives.

The federal CIO Council expanded on that a year later, with the Federal Shared Services Implementation Guide. It made executive commitment the first requirement since, without that, "identifying agency areas that make the most sense for migration

to shared services, and facilitating those migrations, along with the organizational changes that accompany them, will be prohibitively difficult."

That's backed by the results of several recent surveys of agency chief financial officers and IT managers that put much of the blame for a slow adoption of IT shared services in government on executives' reluctance to buy in to the shared services business case.

Beyond that, agency enterprise architectures will provide the structure needed to identify the Shared First approach that needs to be taken, along with a three-to-five-years

list of targets for shared services and, importantly, what areas are not viable candidates for shared services.

The council lists a step-by-step approach that agencies can take to implement shared services:

- Inventory, benchmark and assess current internal functions and services.
- Identify potential shared service providers.

- Decide post-deployment operations and management.

More recently, the Partnership for Public Service, which conducts various workshops on shared services throughout the year to get input from both government and private sector sources, said it discovered a “lack of a transparent and competitive shared services marketplace” that would let

• Conduct an assessment of current costs and performance of management activities to assess what the benefits would be of moving to shared services, and to provide key metrics for that.

- Reduce the risks for agencies moving to shared service providers by interoperability standards for similar service areas.

• Adopt joint performance standards for providers and customers to ensure both parties are meeting their obligations in a migration services.

- Create a centralized government-wide catalog or database of available shared services.

This will require the participation of multiple players, including the OMB, the General Services Administration, Congress, federal shared service providers, customer federal agencies and the private sector, the partnership said.

MAKE A GO/NO GO DECISION ON WHETHER TO IMPLEMENT SHARED SERVICES.

- Analyze legacy services to shared service providers.
- Make a go/no go decision on whether to implement shared services.
- Fund the services.
- Negotiate inter-agency and service level agreements.

agencies assess providers based on past performance, and ensure their compatibility with current agency systems.

It recommended a series of actions government can take to build that marketplace:



Program Support Center

MANAGING
THE BUSINESS OF
GOVERNMENT™

**In 2014 PSC helped our customers procure nearly
\$360 million in IT equipment, products, and services.**

As a Federal Shared Services Provider,
PSC is ready to support your agency's mission.

Visit www.psc.gov

Program Support Center • 7700 Wisconsin Avenue, Suite 920, Bethesda, MD 20857 • P: (301) 492-4600 • www.psc.gov



THE 'ISIS'

ON DOD NETWORKS

From Kuwait to Honolulu, the war with Islamic State militants is changing how the U.S. military communicates

BY SEAN LYNGAAS

AP IMAGES



In bombing the Islamic State group beginning last August, the Pentagon turned to a familiar method with an unfamiliar underpinning. The U.S. military once again employed its vaunted air power, but effectively communicating across the services and with allied countries required an entirely new infrastructure.

It had been a few years since the military withdrew from Iraq and took with it the communications networks that supported fighting there. Enter Brig. Gen. Garrett Yee, who arrived at the Army's 335th Signal Command post in

Kuwait last May to what he described as a "Sleepy Hollow" atmosphere in which the main focus was withdrawing equipment from Afghanistan.

"We used to have quite the network [in Iraq], and when we left in 2011, we took it all with us," he told FCW.

The 2007 surge in Iraq, which ramped up the number of U.S. troops there to about 170,000, was accompanied by a surge in communications infrastructure. The U.S. military laid miles of fiber-optic lines in Iraq and used a variety of methods to communicate among bases and troops, said Bob Stasio, who led an

Army signals intelligence platoon in Iraq at the time.

The priority that commanders placed on turning the war around empowered field officers to request a range of communications equipment that might help the cause, Stasio said. His unit, for example, was one of the first to use Forward Battle Communication Command and Control Systems, which he described as a "localized network that ran on terrestrial point-to-point radio communications." His platoon could track Stryker vehicles using GPS and send voice and digital dispatches to the vehicles.

But much of that equipment had been stripped away. "When we left Iraq, we left hook, line and sinker," said Stasio, who is now a fellow at the Truman National Security Project. "We didn't keep those [forward operating bases]. We gave them to the Iraqis, so we pretty much took all that stuff with us or left it there. And [what we did leave,] probably ISIS owns most of it now."

To get the military's communications up and running again in Iraq in the past year, Yee and his team initially relied on the U.S. embassy's communications infrastructure but almost immediately outgrew it. The next step for Yee, who is commanding general of the 335th Signal Command, was to set up satellite terminals in cities such as Baghdad, the Kurdish capital of Erbil and Taji, where U.S. military advisers have trained Iraqis to fight the Islamic State group.

Like adding an app

The satellite terminals that connected U.S. military personnel to other bases throughout the world were but a stepping-stone for Yee. Another tool provided much more bandwidth and security and allowed the military to make the jump from tactical to strategic communications, he said.

“What we don’t want to do is create more of a burden on our allies and partners to have to stand up multiple networks and network infrastructure in order to be able to communicate with different segments of the U.S. Defense Department.”

— REAR ADM. NANCY NORTON

That tool is known as a Technical Control Facility in a Box. The apparatus consists of a few dozen transit cases that each hold a router and a core switch, and it takes about a day to assemble. TCFB allows for secure emailing and file sharing among network users. In the past year, Yee has made four trips to Iraq to get the communications network up and running, with the goal of having several U.S. allies using the system in the next few months.

The U.S. military is developing similar networks elsewhere in the world, Yee said, but today’s air strikes on the Islamic State group, much like the 2007 surge, are making better communications in the region a priority. The anti-Islamic State coalition is providing an impetus “to move this effort along more aggressively,” he said. “As it matures, it will be easier to use, [and] we’ll have more services available to it.” He compared that incremental progress to adding applications to an iPhone.

This is the U.S. military’s third attempt to set up a coalition communications network in either Iraq or Afghanistan, Yee added. In 2006, the Defense Department used a system called Centrix that was supposed to enable communication with allies in Iraq via a classified network, but “it just became another computer box” because it was ineffective, he said.

TCFB could represent a turning point, though. “If we get this right, then hopefully this can help enable us to have a DOD-wide solution,” he said. The project has the backing of Brig. Gen. Peter Gallagher, director of Central Command, with whom Yee said he has worked closely.

Stasio said one of the lessons he drew from his experiences in Iraq was not prescribing a “one-size-fits-all solution” to tactical communication needs on the battlefield. Yee seems to be applying that lesson through TCFB.

The Asia IT pivot

While Yee was setting up telecom-in-a-box capabilities in Iraq, his colleagues halfway around the world were working on a broader project. Their goal was to communicate quickly and discreetly across the vast Pacific Command, which stretches from the U.S. West Coast to India.

Military communications in the Pacific are not as structured as they are in, say, continental Europe, which is defined by NATO networks, said Rear Adm. Nancy Norton, who until March was the Pacific Command’s director of command, control, communications and cyber. A humanitarian assistance operation in Southeast Asia, for example, might entail an ad hoc group of countries working together on a project for which there is no preexisting communications protocol, she added.

“Our networks don’t have the ability to flex that well and that quickly, and our approval processes aren’t currently set up to be able to support that very quickly,” Norton told FCW.

She said she was concerned that the ad hoc nature of Pacific Command communications could hinder the way countries such as Australia took part in the fight against the Islamic State group. “What we don’t want to do is create more of a burden on our allies and partners to have to stand up multiple networks and network infrastructure in order to be able to communicate with

different segments of the U.S. Defense Department,” she said.

And so Norton turned to something called the Joint Capability Technology Demonstration to tackle the Pacific Command’s communications riddle. JCTD is a common network divided into “virtual enclaves” that offer participants separate secure channels of communication. The network architecture can be assembled quickly and is well suited to the ad hoc coalitions Washington works with in the Asia-Pacific theater, according to Norton.

As with Yee’s telecom-in-a-box, Central Command has expressed strong interest in the communication tool Norton implemented. That’s because “the long-term Afghan mission network that we had in support of Afghanistan isn’t what we now need” for the fight against the Islamic State group, she said.

And like Yee’s work, JCTD could outlast a war against the Islamic State that U.S. commanders have said might take years. Norton said the network architecture is “becoming the foundation for the Joint Information Environment...that all of the combatant commands across the world are working toward because we all have similar requirements for this.”

Thus, the war against ISIS is helping drive JIE, a DOD-wide IT initiative that has been largely abstract until now. If the projects initiated by Yee and Norton are any guide, the future of military communications will be defined by nimble, ad hoc methods capable of being quickly packed up and sent to the next conflict, thousands of miles away. And commanders will be able to see very quickly just how much these new unified communications systems can help troops in the field. ■

Are agencies really ready for the Internet of Things?

From storage to security, the risks are significant — but ignoring the IoT is not an option

BY ZACH NOBLE

It's a hydra-headed opportunity and test — and it's not something agencies can afford to ignore.

The much-hyped Internet of Things (IoT) is exponentially more risky, rewarding and challenging than yesterday's tech arrangements. Increasingly connected, sensor-laden and data-driven systems are poised to change everything from national security to office-space management. But they generate more data and complexity than many agencies are comfortable managing, which means serious changes are on the horizon.

Cisco Systems predicts the IoT will generate \$4.6 trillion for the public sector before 2025, in value added and costs saved. And although the General Services Administration has not yet come close to those sorts of returns, the agency — which manages nearly 10,000 government-owned buildings around the country — has pioneered IoT building management with its GSALink initiative.

Collecting 29 million data points per day from myriad sensors throughout its buildings, GSA is able to monitor everything from light use to humidity, enabling the agency to boost productivity and promote good health by optimizing conditions when workers are present and saving on energy costs when they're not.

Other big adopters include the intelligence community and

the Defense Department. Warfighters can benefit from sensors that improve their tactical awareness, while vitals monitors can help commanders know who's healthy or injured.

"I do see the Defense Department out in front [of IoT]," said Gary Hall, chief technology officer for Federal Defense at Cisco.

Hall added that there is plenty of room for crossover. Municipal experiments with smart lighting or parking, for instance, could inform similar adoption on agency campuses or military bases. "I've been on a lot of military bases, and the parking situation could certainly be improved," he quipped.

At its core, the IoT consists of Internet-connected objects — such as computers, thermostats or simple sensors that ping a single data point — and the networks to which they're connected.

The term "Internet of Things" refers to the physical elements of a connected network — the "things" — while the term "Internet of Everything" is used to refer to the whole shebang: servers, sensors, data flows between them, people interpreting the

data and even people talking to other people about the system.

And as with all seismic shifts, the people will wind up mattering just as much as the tech.

Quick stats

50 billion

Number of Internet-connected "things" that will be online by 2020

\$4.6 trillion

IoT's value for the public sector

70/30

Percent of IoT benefit that will be agency-specific vs. percent that will come from cross-agency adoption

x4

IoT's force-multiplier effect

Source: Cisco Systems

'Humans can't deal with the volume'

With massive scope comes management trouble. The IoT's hurdles revolve around the problem of too much: too much data, too many new security holes to plug and too much guidance, not all of it useful.

Even simple storage becomes an issue. The number of connected "things" is expected to balloon from around 16 billion today to 50 billion by 2020, with skyrocketing data generation spurring a need for a 750 percent expansion in data center capacity.

Hall pointed to the problem of "big, large data" because both the overall volume and the size of individual files have exploded. That creates a need for pre-processing with machines rather than people.

"Humans can't deal with the volume of data we're producing," Hall said.

The security risks are also enormous.

Each Internet-connected object could theoretically become a point of entry for hackers. At a conference in April, Martin Scott, general manager of Rambus' Cryptography Research Division, cited IDC estimates that within two years, 90 percent of all IT networks will face an IoT-based security breach.

Ron Ross, a fellow in the National Institute of Standards and Technology's Computer Security Division, recently labeled the IoT practically indefensible.

"As we see continued innovations in information technology and that technology is increasingly connected through wireless networks in things like cell phones, cars and appliances, we get a simultaneous increase in complexity," Ross told FCW. "That means an increase in the potential 'attack surface' that is now an inherent part of that IT infrastructure, giving adversaries more opportunities to penetrate and compromise our IT systems and cause problems."

Several experts pointed to the 2013 Target breach as the classic example of that broad attack surface being exploited. Security credentials stolen from a heating, ventilation and air conditioning contractor hired to remotely monitor stores' energy use gave hackers access to Target's point-of-sale systems and credit card information.

Official instructions are of limited help. Ross said agencies are "drowning in guidance," yet clear, actionable guidelines for IoT adoption are still scarce. To remedy the situation, NIST's Cyber-Physical Systems Working Group is developing guidance to lead agencies through the process of creating resilient systems.

Securing networks, handling data

The consensus among IoT experts is that agencies cannot avoid the issue any longer, and those that have not started planning IoT implementations are behind the curve.

"This is the next big disruption. It's important that we aren't so afraid of the fear of attack that we don't realize the value."

GARY HALL, CISCO

Awareness is crucial. It's important to know what's on your network and how it's supposed to behave before any attack occurs, said Peter Romness, a business development manager at Cisco, at a recent GovLoop seminar.

"If a sensor that's supposed to relay temperature and humidity starts to take information from your network, that's a warning sign," he said.

But he added that there is no "silver bullet" defense, so agencies must prepare to both prevent attacks and manage inevitable intrusions.

"It's not a question of if you're going to get hacked, it's a matter of when," he said. Even before the number of connected devices explodes, "you probably already have some malware in your network."

Hall advocated protection at the data level and putting advanced encryption on devices. Adopting a coherent plan for normalizing data is also essential.

"When you're dealing with different systems, different vendors, in different buildings, getting them to talk together was a challenge," said GSA spokesman Matthew Burrell. "As the blurry line between industrial systems and IT systems becomes more clear, we are finding that it is critically important to work with industry to homogenize the data so that one system's data stream and reporting capability is the same as the next."

Prepping employees for the change is also crucial, he added. "Don't wait till the end to deal with the people."

Yet despite all the challenges, the IoT is a wealth of transformative potential.

"The biggest lesson has been that this is not just a technology tool, this is a technology 'way of doing business,'" Burrell said. "It affects process, workflow, training and even vendor contracts."

"This is the next big disruption," Hall said. "It's important that we aren't so afraid of the fear of attack that we don't realize the value."

For agencies that haven't yet embraced the IoT, he added, "it's not something they can avoid." ■

FCW Index

People

Baker, Roger 24	Gavino, Amando ... 10	Romness, Peter..... 32
Balutis, Alan..... 16	Grassi, Paul 8	Ross, Ron 32
Bruch, Lisa 20	Hall, Gary 31-32	Rung, Anne 24
Burrell, Matthew.... 32	Haines, Fred..... 10	Scott, Martin 32
Carter, Ashton.... 15, 16, 20-21	Hawkins, Ronnie..... 9	Scott, Tony..... 23
Clapper, James..... 9	Johnson, Jeh 16	Sisti, Tom..... 21
Clark, AJ..... 15	Kelman, Steve 16	Snowden, Edward..... 16
Connolly, Gerry 23	Kendall, Frank 15, 21-22	Sones, Jimaye 9
Crum, Maynard 9	Leff, Mike 20	Stasio, Bob 29-30
Davie, Mary 19-20	McCain, John..... 21	Tarasiuk, Al 9
Dorris, Martha..... 9	McClure, Dave 14	Thornberry, Mac..... 21-22
Gallagher, Peter..... 30	Neffenger, Peter..... 9	Warren, Steph..... 3
Garcia, Michael..... 8	Norton, Nancy 30	Yee, Garrett..... 29-30
Garland, Michael..... 23-24	Obama, Barack 9	

Agencies/Organizations

Amazon 15	NDIA 15
Army 29-30	NIST 8, 32
AT&T 20	NSA 16
Central Command 30	OFPP 24
CenturyLink..... 20	OMB..... 22-24, 34
CIA 15	Pacific Command 30
Cisco 16, 31-32	Rambus 32
Coast Guard..... 9	SAP America 21
Congress 21-24	Thermopylae Sciences and Technology..... 15
DHS..... 8, 16	Truman National Security Project..... 29
DISA..... 9	TSA 9
DOD 9, 15, 16, 20-22, 28-30, 31, 34	VA..... 3
Forrester Research 10	Veris Group 14
GSA..... 9, 10, 19-20, 24, 31-32	White House 9, 23
Harvard..... 16	

Advertisers

CDW Government, Inc

www.CDWG.com **11-13**

FCW Rising Stars Nominations

www.FCW.com/2015risingstars **17**

Fedbid, Inc.

www.FedBid.com **36**

InterSystems Corp.

www.InterSystems.com/federal1CC **35**

Panasonic Corporation of North America

www.us.panasonic.com/toughpad **1a-1b**

QTS

www.qtsdatacenters.com **6-7**

The Federal IT Acquisition Summit

http://fcw.com/fias **2**

U.S. Department of Health and Human Services

www.psc.gov **27**

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.

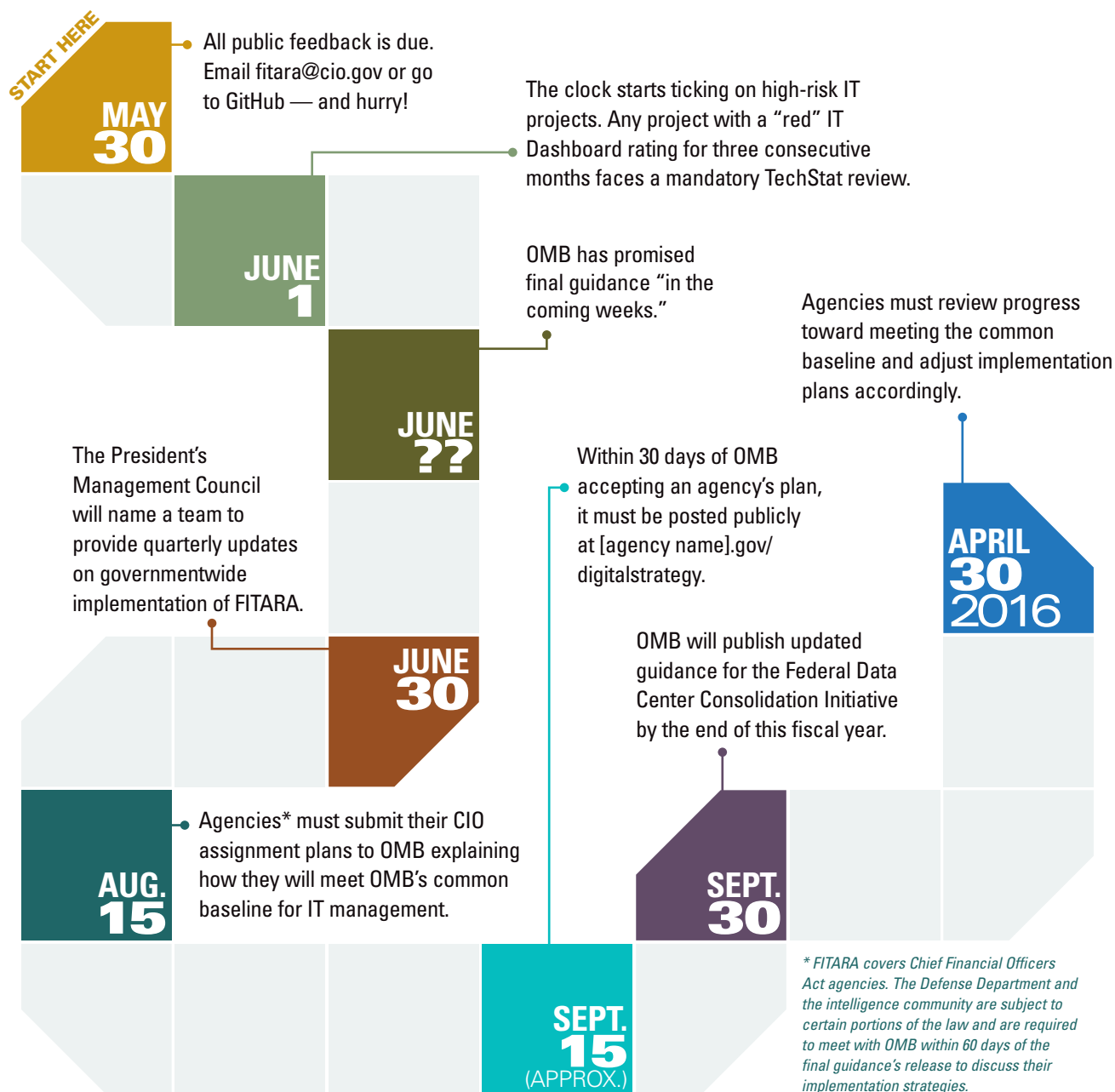
FCW (ISSN 0893-052X) is published 18 times a year, two issues monthly in Mar through Sep, and one issue in Jan, Feb, Oct and Dec by 1105 Media, Inc., 9201 Oakdale Avenue, Ste. 101, Chatsworth, CA 91311. Periodicals postage paid at Chatsworth, CA 91311-9998, and at additional mailing offices. Complimentary subscriptions are sent to qualifying subscribers. Annual subscription rates payable in U.S. funds for non-qualified subscribers are: U.S. \$125.00, International \$165.00. Annual digital subscription rates payable in U.S. funds for non-qualified subscribers are: U.S. \$125.00, International \$125.00. **Subscription inquiries, back issue requests, and address changes:** Mail to: FCW, P.O. Box 2166, Skokie, IL 60076-7866, email FCWmag@1105service.com or call (866) 293-3194 for U.S. & Canada; (847) 763-9560 for International, fax (847) 763-9564. **POSTMASTER:** Send address changes to FCW, P.O. Box 2166, Skokie, IL 60076-7866. Canada Publications Mail Agreement No: 40612608. Return Undeliverable Canadian Addresses to Circulation Dept. or XPO Returns: P.O. Box 201, Richmond Hill, ON L4B 4R5, Canada.

©Copyright 2015 by 1105 Media, Inc. All rights reserved. Printed in the U.S.A. Reproductions in whole or part prohibited except by written permission. Mail requests to "Permissions Editor," c/o FCW, 8609 Westwood Center Drive, Suite 500, Vienna, VA 22182-2215. The information in this magazine has not undergone any formal testing by 1105 Media, Inc. and is distributed without any warranty expressed or implied. Implementation or use of any information contained herein is the reader's sole responsibility. While the information has been reviewed for accuracy, there is no guarantee that the same or similar results may be achieved in all environments. Technical inaccuracies may result from printing errors and/or new developments in the industry.

**PUBLIC SECTOR
MEDIA GROUP**
CORPORATE HEADQUARTERS
9201 Oakdale Ave., Suite 101
Chatsworth, CA 91311
www.1105media.com

What comes next for FITARA implementation

If you move fast, you might still be able to submit your feedback on the Office of Management and Budget's draft implementation guidance for the Federal IT Acquisition Reform Act (see Page 22). Barring major revisions, here's what happens now:



Source: OMB's draft implementation guidance for FITARA, available at management.cio.gov

A close-up photograph of a young Black man with short dark hair, smiling warmly at the camera. He is wearing a white hospital gown with a blue collar and a small pattern. He is lying in a hospital bed with white pillows and bedding in the background.

**“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](https://www.intersystems.com/Federal1CC)

INTERSYSTEMS®

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

Power up to Meet Your Small Business Utilization Goals With the Click of a Button.

**\$3.5B AWARDED
TO SMALL
BUSINESSES
THROUGH
FEDBID:**

16,227 AWARDS

\$808 MILLION TOTAL

TO VETERAN-OWNED SMALL BUSINESSES

13,657 AWARDS

\$715 MILLION TOTAL

TO DISADVANTAGED SMALL BUSINESSES

10,059 AWARDS

\$629 MILLION TOTAL

**TO SERVICE-DISABLED VETERAN-OWNED
SMALL BUSINESSES**

10,355 AWARDS

\$395 MILLION TOTAL

TO WOMEN-OWNED SMALL BUSINESSES

5,104 AWARDS

\$301 MILLION TOTAL

TO HUBZONE SMALL BUSINESSES

**Data based on Fiscal
Years 2012 – 2014*

Visit www.FedBid.com to learn more.

FedBid®