



THE BUSINESS OF FEDERAL TECHNOLOGY



## Agile in action

PAGE 20

## Halvorsen and Silicon Valley

PAGE 22

## The 'fair and reasonable' pricing trap

PAGE 30



**VS**



## **BUY**vs**BUILD**

It's a timeless question  
— and the answer  
might not be as clear-cut  
as agencies think

PAGE 16

# ENDURING SUPPORT

Logistics & Training

Life-Cycle Support Services

Supply Chain Management

Systems Integration

Maintenance & Modifications





 **BOEING**

## A successful cyber sprint, with a questionable finish line

The federal government's 30-day cybersecurity sprint wound down on July 12, but the work is far from over.

U.S. CIO Tony Scott told reporters on July 9 that the initial news seemed good.

The memo announcing the sprint called for agency CIOs to scan for "indicators of compromise" listed in the U.S. Computer Emergency Readiness Team's Analysis Report and inform the Department of Homeland Security immediately about any evidence of malicious cyber activity; patch critical vulnerabilities; accelerate implementation of multifactor authentication, with a priority on privileged users; and tighten policy and practices for those users.

Scott said agencies had dramatically increased two-factor authentication for privileged users during the sprint, and "a number of agencies have hit 100 percent." Governmentwide, two-factor authentication increased 20 percent, he added.

Chris Edwards, chief technology officer at identity management firm Intercede, praised the sprint for pushing two-factor authentication.

"It is certainly needed as the first

line of defense and does significantly raise the bar for hackers to clear," he told FCW. "It should also be one of the simplest first steps to take. Even if you can only enforce smart card systems logon for 95 percent of the workforce, that still greatly reduces the number of people who actually have a password that can be phished, intercepted or guessed."

However, agencies leave "username/password 'back doors' to support certain legacy systems," Edwards said, and that approach undermines two-factor authentication.

"Additionally, relying on incoming perimeter defenses alone does little to reduce the impact of Trojans and other [advanced persistent threat] software if that is able to acquire systems-level permissions and leak data over a long period of time," he said.

Ralph Kahn, vice president of federal at security firm Tanium, told FCW that the "urgent but fairly broad" language of the sprint memo was a good approach.

"You risk setting up agencies to fail" if you list specific demands, he said, adding that the open language hope-

fully prompted fuller participation from agencies in desperate need of an honest look at their cybersecurity situations.

He said the patch issue is one of the most crucial problems. "In many cases, agencies just don't know" where they stand with software patches, he said, noting that many run legacy systems for which patches aren't available or rely on "incomplete tools" that might report issues have been patched when they haven't.

"That whole patching thing is a lot more complicated than a 30-day sprint would indicate," Kahn said.

And although Scott said the sprint has "greatly enhanced the cybersecurity profile of the U.S. government as a whole," many experts have cautioned that cybersecurity is a complex, long-haul proposition.

"Cybersecurity...is not a sprint, it's a marathon," said Gregory Wilshusen, director of information security issues at the Government Accountability Office, during a congressional hearing on July 8. "It needs to be going on a continuous basis."

— Zach Noble

### FCW CALENDAR

#### 8/19 CDM

The Department of Homeland Security's Jim Quinn and the General Services Administration's Chris Hamm are among the speakers at this FCW event on the next steps toward improving agencies' security posture. Washington, D.C.

[fcw.com/cdm](http://fcw.com/cdm)

#### 9/2 Acquisition

Washington Technology's Department of Health and Human Services IT Day will dig into specific fiscal 2016 acquisitions at the Food and Drug Administration, Centers for Medicare and Medicaid Services and other HHS components. Falls Church, Va. [is.gd/WT\\_HHS\\_IT](http://is.gd/WT_HHS_IT)

#### 9/2 Defense

Brig. Gen. Mark Weatherington, the Joint Staff's deputy director for C4/cyber, and Veterans Affairs Undersecretary for Benefits Allison Hickey are among the speakers at AFCEA NOVA's Joint Warfighter IT Day. Vienna, Va. [is.gd/AFCEA\\_defense](http://is.gd/AFCEA_defense)



# Contents



## 16 **TECHNOLOGY** **Buy or build?**

It's a timeless question — and the answer might not be as clear-cut as agencies think

BY BRIAN ROBINSON

## 20 **INNOVATION** **How one company is embracing agile**

CivicActions offers an inside look at how it is using agile development to respond to 18F's RFQ

BY ZACH NOBLE

## 22 **DEFENSE** **Terry Halvorsen's Silicon Valley trip shakes up JRSS**

Peeks at new tech convince the Pentagon's CIO to ask for things once thought impossible

BY SEAN LYNGAAS

## 30 **DRILL DOWN** **A better path to fair and reasonable pricing**

The Commercial Sales Practices approach sets a trap that can snare even diligent contractors. Government and industry both deserve a smarter solution.

BY MICHAEL GARLAND

## TRENDING

### 4 **CYBERSECURITY**

A successful cyber sprint, with a questionable finish line

### **FCW CALENDAR**

Where you need to be next

### 8 **INDUSTRY**

Pentagon's Silicon Valley unit gets \$1.75M for fiscal 2015

### 9 **POLICY**

Justice Department seeks new authorities to fight cybercrime

### 10 **SPECTRUM**

Obama administration is nearly halfway to its spectrum goal, and Halvorsen emphasizes 'secure enough' mobility

### 11 **MANAGEMENT**

State got high marks for managing records under Clinton, and lawmakers propose taking the clearance system away from OPM

## DEPARTMENTS

### 12 **COMMENTARY**

Finding security in the cloud

BY PETE NICOLETTI

NS2020 EIS: Another step forward for GSA

BY BOB WOODS

U.S. must do more to protect privacy

BY JULIE M. ANDERSON

### 24 **EXEC TECH**

An explainer on containers

BY WILL KELLY

### 26 **BOOKSHELF**

Cracking the code on past performance

BY MARK ROCKWELL

### 33 **FCW INDEX**

### 34 **BACK STORY**

What primes say about subs



**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,  
Will Kelly, John Moore, Brian Robinson,  
Sara Lai Stirland

**Editorial Fellows** Eli Gorski, Jonathan Lutton,  
Bianca Spinosa

**Editorial Assistant** Dana Friedman

**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 Szenker, 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



# Security Awareness

## How secure are you?

### Assess and Identify vulnerabilities of your network's security

Network security's passive nature forces validation of its effectiveness to a time of attack. Your weaknesses are not identified until after your security is breached — if even then.

#### Some questions you should ask:

- ▶ Are you aware of any external security breaches into your environment?
- ▶ Have your websites been subjected to attacks?
- ▶ Do you have a firewall? Is your firewall secure?
- ▶ Are your servers and workstations secure and patched?
- ▶ Do you have sufficient virus and spyware protection on your network?
- ▶ Are your wireless devices secure?



## PCMG's Enterprise Security Assessments identifies and provides actionable recommendations:



#### Network Assessment

*Real-world assessments of your network and website protection from external sources-leveraging the same strategies and tools that hackers employ today.*



#### Environment Assessment

*Professional assessments of your internal security, permissions, and network protection-leveraging the same tools that provide access throughout your environment.*



#### Expert Advisement

*Professional recommendations on securing your environment. PCMG's engagement is fast, built by network security experts, and delivered by our experienced engineers.*

Let our team of experts give you the best security options for your organization.

**Contact your PCMG Account Executive to get started today.**

**1-800-625-5468.**

#### Federal Government Wide Acquisition Contracts

- GSA Contract: GSA-35F-5946H
- NASA SEWP V Contracts: NNG15SC18B and NNG15SC44B
- Netcents-2: FA8732-14-D-0006

# PCMG

1.800.625.5468 | [pcmg.com](http://pcmg.com)

## MSPB: Hack not to blame for IT failure

The Merit Systems Protection Board suffered a systemwide network failure that could result in the permanent loss of some of its data.

The lost data had been stored via VMware's virtual desktop infrastructure. Efforts are underway to recover data from backup tapes as far back as November 2014.

However, files dating to late May of this year could be unrecoverable, according to email messages obtained by FCW.

The outage began on June 30, the same day that MSPB switched its employees to the virtual desktop interface and deactivated its virtual private network connection.

The work of all 219 MSPB employees has been affected. Since the outage began, they have been able to access the agency's systems via the Internet version of VMware but not the desktop client.

According to an MSPB statement, the outage "was not the result of any external cyber intrusion or hacking."

The agency's website, MSPB.gov, was down sporadically, and the electronic filing service (e-Appeal Online) was also down, which affected federal employees who were appealing dismissals or suspensions, or filing pension claims.

Because of the disruption, people filing with MSPB were eligible for an extension, provided they stated that the outage was the cause of a missed deadline.

As of press time, e-Appeal Online was functioning, although users were cautioned to expect some sluggishness. MSPB said documents submitted electronically by appellants or counsel in open cases were probably not lost.

— Adam Mazmanian

## Pentagon's Silicon Valley unit gets \$1.75M for fiscal 2015

The Defense Department's full-time outreach office in Silicon Valley is up and running after Deputy Secretary Robert Work directed that \$1.75 million be allocated to it in fiscal 2015 and \$5 million from 2016 to 2019.

The Defense Innovation Unit Experimental will be staffed by a Senior Executive Service official and a handful of reserve officers and civilian employees, among others. According to a USAJobs notice, the SES position involves cultivating relationships with local tech gurus and small businesses, broadening the Pentagon's access to technologies for use beyond the intelligence community, and serving as a broker between acquisition officials and technology executives.

"While the department is beginning to focus on innovation in the commercial technology sector, a more concerted effort is needed," Work wrote in a

memo. The office's mission will be "to strengthen existing relationships and build new ones, scout for breakthrough and emerging technologies, and function as a local interface node for the department."



Robert Work said the new office will be a focal point for DOD's outreach to startup companies.

Defense Secretary Ashton Carter announced plans for the office while on a trip to Silicon Valley in April. The goal is to tear down what some say is a bureaucratic wall between the Pentagon and innovative startup companies. The Air Force has since revealed that it is setting up its own outreach office.

Carter traveled to Sun Valley, Idaho, earlier this month to attend a meeting of technology business leaders and pitch them on the "importance of a strong partnership between private-sector innovators and government," according to a Pentagon statement.

— Sean Lyngaas

### INK TANK





## Justice Dept. seeks new authorities to fight cybercrime

The Justice Department and some lawmakers are concerned about potential gaps in the government's ability to prosecute cybercrimes under the Computer Fraud and Abuse Act, and are seeking to update the law to reflect the challenges of cyberspace.

The law dates back to 1986. "Technology has changed a great deal since then," said Sen. Lindsey Graham (R-S.C.) at a hearing of the Senate Judiciary Committee's Crime and Terrorism Subcommittee earlier this month.

David Bitkower, deputy assistant attorney general in the Justice Department's Criminal Division, agreed. "We do have currently authorities and capabilities to address a vast array of cybercrime, but we have observed through prosecutions and investigations we've

done that there are gaps in certain areas," he said.

He added that a recent federal appeals court decision has led circuit courts to differ in their application of parts of the law. Additionally, some uses of technology by cybercriminals are not covered in the statute.

Security experts have expressed concerns about an Obama administration proposal that would target certain categories of insider threats by punishing individuals who exceeded their authorized access to a computer.

The goal is to prosecute employees who use private information on their company or its customers for nefarious purposes.

However, security researchers said the measure could compromise their

efforts to probe sites and services for weaknesses.

"We understand that creating a carve-out is a challenge [because] often researchers' efforts mirror those of cybercriminals, despite radically different intentions," said Jen Ellis, senior director of community and public affairs at security firm Rapid7, at the hearing. "We strongly urge the committee to consider this problem and whether there is a way to create an exemption for research, perhaps based around intent or outcomes."

Bitkower said the updates were not intended for trivial or unknowing violations or for researchers or security professionals. "We're not interested in prosecuting those cases," he said.

— Adam Mazmanian

### EDITOR'S NOTE

## Are we seriously talking about shutdowns again?

It might not feel that way for cash-strapped agencies, but the past two years have been relatively stable on the budget front. As we move toward Oct. 1 and fiscal 2016, however, that's about to change.

Come Sept. 30, the deal struck in December 2013 to lift the Budget Control Act caps expires — which means sequestration is back.

Congressional Republicans have been moving appropriations bills that adhere to those spending limits, while Democratic legislators and the White House are asserting that the resulting cuts are non-starters.

And although we have two full calendar months until fiscal 2015 funding expires, there are far

fewer legislative days available for Congress to hash out a funding deal. Longtime budget analyst Stan Collender, who recently pegged the likelihood of a shutdown at 33

percent, noted that there are less than a dozen real workdays for Congress between now and Oct. 1 — and many of them are already promised to non-appropriations issues.

In theory, a budget deal is still possible, but the realistic best-case scenario is yet another continuing resolution to extend funding into December, with Congress returning for a special session to work out fiscal 2016 funding then. And if one side miscalculates — or if even a handful of legislators dig in their heels — then we may once again see systems

powering down and federal workers staying home to start the fiscal year.

Technology, of course, is not a sticking point in the budget debate, but the federal IT community will feel the fallout nonetheless. Even if a continuing resolution is passed without drama, we're still looking at another autumn without the budget clarity needed to plan and properly manage programs.

The relative stability of fiscal 2015 helped federal IT get out of its defensive crouch. So it's truly unfortunate that, as Rep. Nita Lowey (D-N.Y.) recently put it, "the fall is shaping up to be the most predictable — and, really, avoidable — budget crisis in memory."

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



## IN THE IT PIPELINE

**WHAT:** A request for proposals from the Intelligence Advanced Research Projects Activity for its quantum computing Logical Qubits (LogiQ) Program.

**WHY:** The intelligence community has been pushing for a new computing model to tackle its exploding data processing needs. IARPA's RFP is the next step in the quest to develop a new quantum bit (qubit) circuit design. Quantum computers process huge amounts of data, which would provide a substantial leap forward.

Quantum computing, however, is inherently unstable because qubits can "flip" unexpectedly and introduce serious errors into the computations. IARPA said it wants to "build a logical qubit from a number of imperfect physical qubits by combining high-fidelity multi-qubit operations with extensible integration."

That's a complex way of saying the organization is looking for a more efficient way to scale quantum computing systems.

According to the solicitation, success in building practical quantum computers hinges on the ability to control for the errors in quantum gates, which can be achieved by finding a way to encode physical qubits into a logical qubit.

The deadline for the initial round of proposals is Sept. 1. The LogiQ Program is slated to begin Feb. 1, 2016, and end by Jan. 31, 2021.

**Read the RFP:**  
[is.gd/FCW\\_IARPA\\_qubit](http://is.gd/FCW_IARPA_qubit)

## Administration halfway to spectrum goal

In 2010, the White House released an ambitious plan to repurpose 500 MHz of federal and commercially licensed spectrum for use by providers offering high-speed mobile Internet access.

The administration is about halfway to meeting its goal, according to a blog post by Paige Atkins, associate administrator of the Office of Spectrum Management at the National Telecommunications and Information Administration. Over five years, NTIA — in partnership with the Federal Communications Commission — has freed up 245 MHz of spectrum for use in licensed and unlicensed mobile broadband.

More will come next year. A planned reverse auction of existing broadcast TV spectrum licenses could yield as much as 144 MHz, according to government estimates.

It's not clear how the government will reach the 500 MHz target, and Atkins noted that the process "only increases in difficulty."

She said regulators would continue to look to government and commercial users to "identify additional spectrum for potential repurposing, including through shared access, while ensuring federal agencies have access to spec-

trum needed to perform their critical missions."

— Adam Mazmanian

## Halvorsen touts 'secure enough' mobility

Defense Department CIO Terry Halvorsen said data has a shelf life, and it is impractical to secure everything.

Like food, data should come with an expiration date because after a couple months, it is generally less valuable and therefore less worth securing, he said.

"I think it's becoming a whole lot less about the devices and a whole lot more about...intelligently understanding the data," Halvorsen told attendees at a mobility conference hosted by AFCEA's D.C. chapter in July. "And I really do think you all can help us with that."

Halvorsen appealed to the data specialists in the audience to collaborate more closely with DOD, as he said industry did during World War II. "We've gotten away from some of those partnerships, and we definitely need that back today," he said.

The cyberthreats of today make that partnership all the more urgent, Halvorsen added, because cyberspace is both "the new warfare area" and "the new economic area."

— Sean Lyngaas



**Noblis Engineering**

@NoblisE3S

@WhiteHouse is talking to @ULdialogue about a potential #IoT certification. @FCWnow: <http://ow.ly/PvByF>

Reply Retweet Favorite

6:01 AM - 13 Jul 2015

## Join the conversation

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

Learn more at [Twitter.com/FCWnow](http://Twitter.com/FCWnow).



## State got high marks for managing records under Clinton

The State Department was rated as a low-risk agency in terms of records management during the time that Hillary Clinton was secretary, even though Clinton maintained a private email network for her official correspondence.

The disconnect might not be as strange as it sounds.

Since 2009, the National Archives and Records Administration has surveyed records officers across the government to get a sense of their management practices. NARA probes agency policies and training in the surveys but doesn’t ask for details about particular problems or specific employees. And when it comes

to practices among political appointees, career functionaries can be among the last to know.

“The way the world works is that

people at a much removed level from Ms. Clinton’s orbit are the ones who typically answer NARA surveys,” said Jason Baron, a lawyer at Drinker Biddle and formerly director of litigation at NARA.

Former State Department Records Officer Tasha Thian reported in 2009 that the department explained policy on how to manage email sent or received via non-federal accounts and that high-level executives and political appointees were routinely trained on how to manage their email. In 2010, Thian reported that the agency ensured that federal email records were “preserved in the appropriate agency recordkeeping system.”

Because of those self-assessments, the State Department earned the lowest possible risk score of 100 for 2012

and 2013. State scored 94 in 2009, when the average score was 76, then dipped to 87 in 2010 before climbing to 92 in 2011.

The 2013 self-assessment reported on the records officer’s plans for the end of Clinton’s tenure. If anyone at the records management level had learned that Clinton maintained her email on a personal server, that information was not included in reports to NARA.

The State Department did not comment on whether the records management officer was aware of Clinton’s email practices. At the time, there was no law or regulation preventing a State

Department official from using a personal system.

Paul Wester, chief records officer for the U.S. government at NARA, said the attention from the

media, congressional overseers and watchdog groups was generating activity related to records management.

“It’s giving records officers and senior agency officials the opportunity to have conversations with people they were never having conversations with regarding these issues,” Wester told FCW. “It’s putting stress on people to do better, which is a good thing, but they are stressed.”

Government agencies are facing a key deadline for a presidential directive to manage email in electronic form for the purposes of recordkeeping by the end of 2016. NARA has developed guidance designed to take some of the human activity out of recordkeeping. It also specifies requirements for certain high-level jobs and key functions.

— Adam Mazmanian

## Lawmakers propose taking clearance system from OPM

A pair of congressmen want to take stewardship of files on government and contractor employees with security clearances away from the Office of Personnel Management, in light of the hacks that resulted in the breach of data on more than 22 million people.

Reps. Ted Lieu (D-Calif.) and Steve Russell (R-Okla.) plan to introduce legislation to move the security clearance system out of OPM.

Lieu noted in a statement that the agency’s inspector general had identified vulnerabilities in the clearance system “year after year,” but they went unaddressed.

“In hindsight, it was a mistake to move the security clearance system to OPM in 2004,” Lieu said. “We need to correct that mistake.”

The bill had not yet been introduced as of press time, and details were not available. But according to Lieu, the basic plan was to give custody and control of the security clearance database to “another agency that has a better grasp of cyberthreats.”

Russell, meanwhile, complained about the money sunk into insecure IT systems in general.

“We have spent over a half a trillion dollars in information technology and are effectively throwing it all away when we do not protect our assets,” he said. “OPM has proven they are not up to the task of safeguarding our information, a responsibility that allows for no error.”

— Adam Mazmanian



Rep. Ted Lieu

The attention around Hillary Clinton’s email records is “putting stress on people to do better, which is a good thing, but they are stressed.”

— PAUL WESTER, NARA



## Finding security in the cloud

A few key considerations can make it easier to choose a cloud provider in a complex regulatory landscape

Despite all the traction cloud computing has gained in recent years, IDC is predicting even bigger things for the future. The federal government is projected to spend \$7.7 billion on private cloud solutions by 2017, a nearly \$6 billion increase from the projected \$1.7 billion spent in 2014.

As federal agencies show increasing interest in the cloud, IT executives must understand how to navigate compliance programs, particularly the Federal Risk and Authorization Management Program (FedRAMP) and particularly when it comes to managing security, costs and processes efficiently.

Furthermore, given the myriad regulations in place for securing data and personally identifiable information — including the Federal Information Processing Standards and directives from the National Institute of Standards and Technology — agencies must be aware of the regulations they are subject to, the protections that their cloud providers offer and the differences between what they do in their managed environment versus the customer environment.

It is also important to understand which aspects of an organization's cloud strategy require complying with those regulations and which do not. For example, the IRS' public-facing informational website does not require the same level of security as a portal that collects personally identifiable information. If the same levels of security are

unnecessarily applied to an agency's entire cloud model, it can result in increased costs and resource burdens.

CIOs, chief information security officers, chief technology officers, chief financial officers and other decision-makers navigating complex infrastructure-, software- and platform-as-a-service cloud offerings have much to consider when

**Agencies must be aware of the regulations they are subject to and the protections that their cloud providers offer.**

choosing a FedRAMP-compliant provider. Decision criteria must include optimizing the management of security and other costs while maximizing efficiency.

Another critical area for consideration is encryption, which is not currently mandated. Encryption is the key to any data protection program, but FedRAMP and NIST have not kept up with the bad guys and real-world threats in this regard. Old-school approaches to protecting data during all phases of its life cycle need rethinking.

With the latest advances in database and file server encryption, there is no reason for an agency not

to deploy encryption. It can even be put in place before moving to the cloud. If encryption were deployed correctly and pervasively, we would see fewer news reports of hacked companies, China grabbing agencies' personally identifiable information and Edward Snowden divulging state secrets.

Another important consideration is visibility into operations. IT leaders need insight into the entire data-hosting network system to ensure that compliance standards are met and that the provider is operating transparently. Areas outside the continental U.S. — including Hawaii — are risky places to base hosting services and cannot be considered for U.S. agency workloads.

Geolocation and geofencing ensure that operational changes do not move computing resources or associated data into a non-compliant environment at another data center, which could unknowingly be located in another city or even country.

A perfect storm of digital opportunities, online threats, demands for accelerated system deployments and IT's mandate to save money is creating a sense of urgency across the government. Selecting the right cloud provider is difficult enough; with the added challenge of navigating the compliance and regulation landscape, decision-makers must keep these tips in mind in order to keep their agencies operating in a secure, compliant, budget-conscious and efficient manner. ■





# NS2020 EIS: Another step forward for GSA

The agency's latest approach to telecom contracting builds on its past successes while embracing competition and innovation

Delivering flawless network services across very large enterprises is an enormous challenge. In the public sector, federal agencies expect their CIOs and telecommunications managers to meet demands unheard of just 10 years ago: deliver access anywhere, anytime and to any device securely. And they are expected to deliver those benefits while adopting and integrating the technologies needed to thrive in the 21st century, which include cloud services, cybersecurity, big-data analytics and the Internet of Things.

Federal CIOs and telecom managers, in their always-on quest to reduce complexity, are increasingly turning to companies that can deliver those services as an integrated solution.

The General Services Administration is bringing much-needed relief to federal CIOs and telecom managers by developing a set of contracts that simplifies complex purchases of network-related services, one that allows agencies to buy what they need at market-best prices while ensuring robust vendor competition and transparency. The strategy for this new set of contracts is known as Network Services 2020.

GSA's first contract for buying telecom, cloud, cybersecurity and other network-related services under NS2020 is Enterprise Infrastructure Solutions, which is the successor to the current Networx contracts. EIS represents insight and input from agency CIOs and reflects the evolution of modern

telecom technologies. It is a smart, strategic approach to technology purchasing that prioritizes simplicity, cost reduction, modernization and efficiency.

That is what GSA does best. It creates a flexible market purchasing environment for agencies that caters to their needs with the implicit acknowledgment that there is no one-size-fits-all solution to complex government technol-

EIS prioritizes  
simplicity, cost  
reduction,  
modernization and  
efficiency.

ogy requirements. GSA has created multiple-award schedules for buying common commercial items or services, governmentwide acquisition contracts for broad IT solutions and NS2020 contracts for telecom services.

In effect, GSA has created a menu of options that empowers agencies with multiple choices for how and from whom they buy technology. GSA's strategy fosters competition within the contracts and among the different types of contract vehicles. It is smart and forward thinking, and it ultimately keeps prices competitive for agency customers.

U.S. telecom companies have

invested approximately \$1.1 trillion in their networks since 1999, according to the Wall Street Journal. GSA's strategy allows agencies to directly benefit from that investment in innovation and infrastructure. Then there are the significant cost benefits agencies can achieve as a result of continued innovation and robust competition among providers. Mary Davie, assistant commissioner of GSA's Office of Integrated Technology Services, said the agency's network services programs — FTS 2001 and Networx — have saved agencies more than \$8.4 billion in the past 15 years.

Although GSA has been criticized for developing multiple contracting efforts, overlap is actually an integral part of its strategy. An agency can buy a turnkey solution using a single solutions-based contract, or it can use a set of contracts to buy and assemble components for an integrated solution. That approach creates a competitive marketplace within contracts and across multiple vehicles, giving agencies enormous flexibility and leverage.

As the latest purchasing advance from GSA, NS2020 EIS puts agencies first and will provide them with secure, resilient, cost-effective, innovative and excellent quality telecom solutions and services by taking advantage of industry investment and expertise.

Meeting the network services needs of federal agencies is not an easy job, but GSA is entering its fourth generation of doing it. ■



# U.S. must do more to protect privacy

The government's latest effort on surveillance reform is a good step, but now it's time to work on the rules for international information exchange

WikiLeaks' recent release of inter-country espionage records once again highlighted concerns about government surveillance practices and individual privacy. In the time since the original WikiLeaks and Edward Snowden scandals, many countries, media organizations and privacy advocates have cried out for changes to current practices.

And although the U.S. government recently took steps to change surveillance programs and shore up privacy protections, much work remains in reforming domestic laws and international treaties that govern information exchange among countries.

Congress passed the USA Freedom Act in June in the most recent federal action to change surveillance practices. Most notably, the law ended the bulk collection of data, one of the most contentious surveillance programs undertaken after the 2001 terrorist attacks. It also reforms some surveillance laws by creating added transparency and greater accountability for government.

The law is not without controversy, however. Fierce congressional debate was punctuated by a coalition of technology companies and government agencies advocating for its passage. Some privacy advocates strongly opposed the bill, and others offered only tepid support.

Despite those recent efforts, one of the highest-profile cases related to surveillance practices remains unresolved. The "Microsoft Ireland" case, initiated in 2013, asks a larger question: Can a U.S. law enforcement

agency compel a U.S. communications provider to turn over digital information that is stored in a location outside the U.S.? The USA Freedom Act does not directly address the issues raised by that case.

There are two things the U.S. can do to demonstrate its leadership on these issues and enable law enforcement to fulfill its mission while

If the U.S. fails to assert its international leadership role, national security and individual privacy could continue to suffer.

protecting individual privacy. On its own, each action is necessary but not sufficient.

• **First, Congress should pass the Law Enforcement Access to Data Stored Abroad Act.** The rules governing law enforcement's access to communications are almost 30 years old; they were passed long before the advent of email and cloud computing. The LEADS Act clarifies that U.S. warrants do not apply to email messages of non-U.S. citizens that are stored in other countries. The legislation is a bipartisan opportunity to improve international law enforcement practices while protecting the privacy of individuals.

To date, companion bills with co-sponsors from both parties have been introduced in the House and the Senate.

• **Second, the U.S. should lead the effort to reform mutual legal assistance treaties with other countries.** Reforming U.S. law isn't enough. The international processes need to change to support the reality of transnational threats. As a long-established process, MLATs govern how countries share information sought by law enforcement agencies.

To be sure, the processes are antiquated and slow, particularly given the pace at which electronic communication now operates. But there are long-standing cooperative relationships between countries that should be preserved. Instead of throwing out the MLAT process or circumventing it, new processes should be designed to update the existing rules.

Congress and the executive branch have a tall order in enacting those reforms. However, if the U.S. fails to assert its international leadership role, national security and individual privacy could continue to suffer. The game theory of international cooperation means that if we violate the rights of other countries by accessing the correspondence of their citizens, other countries may do the same to us.

Updating the rules will allow us to preserve our alliances with other countries, which will, in turn, benefit law enforcement and individual privacy. ■

# SQL Server<sup>™</sup> **LIVE!**

TRAINING FOR DBAs AND IT PROS

## ORLANDO

ROYAL PACIFIC RESORT AT  
UNIVERSAL ORLANDO

## NOV 16-20



**5**  
*Great  
Conferences*  
**1**  
*Great Price*

## Driving Data Forward

After 5 days of workshops, deep dives and breakout sessions, SQL Server Live! will leave you with the skills needed to Drive Data Forward.

With timely, relevant content, SQL Server Live! helps administrators, DBAs, and developers do more with their SQL Server investment. Sessions will cover performance tuning, security, reporting, data integration, adopting new techniques, improving old approaches, and modernizing the SQL Server infrastructure.

**REGISTER BY AUGUST  
12 AND SAVE \$500!**



Use promo code  
SQLAUG1

Scan the QR code  
to register or for  
more event details.



SQL Server **LIVE!**  
SQL SERVER FOR MODERN DEVELOPERS

Visual Studio **LIVE!**  
EXPERT SOLUTIONS FOR .NET DEVELOPERS

SharePoint **LIVE!**  
TRAINING FOR COLLABORATION

Modern Apps **LIVE!**  
MOBILE, CROSS-DEVICE & CLOUD DEVELOPMENT

**TECHMENTOR**  
IN-DEPTH TRAINING FOR IT PROS

SUPPORTED BY

Visual Studio

msdn  
magazine

Visual Studio  
MAGAZINE

PRODUCED BY

1105 MEDIA

**SQLLIVE360.COM**





# Buy **or**

**BY BRIAN ROBINSON**

If agencies had all the money and time they needed, most would probably still prefer to build their own IT applications and house them on hardware located on agency premises. But that option is no longer viable.

Now, IT departments are governed by an ever-present squeeze on budgets and resources and a brave new world of 24/7 expectations — from the public to provide information and services and from their own employees for the up-to-date tools they need to do their jobs.

The appeal of building solutions in-house will likely never go away. The bespoke approach, after all, comes with the ability to exercise greater control over development and quality,

integrate new technology more tightly with existing applications, better track documentation for ongoing support and react more quickly to requirement changes.

Some agency IT leaders have even pushed back against a headlong rush to the new. Last year, Terry Halvorsen, who was the Navy Department's CIO at the time, cautioned that new is not always the answer.

"In today's world, where technology changes in the blink of an eye and the race to be faster, more capable, bigger, etc., moves at lightning speed, we sometimes forget to ask ourselves that very simple question," he wrote in a blog post. "As prudent stewards of [Navy] resources, we have to decide



## It's a timeless question — and the answer might not be as clear-cut as agencies think

when it makes sense to invest in new technology” and when to stay with something that is still reliable and fully supports the Navy’s mission.

Nevertheless, new — even if that means embracing a modified version of old — is the goal for most agencies. The question then becomes whether to buy or find a way to efficiently and cost-effectively build.

### From custom to COTS

Commercial off-the-shelf software has long been the answer for many government needs. For example, agencies have used Microsoft’s suite of word-processing, spreadsheet,

collaboration and email applications for years. However, the more complex the requirements that COTS software is expected to meet, the more that software must be customized. At some point, customization becomes so extensive and costly that it makes more sense for agencies to build the software themselves.

The Defense Information Systems Agency reached that point a few years ago when officials reviewed COTS applications and concluded that the available options were not appropriate, were too expensive or would have to be changed too much to meet the agency’s workflow requirements.

On the occasions when DISA officials turned to outside



**Platform reuse “not only reduces IT costs and complexity, it also reduces the burden on GSA’s end users by reducing the number of disparate applications and tools they need to learn and access.”**

— BOX’S SONNY HASHMI, FORMER GSA CIO

developers for help, they were told the applications could not be built at all.

So they decided to develop their own software, aimed initially at internal needs for human resources, security training and personnel management activities. The resulting Web-based application now comprises some 110 modules and is available to government and nongovernment entities as the Open Source Corporate Management Information System.

The open-source community’s credo of reusing software modules is becoming a standard way for agencies to spread the cost of software development among many users and thereby benefit from some of the volume-based advantages of COTS. The Department of Health and Human Services, for example, has made reuse part of its enterprise architecture principles, one of which states that HHS “evaluates investments against business requirements and service needs, with a philosophy of first reuse, then buy, then build.”

More recently, the General Services Administration latched onto reuse as a major driver for its IT projects. In 2014, then-CIO Sonny Hashmi made “platform reuse first” one of the nine key principles that would guide the agency’s IT modernization. In doing so, he essentially melded open-source with cloud-first policies.

Capitalizing on GSA’s existing investment in common application and infrastructure platforms “not only reduces IT costs and complexity, it also reduces the burden on GSA’s end users by reducing the number of disparate applications and tools they need to learn and access,” Hashmi said at the time.

He added that he hoped the approach would eventually lead GSA to build custom solutions for no more than 20 percent of projects.

### **Cloud can cut down on the one-offs**

Deciding whether to borrow, buy or build requires a clear-eyed assessment of an agency’s particular needs and a broad understanding of what existing solutions can and cannot do,

said Dave Zvenyach, director of acquisition and management at GSA’s 18F.

“In practice, much — if not most — of the things we need in government are very similar to needs experienced outside of government,” Zvenyach said. “In those cases, we borrow or buy. But where the government’s needs differ, we’ll look to borrow or build.”

Over time, he added, the hope is that the number of situations in which open-source solutions are borrowed will outnumber the situations in which they must be built.

However, some agencies will continue to need custom applications. For instance, the classified networks of intelligence agencies and some parts of the Defense Department cannot securely be connected to the Internet, which means that DOD and the intelligence community have missed out on some of the advantages of cloud services. That could be changing, though.

“The intelligence community has started to look at how to solve that problem by having public cloud providers come in and build a public cloud in a government facility,” said Stan Tyliczszak, staff vice president for technology integration and chief engineer at General Dynamics IT. “That gives them all the advantages of public cloud technology and the expertise associated with that, while still operating in a constrained environment where the physical and virtual access to resources is restricted for anyone who is not in the community.”

Last year, the CIA took the leap into the cloud after striking a \$600 million deal with Amazon Web Services in 2013 to develop a private cloud for the 17 agencies that make up the intelligence community. Now users at those agencies can get a variety of computing and analytical services on demand from the CIA and the National Security Agency.

The deal was the result of a longtime effort by the CIA to boost the performance of its data centers and provide its analysts with better tools. It gives the agency “the flexibility to optimize resources across different workloads at different





Ready For The Next  
Big Thing For Government

**SAMSUNG**  
BUSINESS™



In today's global economy, technology offers the potential for unparalleled innovation. To realize that potential, you need a partner with the knowledge, innovation and capabilities to empower and strengthen your government agency in a timely manner.

As a trusted provider of secure technology solutions to the U.S. government, Samsung Business™ has put its spirit of innovation and collaboration into delivering products that will help your agency stay ahead of the curve while lowering costs, increasing efficiency and maintaining security.

## Nobody Can Predict The Future, But We Can Help You Be Prepared to Navigate It

Unforeseen conditions and rapid changes are inevitable in the technology arena. We can help you adjust quickly to – and successfully route – such changes through our business-class products that seamlessly integrate with your agency's infrastructure, keep your data safe with comprehensive solutions and provide employees with beneficial features they truly enjoy using.

# Mobile Products

Communicate and collaborate with colleagues more easily and securely than ever with our selection of innovative mobile products and defense-grade Samsung KNOX™ mobile security platform.

## Samsung Galaxy S6 and Samsung Galaxy S6 edge

Get our best display, fastest mobile processor and powerful productivity features wrapped in a sleek metal and glass design you and your employees will want to use.



## Samsung Galaxy Note 4 and Samsung Galaxy Note Edge

Work more efficiently from a mobile device and accurately take notes on-screen just about anywhere with the big, bold and brilliant Samsung Galaxy Note 4 and Samsung Galaxy Note Edge.



## Samsung Gear S

See who is calling without reaching for your phone. Reply to emails while you're at a trade show. Send texts right from your wrist. Keep in touch without keeping your phone on you every moment with Samsung's first network-connected\* wearable.

\*3G coverage not available everywhere and requires a qualifying wireless plan. Consult your carrier for details.



## Samsung Galaxy S5 Active (AT&T Only) and Samsung Galaxy S5

The stunning, powerful, water-resistant\*\* Samsung Galaxy S5 delivers a brilliant display, fast camera and integrated S Health™ technology to enhance every day. The Samsung Galaxy S5 Active is IP67- and MIL-STD-810G-certified for salt, dust, water and thermal shock-resistance, engineered for use in the field.

\*\*Device has been tested and received an IP (Ingress Protection) rating of IP67, which means that it is protected against dust intrusion and capable of withstanding water immersion between 15cm and 1 meter for 30 minutes.



## Samsung KNOX

Defense-grade Samsung KNOX security is a highly resilient mobile platform that brings unprecedented device security to government and enterprises. KNOX allows individuals to combine a single device for work and personal use without compromising security. It also provides greater protection for your sensitive data and cooperation with your IT department's policy requirements by easily integrating with your agency's existing security solution.



## Common Criteria and FIPS-Certified Devices

Along with Samsung KNOX security, numerous Samsung mobile devices have Common Criteria certification – which evaluates a mobile device to see that it provides adequate security for its intended purpose. These devices are also FIPS 140-certified, which validates that a mobile device uses and implements encryption algorithms correctly.



# Tablets, Laptops and Zero Client Displays

Put the power of Samsung's mobile computing products to work for you and keep your agency at the cutting edge of innovation while also keeping secure communication a priority.

## Samsung Galaxy Tab A

The Samsung Galaxy Tab A improves productivity and transforms workflow efficiencies with powerful multitasking features, Microsoft® Office for Android™ apps preloaded\* and defense-grade Samsung KNOX™ security, so your team can work from virtually anywhere.

*\*A single Microsoft app is preloaded on the tablet; when the device is connected to the internet and when the app is pressed, the suite of Microsoft Office for Android apps is downloaded.*

**8" Wi-Fi®** | Smokey Titanium: SM-T350NZAAXAR | White: SM-T350NZWAXAR  
**9.7" Wi-Fi** | Smokey Titanium: SM-T550NZAAXAR | White: SM-T550NZWAXAR  
**9.7" Wi-Fi with S Pen** | Smokey Titanium: SM-T350NZAAXAR



## Samsung Galaxy Tab Active (Wi-Fi Only)

Ruggedized, enterprise-ready and solutions-ready, the Samsung Galaxy Tab Active is IP67-certified for water and dust resistance and is field-/outdoor-ready thanks to its bundled protective case and 8" daylight-readable display. Don't worry about drops or impacts in active business environments. With its included cover, the Galaxy Tab Active is designed to handle drops of up to 1.2 meters (3.9 feet)\*\*\* In addition, it also incorporates NFC, a user-replaceable battery and a 3-year warranty. Finally, defense-grade Samsung KNOX security allows your team to work from virtually anywhere.

*\*\*\*Drop test results meet MIL STD 810G standard.*

SM-T360NNGAXAR



## Samsung ATIV Book 9 and Samsung ATIV Book 9 Plus

Bring clarity to your work on the impressively thin, lightweight ATIV Book 9. SideSync™ capability lets you automatically sync files with select Samsung smartphones, or use the device as a second display. A long-lasting 10-hour battery ensures all-day productivity. Step up to the ATIV Book 9 Plus for full-touch screen capability.

**ATIV BOOK 9** | NP900X3K-S01US | NP900X3K-S02US  
**ATIV BOOK 9 PLUS** | NP940X3K-S01US | NP940X3K-S02US | NP940X3K-K02US



## Zero Client Desktops and Displays

The NX-N2-T Zero Client Desktop features built-in PCoIP® technology, which connects users to the corporate cloud while simplifying and securing the endpoint device. NC Series Zero Client Cloud Displays integrate business-class monitor designs with the latest in VDI zero client technology in an elegant all-in-one package. Samsung zero clients are purpose-built for VDI access, making them the ideal products for a truly centralized IT infrastructure.

**21.5-INCH:** NC221-S | **24-INCH:** NC241-TS | **Stand-Alone:** NX-N2-T



## Solid State Drives

Handle workloads from high-end computing on client PCs to heavy data center use with our new generation of solid state drives. From our portable T1 SSDs to our 850 EVO and 850 PRO series SSDs, you'll have speed optimized for business use, AES 256-bit encryption to protect sensitive data and high endurance for long-lasting performance.



**850 EVO SSD** | 1.0TB: MZ-75E1T0B/AM | 500GB: MZ-75E500B/AM | 250GB: MZ-75E250B/AM | 120GB: MZ-75E120B/AM  
**850 PRO SSD** | 1.0TB: MZ-7KE1T0 | 512GB: MZ-7KE512 | 256GB: MZ-7KE256 | 128GB: MZ-7KE128

## Digital Displays

From conference rooms to lobby signage to fully customized video walls, Samsung SMART Signage Displays allow you to deliver dynamic content and messaging while creating new communication opportunities and experiences at your agency.

### ED-D Series LED Display (32"-75")

Get excellent Full HD quality at a smart price with these energy-efficient LED displays that are perfect for boardrooms, conference rooms and general signage in and around your agency.

32 INCH: ED32D | 40 INCH: ED40D | 46 INCH: ED46D  
 55 INCH: ED55D | 65 INCH: ED65D | 75 INCH: ED75D

Metro Airport Arrivals						
Airline	Arrivals	Time	Flight	Gate	Status	
American	Burbank	11:22a	976	C7	on time	
Delta	Long Beach	7:35p	789	B5	on time	
Southwest	Oakland	11:05	4233	D7	delayed	
United	Seattle	5:15	154	P9	on time	
Continental	San Francisco	4:18	818	H5	on time	
American	San Francisco	3:04	820	E6	on time	
Delta	Burbank	1:32	2233	R8	on time	
United	Boston	8:03p	1732	E1	on time	
American	Charlotte	8:55a	1549	F22	delayed	

### DM-D Series LED Display (32"-82")

Built for reliable, continuous 24/7 operation, these stunning Full HD displays feature an upgraded Samsung SMART Signage Platform and full range of connectivity options like embedded Wi-Fi® so you can customize your content.

32 INCH: DM32D | 40 INCH: DM40D | 48 INCH: DM48D | 55 INCH: DM55D  
 65 INCH: DM65D | 75 INCH: DM75D | 82 INCH: DM82D

Metro Airport Arrivals						
Airline	Arrivals	Time	Flight	Gate	Status	
American	Burbank	11:22a	976	C7	on time	
Delta	Long Beach	7:35p	789	B5	on time	
Southwest	Oakland	11:05	4233	D7	delayed	
United	Seattle	5:15	154	P9	on time	
Continental	San Francisco	4:18	818	H5	on time	
American	San Francisco	3:04	820	E6	on time	
Delta	Burbank	1:32	2233	R8	on time	
United	Boston	8:03p	1732	E1	on time	
American	Charlotte	8:55a	1549	F22	delayed	

### UD-D Series LED Display (46" and 55")

Create a seamless, premium video wall solution with Full HD displays that have near-seamless 3.5mm bezel-to-bezel specs, ColorExpert Calibration to ensure vibrant, accurate, consistent colors and an embedded SMART Signage Platform.

46 INCH: UD46C | 55 INCH: UD55D

Metro Airport Arrivals						
Airline	Arrivals	Time	Flight	Gate	Status	
American	Burbank	11:22a	976	C7	on time	
Delta	Long Beach	7:35p	789	B5	on time	
Southwest	Oakland	11:05	4233	D7	delayed	
United	Seattle	5:15	154	P9	on time	
Continental	San Francisco	4:18	818	H5	on time	
American	San Francisco	3:04	820	E6	on time	
Delta	Burbank	1:32	2233	R8	on time	
United	Boston	8:03p	1732	E1	on time	
American	Charlotte	8:55a	1549	F22	delayed	



## Desktop Displays

Improve efficiency and productivity with a broad lineup of reliable, cutting-edge Samsung Business™ desktop displays. These commercial-grade monitors have all the power, performance and versatility to handle your agency's needs.

### 450 Series Monitors

These reliable, cost-effective monitors are perfect for everyday agency use. Energy-efficient improved ergonomics with adjustable stand, a narrow-bezel design and wider connectivity options make the 450 Series versatile enough to meet your agency's needs.

19 INCH: S19E450BR | 21.5 INCH: S22E450B | 21.5 INCH: S22E450D  
23.6 INCH: S24E450DL | 23.6 INCH: S24E450D | 27 INCH: S27E450D



### UHD 850 and 970 Series Monitors

Make your users more productive with higher-resolution monitors. Our QHD and UHD monitors offer higher resolution than standard 1080p monitors so users can see more details on the screen. Perfect for engineers, programmers, designers, command and control, and anyone wanting more accurate and detailed images that are critical to performing their tasks efficiently and accurately.

23.5 INCH: U24E850R | 28 INCH: U28E850R | 31.5 INCH: U32E850R



### Curved Monitors

Enjoy truly immersive viewing experience that lets you enjoy big, bold and stunning panoramic views while you work. With a design inspired by the curve of the human eye and flicker-free technology, Samsung's energy-efficient, eco-friendly curved monitors deliver a more comfortable, more enjoyable viewing experience.

23.5 INCH: S24E650C | 27 INCH: S27E650C





# Printers

Samsung's high-performance and resource-efficient printers offer reliable, cost-competitive document-handling solutions while keeping security at top of mind. All printers listed are TAA-compliant for United States government use.

## ProXpress M4530ND/TAA

Take business performance to a new level with this monochrome single-function printer. Work fast with a 47 ppm engine and intuitive, easy to use controls. Extra-high-yield toner and drum life lower total cost of ownership and save space in the stockroom.



---

## ProXpress M4020ND/TAA

Enjoy fast 42ppm performance, professional quality and lower operating costs from this monochrome laser printer. ReCP (Rendering Engine for Clean Page) technology delivers solid printouts with sharp, clear text, while the compact footprint allows this printer to fit in even the most cramped work spaces.



---

## CLP-680ND/TAA

Fast and flexible with true color, this 25 ppm color laser printer for small work groups produces vibrant, high-quality printouts. A simple operating panel, compact design and high-yield toner make it the perfect color printer for any environment.



---

## CLP-775ND/TAA

Optimize the quality of your printouts and reduce operational costs with this 35 ppm color laser printer. It has the speed and easy connectivity to meet your agency's workflow demands, the power to handle print jobs of all sizes and vibrant color to produce brilliant printouts on every page. High-yield toner and up to 3 optional paper trays allow users to print massive reports with minimal intervention.



Samsung Business's extensive portfolio of government contracts includes governmentwide acquisition contracts (GWAC), multiple award schedules (MAS), multiagency contracts (MAC) and blanket purchase agreements (BPA). Below are a sample of some of the contract options available for Samsung products. Products displayed in this catalog are not necessarily available through all of the referenced contracting options.



1200 New Hampshire Avenue NW, 6th Floor, Washington, D.C. 20036  
Product Support: 1-800-SAMSUNG 1-866-SAM4BIZ

For complete product information and accessories, visit [samsung.com/b2bprinters](http://samsung.com/b2bprinters) or [samsung.com/business](http://samsung.com/business)  
Follow us: [youtube.com/samsungbizusa](https://www.youtube.com/samsungbizusa) [@SamsungBizUSA](https://twitter.com/SamsungBizUSA)

**SAMSUNG**  
BUSINESS™

times,” agency CIO Doug Wolfe said in an interview last year with FCW’s sister publication GCN.

That should significantly improve the “time to mission,” he added, because it now takes just days to set up new data center environments and new analytics, rather than the months or years it took before.

NSA and DOD agencies with similar connectivity concerns are considering the same approach, Tylliszczak said.

### Data vs. applications

Other agencies are discovering that they can get the advantages of the cloud while also having applications and services targeted to their specific needs, Tylliszczak said. For instance, they benefit from the economies of scale and operational efficiency that come with developing in the cloud rather than building an application themselves in a small-scale computing environment, and they shift the cost model from one that largely relies on upfront capital expenditures to one that has lower recurring costs.

“These days, you really should be able to put most of what an agency does into a cloud,” Tylliszczak said. “There will always be some legacy application that performs some unique function with unique interfaces that can’t be updated that way, but the reality is that much of the workload that agencies have today can be moved into some kind of cloud-based environment.”

There are other ways to look at the issues. Officials at Hitachi Data Systems Federal, for example, say the focus should be on the data that applications produce and where it needs to go rather than on the applications themselves.

“In the past, agencies would buy a solution and then customize that to get the functionality they needed,” said Brian Houston, the company’s vice president of engineering. “What you would then find is multiple silos of infrastructure for the mainframe, for a [Network File System] type of environment, another for databases and so on.”

Instead, he said that if agencies have an infrastructure that allows them to move data to the appropriate performance tier, it typically doesn’t matter whether the application is built, bought or customized.

“If you build the infrastructure so that it is scalable and flexible enough, so that data can go wherever it’s needed no matter the protocol involved, you really take the risk out of the whole build/buy question,” Houston said. “The real issue is

**“In practice, much — if not most — of the things we need in government are very similar to needs experienced outside of government. In those cases, we borrow or buy. But where the government’s needs differ, we’ll look to borrow or build.”**

— DAVE ZVENYACH, 18F

not about the application but what type of data needs to reside in the cloud, say, versus what needs to reside in an on-premises type of environment.”

He admitted that it isn’t always easy to convince agencies to follow that approach. But once they see the capabilities, it starts to make sense as far as budget and cost justifications are concerned. And it fulfills the mandate that agencies move to the cloud while allowing them to retain control over applications and data, which is still a fundamental concern.

### Rephrasing the question

Officials are also rethinking how the often-turgid government procurement process could be revamped to meet the growing demand for new and better application functionality and the increasing speed at which applications and services must be produced.

That’s why GSA has been developing special procurement processes for its upcoming blanket purchase agreement for agile services, which will enable the 18F program to get vendor help with user-centric design, agile software development and DevOps.

“Ultimately, we want access to the broadest pool of vendors possible in order to establish a marketplace,” Zvenyach said. “In this ‘alpha’ phase of the agile delivery BPA, we are using IT Schedule 70, which has thousands of vendors” and makes it relatively easy for other companies to qualify for an IT Schedule 70 award.

In the end, government technology development might no longer be a choice between buy or build.

“There are some things we’ll build, some we’ll buy, some we’ll commission to get certain parts,” said Aaron Snow, acting executive director of 18F. “Our mission is to help our agencies buy and build great digital experiences, however that may work out.”

Whether you use COTS, build custom solutions or do something in between is not really the question anymore, Tylliszczak said.

“It’s more a matter of how well the products you are buying off the shelf fit the agency’s need and how much customization is needed for that,” he said. “So it’s a hybrid of COTS, some customization and maybe some build, and the real challenge is in identifying how much of each is required.” ■

# How one company is embracing agile

CivicActions offers an inside look at how it is using agile development to respond to 18F's RFQ

BY ZACH NOBLE

**T**he scrum meeting starts, and some dozen members of a team spread across the country fire off status updates, questions and a “balance score.”

It's scheduled to take 15 minutes yet runs closer to 25, but the crew doesn't waste a moment and dives right into a second call, a retrospective look at the project that has dominated everyone's schedule at CivicActions for the past few weeks: the General Services Administration's blanket purchase agreement for agile services.

The team members at CivicActions are confident that they're doing agile right as organizations from GSA's 18F to the old guard of contracting struggle to embrace the technique.

## A way of life, not a buzzword

“Agile software development is transformative,” said Aaron Pava, the company's co-founder and chief experience officer (recruiter, salesman and pep squad all in one).

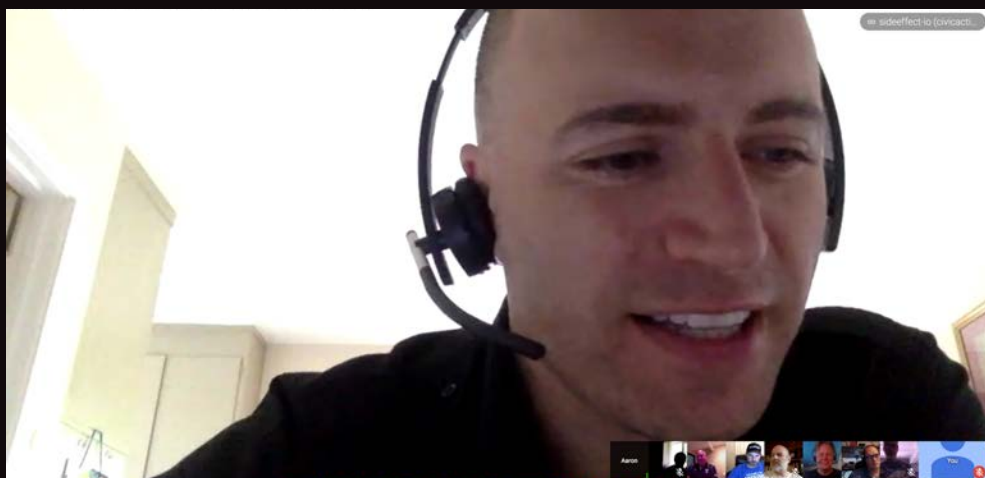
The General Services Administration's 18F released a much-anticipated request for quotations last month seeking to build an easily accessed pool of agile GSA Schedule 70 vendors through a novel process, and in response CivicActions embarked on a 10-day dash to get it done.

Instead of just a quote, 18F asked vendors to produce a working product using Food and Drug Administration data.

CivicActions got in touch with real users of FDA data on the first day — user-centered design in practice — and banged out <https://sideeffect.io> in little more than a week. The app compares the number of reported side effects for a list of drugs.

An agile mentality permeates everything CivicActions does, Pava said, even following the team home in a way. The “balance score” is a self-reported measure of how people are feeling on personal, professional and spiritual levels. The

The CivicActions team, which often meets via a Google Hangout, is built around the agile methodologies that 18F is trying to encourage in federal IT acquisition.





most commonly reported score on the July 2 call was a 9/10, indicating that the team was very happy and/or that a public self-reported scoring system promotes some degree of grade inflation.

The team used “a lot of the tools any startup would use,” said co-founder and CEO Henry Poole, though email factored into the equation “only a little bit.” Instead, the team’s tools of the trade revolved around communication and collaboration: Slack, Trello and the 18F-mandated GitHub, in addition to Jenkins for continuous monitoring and the Ubuntu open-source operating system on an Amazon Web Services stack.

### ‘Fiercely open’

The agile tenets of iterative design, failing fast and trying again, and constant communication among team members underpin their work, but they are particularly proud of their “fiercely open” attitude.

“If some other vendor started using our work, that would be a success for us,” quipped Poole, adding that CivicActions had fully embraced the call for open development long before 18F’s agile services BPA.

The guts of the project CivicActions developed for the RFQ are viewable in an open GitHub repository, per 18F’s instructions, but the company has gone a step beyond calling for teamwork among contractors and has been offering advice to competitors on its blog.

Part of that attitude is predicated on the notion that any particular tool or line of code is far less important than the people who make an operation tick. Competitors are free to technically mimic CivicActions, but the company’s selling point is its “humanware,” not its software, Poole said.

Pava said older, established federal contractors talk the agile talk, but they often stumble trying to walk the walk, which makes 18F’s BPA a great filter for future work.

“Dinosaurs just can’t fake [a functional, open, agile process] and deliver in 10 days,” Pava said. “That’s why this [BPA] is so awesome.”

### Dealing with delays

18F’s BPA opened June 17 and was slated to close June 26, but that deadline was pushed back twice because of a torrent of vendor questions about the novel approach. Solicitations finally closed July 7.

“Right as we’re closing up, they extend that deadline,” Pava lamented. “It feels like you’re running a race, you’re winning the race, and then the race gets extended.”

The delays gave laggards a chance to catch up, he added, and partially defeated the RFQ’s purpose of giving vendors an opportunity to show that they could turn out a working product in a short amount of time.

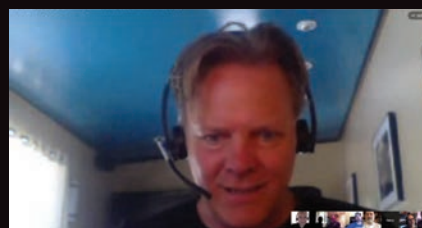
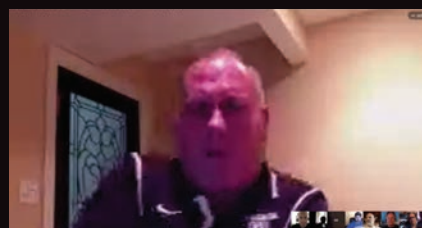
Despite the delays, CivicActions’ leaders say 18F’s BPA process will be a force for good in the government.

Plenty of big contractors are angling to be among the 20 firms chosen for the BPA, “but I think it’s scary for them,” Poole said.

“Win or lose, it’s not really the point,” Pava added. “This is the first step in what’s probably going to be a long game.”

That game involves convincing feds to truly accept agile, and although it won’t be easy — 18F hasn’t been welcomed by the whole of government — the BPA is a valuable step, Pava said.

“If we’re truly going to transform government, it has to be collaborative, it has to be open,” he said. ■



Peeks at new tech convince the Pentagon's CIO  
to ask for things once thought impossible

## Halvorsen's Silicon Valley trip

# shakes up JRSS

BY SEAN LYNGAAS

A visit by the Defense Department's top IT official to Silicon Valley has altered the software makeup of a key departmentwide IT security project. The forthcoming request for proposals for Joint Regional Security Stacks software will ask vendors to incorporate big-data analytics capabilities that DOD CIO Terry Halvorsen observed firsthand in Northern California in April.

Specifically, the next iteration of the software known as the Joint Management System (JMS) should be able to harvest security insights from data that is not intuitively security-related, Halvorsen told FCW in an exclusive interview.

"We'll be able to ask industry to do... certain things that I think we would not have been able to ask them before the trip because we now see that it's capable," he said.

JRSS is a collection of servers, switches and software tools meant to give DOD network operators a clearer view of traffic. By sending that traffic to the cloud for analysis, the stacks can help operators quickly respond to network threats by, for example, open-

ing certain ports or blocking a given IP address.

In a recent speech in Baltimore, Halvorsen said that although he was satisfied with the hardware and command and control of JRSS, he was concerned about the software component, and he hinted that his trip to Silicon Valley might have offered a remedy. Big data is apparently the remedy he had in mind.

The Defense Information Systems Agency expects to issue a request for quotations, a precursor to an RFP, for the next version of the JMS software in late July or early August, DISA spokeswoman Alana Casanova said.

Statistical modeling is another IT capability Halvorsen took note of while in Silicon Valley. The technology is evolving so that an increasing amount of data can be used to perform simulations with increasing fidelity, he said.

"If that type of combination of compute and intelligent tool analysis really does produce, it's game-changing in more ways than I can describe," he added.

One potential DOD application for

that sort of modeling is wargaming, where one could consider "political [and] policy factors at a much higher level because you would be using all of the available data that's out there," Halvorsen said.

He met with a bevy of firms during his trip to Silicon Valley, from household names such as Amazon, Microsoft, Oracle and Google to MarkLogic, a database builder whose website touts secure military messaging and field-based geospatial data capture.

Halvorsen emphasized repeatedly that a meeting with a given firm was not an endorsement but simply an exchange of ideas.

### Chief investment officer

Talk of a culture clash between how Silicon Valley and the Pentagon conduct business has been enshrined in Beltway lexicon for a reason: Startups balk at lengthy and often costly government procurement cycles and at the many compliance challenges that come with selling to the Pentagon. A cultural divide in investment and acquisition cycles was again on display during Halvorsen's trip out West.



**"If that type of combination of compute and intelligent tool analysis really does produce, it's game-changing in more ways than I can describe."**

"If you want to talk to the innovative companies and get them involved initially, and keep their interest, we have to start making investments really in a three- to six-month window. And the good news [is] they don't have to be big investments," he said, adding that investments of well under \$1 million could yield breakthrough research for DOD.

The learning flowed both ways on Halvorsen's trip. He said some in Silicon Valley were surprised to learn just how much the Pentagon spends annually on IT (\$35.9 billion in fiscal 2015, according to Halvorsen's office) and the ripple effect that such investments can have in the defense industry.

DOD's nascent outreach office in Silicon Valley — the Defense Innovation Unit Experimental (DIUX) — will be a focal point for how the department interacts with entrepreneurs. Officials have said the office will be staffed by both active-duty military and civilian personnel, though Halvorsen said it remains to be seen whether his office will have someone full-time at DIUX.

Noting that Silicon Valley is both a physical place and a metaphor, he said

he also plans to visit other tech hubs such as Boston and New York.

### **Managing DISA's workload**

Lt. Gen. Mark Bowman, the Joint Chiefs of Staff's director of command, control, communications and computers/cyber, said recently that he was concerned DISA might have too much on its plate right now given that it is handling mobile security for DOD and running the relatively new Joint Force Headquarters DOD Information Network (JFHQ DODIN), among other things.

When asked if he shared Bowman's concern, Halvorsen said, "I'm always concerned about the workload that I have going [on] at DISA," adding that he continually evaluates DISA's portfolio and the extent to which it should be involved in certain projects.

Data storage is one area in which DISA's role is shifting. Halvorsen said he wants private firms to be able to store DOD data of various security levels. Sharing that responsibility with the private sector would free up more resources for DISA to put toward running JFHQ DODIN, he added.

He is fond of comparing the Pentagon to an immense, federated corporation and invoked that analogy in describing how he will scrutinize DISA's portfolio. "This is not a onetime evaluation," he said. "Most businesses constantly look at where their market space is and what they should be doing."

It is a trade-off between "where do we put our internal assets and where do we leverage industry, and that's going to change, particularly in the IT/cyber business," he added.

Taking charge of JFHQ DODIN is not the only transition underway at DISA. Army Maj. Gen. Alan Lynn will replace Lt. Gen. Ronnie Hawkins as director of the agency this summer. As DISA's vice director, Lynn has worked closely with Halvorsen, who said Lynn shares his vision of constantly evaluating DISA's portfolio.

Halvorsen has told agency leaders that he wants to see a "completely commercial option" for the next version of DISA's unclassified enterprise email service. That approach would free up even more DISA resources as it grapples with its evolving role as the Pentagon's IT infrastructure agency. ■



# An explainer on containers

If containers continue to advance into federal enterprise IT, they could spell the end of monolithic legacy applications

**BY WILL KELLY**

Containers enable developers and systems administrators to build, distribute and run self-contained applications. Experts say their adoption could usher in the age of microservices, a software architecture approach in which agencies develop small, lightweight applications that operate in system-level isolation.

“I think containers are part of a general trend in the government toward more modern application development and architecture,” said Mark Ryland, chief solutions architect at Amazon Web Services’ Worldwide Public Sector.

David Messina, vice president of enterprise marketing at Docker, said the developer workflows that containers enable could become the foundation for a major application transformation — from giant monolithic applications to more distributed models.

## The fundamentals

“Given that it’s a developer-led movement, enabling your development team to use Docker in their developer pipeline has instant productivity benefits,” said Messina, whose company is a leading open-source container developer. “What Docker enables is the ability to make decisions at any point to migrate your applications from one infrastructure to the next,” which is especially useful as agencies move to the cloud.

“Your application can be developed within the four walls of your agency, and then you can have the flexibility of running your Dockerized applications in any cloud and also have a model where it’s hybrid across your own private cloud, in a public cloud or across public clouds,” he added. That portability brings freedom of choice for infrastructure and operations.

“At a certain level, you can think of containers as a way to package the applications and then to deploy them in a predictable and consistent and fast way,” said Kurt Milne,

vice president of product marketing at CliQr Technologies, an application-defined cloud management vendor. Containers eliminate “some of the dependencies [and] configuration issues that can often sideline or slow down a new project.”

## The hurdles

Jared Rosoff, senior director of product management and architecture at VMware, said that right now container companies offer “a code base that is very new and changing very rapidly. [The technology] doesn’t lend itself to an environment where you want to push some code and let it sit for a year. You [must] plan on upgrading the base in a container infrastructure pretty frequently until the technology is stabilized. That’s going to be a problem for everybody.”

He also cautioned that we are only at the beginning of the maturity curve for containers. An ecosystem of tools for managing fault diagnostics, configuration, performance and security does not yet exist for containers.

That means federal agencies might have to cobble together their own container management systems from various parts.

Christian Heiter, chief technology officer at Hitachi Data Systems Federal, stressed the key role an agency’s infrastructure will play. “There are a number of management tools because you will be launching all of these virtualized applications, [so] you need to have a good infrastructure... to be able to keep your costs under control,” he said. “Otherwise, you’re building tools, [but] you’re not really monitoring what’s going on in all these virtualized environments, and the costs can rise.”

There is also the struggle for control between developers and operations teams. “Because you are going to be using the base operating system for the application, you

have to make sure that base operating system is set up correctly for the application or range of applications so that they do not imperil any data or compromise any data or cause problems due to incompatibilities,” Heiter said.

Experts also raised concerns about who would maintain governance over containers. Rosoff summed it up this way: “I can’t just willy-nilly give complete control of that environment back to an application team unless I’m sure that I’ve got the right levels of controls and governance to ensure that same level of data protection, for example. I’m thinking about data protection, but you could pick almost anything.”

“There are multiple approaches to management and multiple approaches to security [and to] the implications of the launch of the containers themselves,” Heiter said.

Therefore, agencies should take a close look at their requirements and then find the best fit for current and future needs.

“A lot of applications have key dependencies that can’t be containerized,” Milne said. “Your containers have to coexist with your existing generation of servers and the reality of multiple OS versions.... These containers are going to end up in a mixed” environment.

In other words, “containers need to run on an OS,” he said. “Basically they’re sharing part of the kernel, so you can’t create a container in one operating system, then run it on another.”

He sees similarities to the early days of private clouds, with containers running on bare OS until agencies figure out how to integrate them into their existing processes.

Ryland had a slightly different take. “Moving toward a DevOps model itself [is] the bigger challenge — getting your head around how to meet compliance and other kinds of requirements in a world in which developers are constantly building and deploying new code on a daily basis,” he said.

“I think historically people have thought that that super agile model is somehow not compatible with the more controlled style of government application development and deployment,” Ryland added.

## The future of containers at federal agencies

Ryland said customers are already recognizing the benefits of containers. “Lately we’ve seen more cutting-edge kinds of customers who say, ‘Look, I can actually do better in meeting the government requirements because it’s completely automated. I’m removing all sorts of human decision-making from my application development-into-deployment process,’” he said.

And those customers have the metrics they need because they have conducted compliance and security tests

to ensure that the code they release meets their requirements, he added.

When asked for his predictions, Milne said, “Containers will be found in traditional agency production environments. It’s going to happen, or it’s happening.”

However, “those uses, those containers won’t be 100 percent containerized.” Instead, he foresees a mix of containers and non-containerized components or tiers, which means agencies will need management platforms

that can handle such mixed environments.

“I think as new applications come online, or as that development process starts, and as people begin to really internalize the DevOps model, and the [continuous integration/continuous delivery] model, then they’ll really look to containers as an important tool,” Ryland said.

Furthermore, containers give developers the ability to create applications wherever they are. “You can literally be writing a federal application on a plane, without Wi-Fi, because you’ve got all the pieces you need there, containerized on your laptop. Then as soon as you land, you can deploy [your application] into a cloud... because the container provides that compatibility layer... between local off-line development and the production environment.”

Heiter was equally enthusiastic about the future of containers for federal agencies. “This is exciting technology,” he said. “I love where the industry is going with this. I love where the open-source community is taking it. It will be highly beneficial to the federal sector moving forward, if not already.” ■

**“I think containers are part of a general trend in the government toward more modern application development and architecture.”**

MARK RYLAND, AMAZON WEB SERVICES

# Cracking the code on past performance

Two veterans of federal contracting help both sides understand this critical but convoluted aspect of acquisition

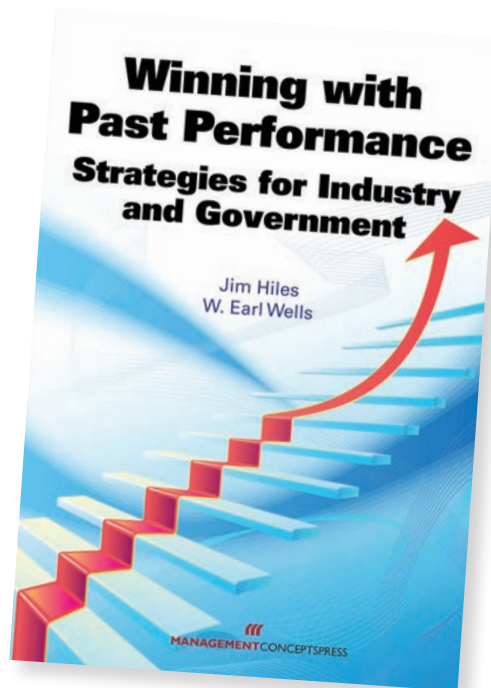
BY MARK ROCKWELL

Would you hire contractors to fix your house's sagging porch without first verifying not only that they could swing a hammer, but that they were competent carpenters whose work had stood the test of time?

Probably not — and neither should the government. Knowledge of a worker's — and a company's — past performance is the grease on the wheels of commerce in the federal acquisition process.

Over the years, the federal government has institutionalized past performance in its deliberations over contracts big and small — so much so that it has become a complicated, sometimes bewildering and utterly integral part of the acquisition environment.

By federal mandate, agencies must have an intricate understanding of a company before they sign a contract with it. It's a laudable goal, but it has also produced daunting electronic and paper trails that contractors must navigate.



## Past performance is defined by:

1. Observations of the historical fact of a company's work experience — the work it performed, when and where it did the work, for whom it did the work and the methods it used.
2. Qualitative judgments about the breadth, depth and relevance of that experience based on those observations.
3. Qualitative judgments about how well the company performed, also based on those observations.

Jim Hiles and W. Earl Wells' "Winning With Past Performance: Strategies for Industry and Government" is a guidebook that can help contractors and federal officials traverse those sometimes difficult paths.

The two authors know what they're talking about. Now retired from the Navy, Hiles led the rollout of SeaPort-e, the Navy's acquisition vehicle for support services in 22 areas, including engineering, financial and program management. Wells has been a proposal manager in the government services division at Electronic Data Systems (now part of Hewlett-Packard) and a proposal and operations manager at other technology companies.

The book delves into the details of how the federal contracting workforce tallies, measures and processes federal contractors' past performance. It gives companies insight into how to craft their answers for federal agencies and gives the federal acquisition workforce a better understanding of how contractors and the





13<sup>TH</sup> ANNUAL  
**ENTERPRISE  
ARCHITECTURE**  
EA TODAY: MAKING THE MISSION POSSIBLE

**FREE**  
for government  
personnel through  
August 25!

## EA TODAY: MAKING THE **MISSION POSSIBLE**



**How? Find Out at the Enterprise Architecture Conference!**

**WORKSHOPS: OCTOBER 5**  
**CONFERENCE: OCTOBER 6-7**  
**WASHINGTON, DC**

WALTER E. WASHINGTON CONVENTION CENTER

**THE 13TH ANNUAL ENTERPRISE  
ARCHITECTURE EVENT IS THE PREMIER**

educational forum for enterprise architects and project managers to convene and learn from expert practitioners in EA on the latest methods, frameworks and policies impacting the EA community.

**EDUCATION TRACKS INCLUDE:**

- Achieve Mission Outcomes
- Strengthen Enterprise Management

**SESSION TOPICS WILL INCLUDE:**

- Agile
  - Security and Privacy
  - Business Analytics
  - Big Data
  - Role of the Chief Data Officer
- ... just to name a few!

Attendees will receive an official certificate of attendance and CEUs for participating at this highly anticipated event.

**Reserve Your Seat Today —  
Register Before August 25  
for Best Savings!**

**GovEAconference.com**

USE PRIORITY CODE: EAE15

PRESENTING SPONSORS



EVENT SPONSORS



PARTNERING MEDIA



PRODUCED BY



commercial world perceive past performance.

Reaching a mutual understanding with regard to past-performance reviews is becoming even more valuable as the Office of Federal Procurement Policy and the General Services Administration seek to centralize all sorts of contracting data into one-stop expert hallways and managed categories for IT products and services.

Past performance is the foundation on which all federal contractors build their livelihoods. However, despite almost 20 years of the federal government using past performance to distinguish bidders, “both the collection and use of past-performance information remain disjointed, siloed and not well understood by either government or industry,” they wrote.

Alan Chvotkin, executive vice president and counsel at the Professional Services Council, notes in the book’s preface that the federal marketplace has seen “an almost continuous expansion of federal regulations, agency initiatives, and contracting officer trainings focused on measuring contractor performance, reporting on that performance in a consistent and timely manner, and evaluating those past-performance reports for future source selection decisions. Government contractors must pay close attention, or they face exclusion from future awards.”

The authors dive deep into Contractor Performance Assessment Reports, past-performance cycles, strategies for filling out past-performance evaluations, documentation and other paperwork.

There are also templates for reports that show strategies and techniques for sharing contractors’ “stories” with federal contracting staff in the most compelling and efficient way.

Details are important, and the authors stress that it’s not enough for a firm to say how many years of experience it has. Instead, companies must explain what kind of experience and the scenarios in which the work was performed.

As Chvotkin notes in the preface, the goal of the book is to show how the federal government uses information on past performance. Hiles and Wells help firms make the most of past-performance information for future opportunities, and they offer a valuable tutorial for agency officials who want to get up to speed on those intricate requirements. ■

---

## What the future holds

Jim Hiles and W. Earl Wells have identified several trends that will affect the measurement of past performance:

- **Increased standardization and digitization.** The 2013 rewrite of Federal Acquisition Regulation Part 42 continued the standardization of past-performance documentation. The melding of the Contractor Appraisal Support System, the Defense Department’s Architect-Engineer Contract Administration Support System, and the Federal Awardee Performance and Integrity Information System into Contractor Performance Assessment Reports is ample evidence of that trend.
- **Faster access to reviews.** Hiles

and Wells predict that information on contractor performance, along the lines of Yelp reviews, will be instantaneously available for federal buyers and suppliers as past-performance data becomes standardized and centralized in federal databases.

- **Increased analyzability of information.** There currently is not enough uniformity in past-performance data to effectively mine it, but standardization will increase capabilities for data mining and analysis.
- **More insight into reviewers’ identities.** The Angie’s List “reviews you can trust” are based on reviewers

who are not anonymous. Being able to understand and validate a federal reviewer’s identity has been missing from the government’s processes, say the authors, who predict that more transparency and access will allow reviewers’ identities to play a larger role in the process.

- **Increased reviewer accountability.** Knowing reviewers’ identities means they will be held more accountable for those reviews. Just as reviewers on Amazon and eBay can lose credibility if they give only positive or negative feedback, federal reviewers could find themselves viewed skeptically if they prove less than objective in their assessments.



Everywhere you want us to be.



Mobile



Tablet



Desktop



Print



# A better path to fair and reasonable pricing

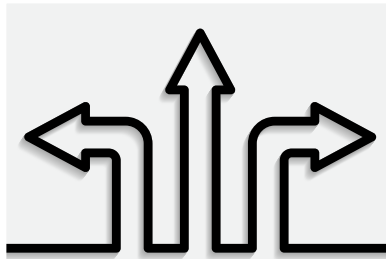
The Commercial Sales Practices approach sets a trap that can snare even diligent contractors. Government and industry both deserve a smarter solution.

BY MICHAEL GARLAND

The recent \$75.5 million Justice Department settlement with Carahsoft and VMware once again highlights for software companies the inherent danger of selling products to the government. Clearly, the Federal Acquisition Regulation and the various fraud statutes, such as the False Claims Act, should penalize cheating and fraudulent behavior by government contractors because protecting taxpayer money is a cause of the highest order. Unfortunately, sometimes the regulations are so complex and onerous that they can easily ensnare contractors who have no ill intent.

The media reports on the VMware settlement indicate that the company had misrepresented its Commercial Sales Practices, which were submitted via Carahsoft in order to create fair and reasonable pricing on Carahsoft's Schedule 70 contract with the General Services Administration. I have no special knowledge of VMware's behavior, but I am familiar enough with the CSP process to know that it is ripe for faulty information.

The point of the CSP submittal is to give a contracting officer enough historic pricing and discounting information to determine that the pricing proposed for the GSA Schedule is acceptable. This is often referred to



**In FASA's spirit of reducing the regulatory burden and inherent danger of contracting with the government, it would be helpful if the government requested important information in ways that gave commercial companies a better chance to accurately comply.**

as a "vertical" price analysis because it only looks at the actual sales of the products in question and does not compare the prices "horizontally" against similar competitive products.

Logically, that approach makes sense because for commercial products it is widely assumed that the price

buyers are willing to spend is the best market determinant for a fair price.

### **A mismatched approach**

To accomplish the pricing analysis task, GSA has created a form Schedule 70 aspirants must complete, through which they must disclose all their discounting practices to specified classes of customers in the preceding 12 months. And here is where things can quickly get off track. The form requires a software company to specifically list its discounting practices to the following classes of customers: Distributors, Dealers/Resellers, VAR/System Integrators, OEM, State and Local Government, Education/Non-Profits, and National and Corporate Accounts.

Although most of us intuitively know what those types of accounts might be, it is also a fact that few if any software companies classify their sales into those types of hard-and-fast categories — nor do they necessarily have any type of standardized discounting for each.

For many software accounting departments, an inquiry with a request for the "standard discount" to the VAR/System Integrator channel over the previous 12 months will be met with stony silence.

Invariably, financial people will do what they are trained to do — apply mathematics to the question and attempt to derive an answer. That answer will appear to be true to the best of everyone's knowledge. But it will be formulaic and not based on some definitive concrete truth. It will depend on which customers were fit into the vague definition of VAR/System Integrator.

It will also depend on the algorithm used to determine the discount number, which can vary greatly depending on whether an average or median is used and whether unique one-time transactions are excluded.

At the end of the day, numbers will be supplied for all the categories of customers, and their ultimate accuracy will be dependent on the interpretation of who fits which category and the calculations that were used to determine discounting at one moment in time.

### **An extreme penalty**

Unfortunately, now the trap has been set. The CSP submittals are the basis of representations that the government relies on to determine that pricing is appropriate. When, at a later date, it determines that there are flaws in the CSPs, it might use the False Claims Act to say the government relied on fraudulent information to make payments that it otherwise would not have made — that the pricing was “defective” because the government relied on false information.

The False Claims Act levels an extreme penalty — as much as \$11,000 for each transaction, regardless of the actual value of the transaction. A single transaction for \$100 incurs the same fine as a transaction for \$1 million. Damages also might be calculated and added to the fines. It adds up very quickly.

Once CSPs have been submitted, the software company is on the hook to

monitor its representations for changes and to inform the government immediately when an update is in order. Now Murphy's Law kicks in. Because the numbers were derived through a one-time-only process (because nobody else has ever asked for that data in that way before), the whole exercise can get lost in the day-to-day urgency of business.

Despite CSPs' importance, people move into new roles or forget how the numbers were achieved, business models change, and products come and go. Very quickly, it can reach the point where the original CSPs no longer make sense.

It's quite easy to imagine how a company could find itself uncertain of how the original numbers were derived. It isn't intentional fraudulent behavior. It's human behavior.

### **A possible solution**

In the wake of the iconic \$800 toilet seat and other procurement scandals, Congress passed the Federal Acquisition Streamlining Act in 1994. FASA's major feat was to define the notion of commercial products, state a preference for the procurement of those products and lessen the regulatory burden on their providers. In FASA's spirit of reducing the regulatory burden and inherent danger of contracting with the government, it would be helpful if the government requested important information in ways that gave commercial companies a better chance to accurately comply.

Because the CSP report is inherently an interpretive exercise, perhaps it could be abandoned for an alternative that achieves the government's goal of price analysis while aligning more closely with how companies keep their own records.

One suggestion would be to do away with the current CSP discount form and replace it with a simple mathe-

matical algorithm that could be easily reproduced in a standard report at any time. A simple request could involve asking a company to compile all the software sales it transacted under the GSA order ceiling of \$500,000 and compare that revenue number to what would have been received if all sales had been done at list price. The difference between the two is the effective average discount rate for all non-large sales.

If the government could look at that rate and ensure that its proposed discount was equal to or better than that, would that not meet the objective of fair and reasonable pricing? Furthermore, the software company and the government would have an effective and easy way to measure compliance at any time.

The current CSP system does not work well for anybody. The interpretive nature of the exercise means the government could routinely be getting data that is well intentioned but suspect. Furthermore, the fact that any CSP can form the foundation of a very expensive False Claims Act undermines the spirit of FASA, has the potential to chill commercial companies' willingness to contract with the government and could ensnare companies that are not willfully misrepresenting their pricing information.

It is time to move to a more simplified and fair way to measure pricing equity — one that serves the purpose of getting the government a fair price while not unfairly trapping an otherwise responsible contractor. ■

---

*Michael Garland is a former vice president at BearingPoint Technology Procurement Services and senior vice president at Siemens Enterprise Communication. He is currently under contract with the federal government supporting IT acquisition modernization.*



## THE CODE THAT NEVER SLEEPS

Visual Studio Live! is hitting the open road on the ultimate code trip to help you navigate the .NET Highway. The next stop? NYC, and we're geared up to be back in the big apple for the first time since 2012.

From September 28 - October 1, Visual Studio Live! is bringing its unique brand of practical, unbiased, Developer training to Brooklyn, offering four days of sessions, workshops and networking events - all designed to help you avoid road blocks and cruise through your projects with ease.

### FEATURED KEYNOTE SPEAKERS



Brian Harry,  
Corporate  
Vice President,  
Microsoft



Mary Jo Foley,  
Journalist and  
Author

*Register by August 5  
and Save \$300!*



Use promo code NYAUG1

Scan the QR code to register  
or for more event details.

VSLIVE.COM/NEWYORK



# FCW Index

## People

Anderson, Julie ..... 14	Hashmi, Sonny ..... 18	Russell, Steve ..... 11
Atkins, Paige ..... 10	Hawkins, Ronnie..... 23	Ryland, Mark..... 24-25
Baron, Jason..... 11	Heiter,	Scott, Tony ..... 4
Bitkower, David ..... 9	Christian..... 24-25	Snow, Aaron ..... 19
Bowman, Mark ..... 23	Hiles, Jim ..... 26, 28	Thian, Tasha ..... 11
Carter, Ashton..... 8	Houston, Brian..... 19	Tyliszczak,
Casanova, Alana..... 22	Kahn, Ralph ..... 4	Stan..... 18-19
Chvotkin, Alan ..... 28	Lieu, Ted ..... 11	Wells, Earl ..... 26, 28
Clinton, Hillary..... 11	Lowey, Nita ..... 9	Wester, Paul ..... 11
Collender, Stan ..... 9	Lynn, Alan ..... 23	Wilshusen,
Edwards, Chris ..... 4	Messina, David ..... 24	Gregory ..... 4
Garland,	Milne, Kurt ..... 24-25	Wolfe, Doug ..... 19
Michael..... 30-31	Nicoletti, Pete ..... 12	Woods, Bob ..... 13
Graham, Lindsey ..... 9	Pava, Aaron..... 20-21	Work, Robert..... 8
Halvorsen,	Poole, Henry ..... 21	Zvenych,
Terry .. 10, 16-17, 22-23	Rosoff, Jared..... 24-25	Dave ..... 18-19

## Agencies/Organizations

AG Strategy Group ..... 14	IARPA ..... 10
Air Force ..... 8	Intercede..... 4
Amazon Web Services ... 18, 24-25	Joint Chiefs of Staff..... 23
Carahsoft ..... 30	Justice ..... 9, 30
CIA ..... 18-19	Microsoft ..... 14
CivicActions ..... 20-21	MSPB ..... 8
CliQr..... 24	NARA ..... 11
Congress ..... 9, 11, 14, 31	Navy..... 16-17
DHS..... 4	NSA..... 18-19
DISA..... 17-18, 22-23	NTIA ..... 10
Docker..... 24	OPM ..... 11
DOD ..... 8, 10, 18, 22-23	Professional Services Council.. 28
Drinker Biddle..... 11	State..... 11
FCC..... 10	Tanium..... 4
FDA ..... 20	Topside Consulting ..... 13
GAO ..... 4	Virtustream ..... 12
General Dynamics..... 18-19	VMware ..... 8, 24, 30
GSA..... 13, 18-19, 20-21, 28, 30-31	White House ..... 4, 9, 10
HHS..... 18	WikiLeaks ..... 14
Hitachi Data Systems..... 19, 24	

## Advertisers

**Enterprise Architecture East**  
www.GovEAconference.com..... **27**

**Face-to-Face Event Series**  
www.FCW.com/events ..... **35**

**PCMG**  
www.pcmg.com..... **7**

**Samsung Electronics America**  
www.samsung.com/business..... **18a-18h**

**SQL Server Live 360**  
www.sqllive360.com ..... **15**

**The Boeing Company**  
www.boeing.com ..... **2-3**

**The Federal IT Acquisition Summit**  
http://fcw.com/fias..... **36**

**Visual Studios Live - New York**  
www.vslive.com/newyork..... **32**

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.

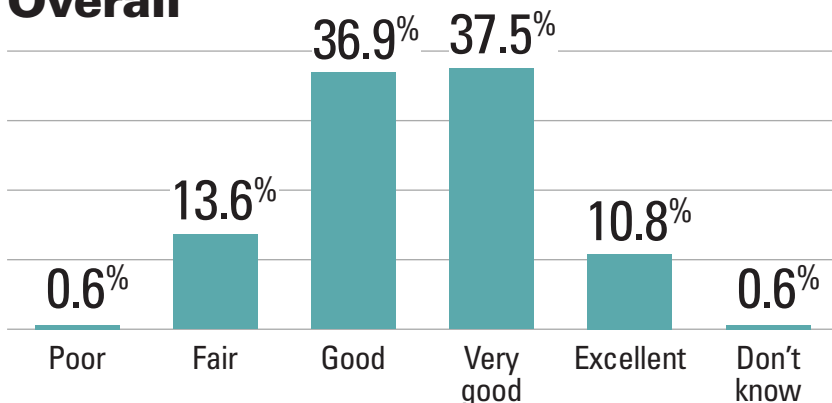
©Copyright 2015 by 1105 Media, Inc. All rights reserved. Printed in the U.S.A. Reproductions in whole or part prohibited except by written permission. Mail requests to "Permissions Editor," c/o FCW, 8609 Westwood Center Drive, Suite 500, Vienna, VA 22182-2215. The information in this magazine has not 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

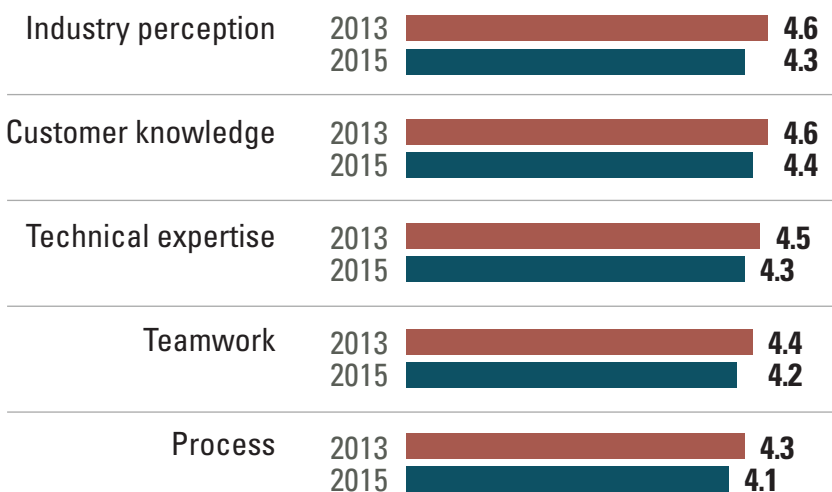
## What primes say about subs

Subcontractors are a critical part of federal acquisition, but their relationships with prime contractors are not always smooth. Here's how the primes grade their partners.

### Overall



**Scores have slipped, however, even for the “best subcontractors” when primes are asked to rate them on a scale of 1-5 for:**



*Ratings for all subs in 2015 averaged 0.5 to 0.9 points lower and showed similar declines from 2013.*

**There are plenty of partnerships to manage:**

**53.6%**

of primes work with five or more subs

**40.5%**

expect that number to grow in the next few years

**To improve the relationships, primes have plenty of advice, including:**

“Accept changes.”

“Be more courteous.”

“Participate in the proposal process.”

“Don’t oversell.”

“Understand completely that [you] are the subcontractor and not the prime.”



# FACE OF FACE

## Face-to-Face Event Series

Providing public sector IT decision makers with real-world strategies and tech tactics to support government, agency and corporate operations.

These events are **FREE** and located in the Washington, DC area.

**FCW.com/events**

### UPCOMING EVENTS

**Cybersecurity: CDM**  
AUGUST 19

**DOD: Joint  
Information  
Environment**  
SEPTEMBER 23

**Cybersecurity**  
OCTOBER 27

**Big Data**  
DECEMBER 2

For event sponsorship information, contact:  
**Alyce Morrison**  
Event Sponsorship Consultant  
703.645.7873  
amorrison@1105media.com



# The Federal IT Acquisition Summit

## Exploring Strategies, Options & Innovations

October 20, 2015

Washington Hilton, Washington, DC

**EDUCATION &  
TRAINING FOR  
KEY CONTRACT  
VEHICLES**

This second event in the Federal IT Acquisition Summit series provides government IT decision makers with contract-specific training opportunities as well as insights on key issues that are reshaping the federal acquisition environment. Featured vehicles include GSA Alliant (including an Alliant 2 update), NASA SEWP V, and NIH CIO-CS.

**Free for  
Government  
& Military  
Attendees**

### Supporting Agencies



### For Sponsorship Opportunities Contact

Alyce Morrison: [amorrison@1105media.com](mailto:amorrison@1105media.com) or Kharry Wolinsky: [kwolinsky@1105media.com](mailto:kwolinsky@1105media.com)

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