FCW
THE BUSINESS OF FEDERAL TECHNOLOGY

The 2015 Federal List

Top contractors, stumbling blocks for shared services, agile assets, CR ripple effects and more!

SEPTEMBER 30, 2015 • VOLUME 29 NUMBER 16

1105 MEDIA

ACQUIRE

Acquisition & Management Show

Coming June 2016!

2016
JUNE
8-9

WALTER E. WASHINGTON
CONVENTION CENTER
WASHINGTON, DC

Exhibit space is now available!
Contact Stacy Money for pricing & details
smoney@1105media.com 415.444.6933

ACQUIREshow.com

Tracks Include

ACQUIRE
Office Management

ACQUIRE
Professional Services

ACQUIRE
Information Technology
FEDERAL IT ACQUISITION SUMMIT

ACQUIRE
Acquisition Management

ACQUIRE
Project Management

ACQUIRE
Industry Days
Washington Technology

ACQUIRE
Happy Fed
Federal SOUP

Trending

1.3% is the proposed pay raise for federal employees in 2016

Halvorsen wants to change economics of cyberspace

Defense Department CIO Terry Halvorsen has called for industry help in changing the economics of cyberspace so that it is more costly for hackers to inflict damage and cheaper for the Pentagon to defend itself.

“From a standpoint of cybersecurity, right now we’re on the wrong side of the financial spectrum here. We’re losing,” Halvorsen said at an AFCEA NOVA conference in Vienna, Va., earlier this month. “The truth is, you can spend a little bit of money and a little bit of time and exploit some of our weaknesses and cause us to have to spend a lot of money [and] a lot of time” responding to the threat.

> “If you have an impending need to survive, you will innovate.”
>
> — TERRY HALVORSEN, DOD

“If you have an impending need to survive, you will innovate,” he said, adding that DOD networks are “getting shot at” — virtually — every day.

DOD spends about $44 billion annually on cybersecurity and IT, Halvorsen said. Moreover, the cost of cleaning up a mess like the recent hack of Office of Personnel Management systems is hefty. DOD and OPM recently announced a $133 million contract to provide identity and credit monitoring services for some of the victims of the data breach. The contract covers contractors and current and former federal employees across government, not just DOD employees.

Halvorsen told the defense contractors at the AFCEA NOVA conference that the Pentagon needs more automated tools for cyber defense because simply hiring more people won’t solve the problem. Furthermore, focusing on endpoint protection alone won’t get the job done, he added, echoing a strategy pushed by security experts who encourage their clients to assume hackers will penetrate network perimeters.

Halvorsen also singled out software integration as a challenge to his mission and said it has animated his approach to the Joint Regional Security Stacks.

He spoke with a great sense of urgency, which might be attributed to the two-hour meeting on cybersecurity he had had that morning with Defense Secretary Ashton Carter. Halvorsen described the meeting as a special cyber session in which participants agreed that DOD needed to adapt to an evolving threat landscape and to “accept that in this business…the rate of change is going to happen much quicker.”

At the conference, Halvorsen also discussed several ongoing IT initiatives at the Pentagon. In the fiscal year that begins next month, civilian employees of DOD will do six-month rotations with private firms to learn tricks of the trade, he said. The program had previously only been open to uniformed personnel.

The Pentagon is also increasingly using mobile devices, Halvorsen said, adding that in the fall, the department will field smartphones capable of securely accessing top-secret information.

— *Sean Lyngaas*

FCW CALENDAR

10/6 Big data The Army’s Gary Good, NASA’s Daniel Duffy and GSA’s Ryan Swann are among the speakers at this FCW event on mission-centric analytics. Washington, D.C. fcw.com/BigDataAnalytics

10/14 GCN Gala FCW’s sister publication will showcase this year’s GCN Award winners, executives of the year and the 2015 Rising Stars. McLean, Va. gcn.com/gala

10/20 Acquisition The Federal IT Acquisition Summit will feature experts on CDM and reverse auctions, and in-depth discussions on GSA Alliant, Army CHESS, NASA SEWP V and NIH CIO-CS. Washington, D.C. fcw.com/fias

ZAID HAMID

Contents

2015 Federal List

TRENDING

DEPARTMENTS

FCW

THE BUSINESS OF FEDERAL TECHNOLOGY

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, Carolyn Duffy Marsan, Brian Robinson, Sara Lai Stirland

Editorial Fellows 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

PUBLIC SECTOR MEDIA GROUP

Chief Operating Officer and Public Sector Media Group President
Henry Allain

Co-President and Chief Content Officer
Anne A. Armstrong

Chief Revenue Officer
Dan LaBianca

Chief Marketing Officer
Carmel McDonagh

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

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

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

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

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

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

1105 MEDIA INC

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

Trending

$133 million is being spent to protect victims whose background-check data was breached

DHS seeks to develop cyber 'drawbridge'

The University of Oregon will develop a cyber "drawbridge" to help defend financial institutions, news organizations and government agencies against large, sophisticated distributed denial-of-service attacks under a $1.38 million contract with the Department of Homeland Security.

DHS said organizations cannot manage traffic flow to their networks because their Internet service providers do it for them. By putting an electronic drawbridge at the ISP traffic point, organizations could work more closely with ISPs to shut down the DDoS messages that can swamp networks.

— Mark Rockwell

FDA expands access to medical device data

The Food and Drug Administration is expanding the data on medical device performance available through its application programming interface openFDA. The agency is adding device classifications and company registrations to its database, which already offers information on product recalls and adverse events, according to a blog post on the agency's website.

The API allows developers to write apps based on FDA data going back to 1976. New categories such as pre-market and supplementary approvals and device clearances are now available.

Officials noted, however, that FDA has changed some of the types of information it collects, which means long-term comparisons of companies and devices might be difficult.

— Adam Mazmanian

A new team approach to IT R&D

A series of new integrated product teams will cut across a variety of the Department of Homeland Security's research and development activities, DHS Secretary Jeh Johnson said in a Sept. 2 statement. The goal is to unify the agency's technological R&D efforts under the department's overarching "Unity of Effort" initiative.

Johnson said the teams will coordinate and prioritize R&D in a number of areas, including aviation security, biological threats, counterterrorism, border security, cybersecurity and disaster resilience.

— Mark Rockwell

EDITOR'S NOTE

The list that really matters

For more than a decade, FCW's Federal List issue has appeared each fall. Yet although I like listicles as much as the next person — and you'll find plenty of interesting enumerations in the pages that follow — the list that is by far my favorite won't appear until next spring.

I'm referring, of course, to the Federal 100 — FCW's annual awards to honor outstanding individual efforts in the federal IT community. Amid all the budget battles, cyber incursions and problem programs, the Federal 100 provides an important reminder of all the great work that gets done despite the obstacles.

That critical list of what's good in federal IT, however, starts with you. No matter how great an individual's accomplishments are, he or she can't win without being nominated. And it's never too early to start thinking about who deserves the federal IT community's most prestigious recognition.

We'll formally open the nomination process in late October, but start making a list and gathering the necessary information now. And please spread the word so that all the worthy women and men get the consideration they deserve.

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

- **This is an individual award.** Teams are important, too, but we're looking for the women and men who power that collaboration.
- **Winners go above and beyond,** whatever their level or rank. A fancy job title is not required, and doing one's job well is not enough.
- **Results matter.** Exceptional effort is necessary but not sufficient. There must have been a clear impact in the past 12 months.

Know some IT leaders who fit the bill? Then please make sure we know about them as well!

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

FACE TO FACE

UPCOMING EVENTS

Cybersecurity
OCTOBER 27

Big Data
DECEMBER 2

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

For event sponsorship information, contact:
Stacy Money
Senior Sales Director, Events
smoney@1105media.com
(415) 444-6933

1105 PUBLIC SECTOR MEDIA GROUP | FCW | GCN | DEFENSE SYSTEMS | Washington Technology

$44 billion is spent annually on DOD cybersecurity and IT

IN THE IT PIPELINE

WHAT: A request for information for a new personal identity verification system at the Department of Veterans Affairs.

WHY: Government agencies raced to implement two-factor authentication in the recent cybersecurity sprint after the devastating hacks at the Office of Personnel Management. VA finished the sprint within the bounds of success set by U.S. CIO Tony Scott, with 100 percent of privileged users and 80 percent of unprivileged users relying on two-factor authentication to access agency networks.

However, technology has changed in the roughly eight years since VA launched its PIV program. Now officials are interested in the next generation of the cards. VA's tech team said it wants to hear from vendors about what is and isn't possible with PIV cards.

Officials are interested in systems that allow for the remote revocation and reassignment of encryption keys and the ability to add biometric features to the mix. They also want to hear about solutions that can interface with databases containing information on cardholders, including criminal records and the results of background checks.

VERBATIM: "The VA PIV program now requires a technology redesign, development and integration to enable a seamless incremental transition of VA's user population from the current legacy system to a new 'next generation' PIV system [that] supports the evolution of smart card technologies."

READ THE RFI: is.gd/FCW_PIV.

Did 307,000 vets die while awaiting care?

As many as 307,000 veterans might have died while awaiting care from the Department of Veterans Affairs, according to a report from the agency's Office of Inspector General. However, faulty data makes it difficult for the OIG to fully assess the scope of VA's enrollment backlog.

The report substantiates allegations by whistleblowers that 867,000 records were marked as pending and that 47,000 veterans died while awaiting care. But because of deficiencies in the records, the OIG can't know when applications were made or whether pending records are associated with applications to enroll in VA's benefits system.

VA auditors arrived at the 307,000 figure by comparing applications marked as pending with people who were reported as deceased in the Social Security Administration's Death Master File.

The report criticizes the lack of controls in VA's enrollment system. There are no limits on how long applications can be marked as pending before a ruling is made, for example. Additionally, related systems at VA allowed claims processors to delete or improperly mark incomplete applications.

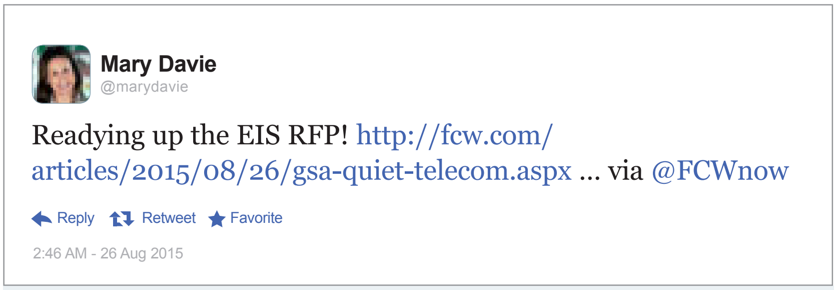
Some deletions were required to eliminate duplicate applications, but the report notes that the lack of a built-in audit trail makes it difficult to rule out manipulation of data as a motivation for expunging records.

The report recommends an overhaul of data management, including controls to guarantee data integrity and rules to govern how long an application may be marked as pending. According to the OIG, VA has an institutional problem with reporting deaths of individuals. Of the 307,000 deceased vets the auditor identified, more than 80 percent have been dead for four years.

The auditors recommend that VA CIO LaVerne Council ensure the collection and retention of audit logs on the system and make sure they are backed up on a monthly basis.

Council said controls would be in place by Aug. 15, a backup system would be active by mid-October, and representatives of VA's OI&T and Office of Accountability Review would meet to discuss whether to take administrative action against any senior IT officials responsible for the lack of controls built into the system. A VA spokesperson did not confirm whether the proposed changes had been implemented or whether the meeting had taken place.

— Adam Mazmanian



Mary Davie
@marydavie

Readying up the EIS RFP! http://fcw.com/articles/2015/08/26/gsa-quiet-telecom.aspx ... via @FCWnow

2:46 AM - 26 Aug 2015

Join the conversation

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

Learn more at Twitter.com/FCWnow.

13TH ANNUAL
ENTERPRISE ARCHITECTURE
EA TODAY: MAKING THE MISSION POSSIBLE

EVENT BEGINS IN 1 MONTH!

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 —
Space is Limitied!

GovEAconference.com
USE PRIORITY CODE: EAE15

PRESENTING SPONSORS
FEAC Institute
ZACHMAN INTERNATIONAL ENTERPRISE ARCHITECTURE

EVENT SPONSORS
In2itive
software AG Government Solutions

PARTNERING MEDIA
OMG WE SET THE STANDARD

PRODUCED BY
PUBLIC SECTOR EVENTS GROUP

STEVE KELMAN is professor of public management at Harvard University's Kennedy School of Government and former administrator of the Office of Federal Procurement Policy.

4 hopes for better contracting next year

What needs to happen to improve IT acquisition — and how likely we are to see it

Here are my hopes for changes that, if implemented, should observably improve the quality of government contracting. I list them in order of how likely they are to happen, starting with the most likely.

1. Agile will spread. The idea that it makes more sense to deliver new IT capabilities in quick, partial spurts rather than a big bang that often never happens is so sensible that, eventually, it has to gain traction. The latest sign that it is making inroads in government is the General Services Administration's recent award of 16 blanket purchase agreements to firms that can perform agile services for agencies.

2. Past performance will become a meaningful part of the acquisition process. Considering past performance is central to satisfying customers. Well-performing suppliers are rewarded with repeat business, and poorly performing ones are gradually weeded out. The government has had a past performance evaluation system in place since the 1990s, but it has been a disappointment in terms of radical change — mainly because the government does a poor job of making honest evaluations. Furthermore, completing the reports is rarely viewed as a central, important feature of contract management.

I still believe that an important regulatory change would be to revise the ability of a contractor to appeal a bad rating as opposed to simply entering the company's view in the contract file. The Office of Federal Procurement Policy has been considering making such a change; now is the time to move on it.

3. Government will commit to training IT subject-matter experts. There are not enough high-quality, up-to-date technical and subject-matter experts in federal IT. We are now coming off a period, inaugurated by the GSA conference scandal a few years ago, of ignorant and populistic disrespect for training feds to develop their knowledge base. Especially in a rapidly changing field like IT, knowledge must be constantly renewed. Given the huge amount of money the government spends on IT, skimping on workforce development almost defines the concept of penny wise and pound foolish.

> Skimping on workforce development almost defines the concept of penny wise and pound foolish.

We need to revamp how agencies conduct conferences and training. Government conferences are too often skewed toward self-promotional "listen to what I did" shows by government and industry representatives. Feds need more opportunities to truly learn from outside experts sharing state-of-the-art knowledge.

4. Officials will begin discussing how to balance IT development responsibilities between contractors and feds. The last thing we want is for government to be in the business of developing IT applications. However, I don't see how it is practical for agencies to do a good job of managing contractors without a cadre of government employees who understand both the technologies and project management well enough to be able to evaluate what contractors are saying. And for that to happen, feds need hands-on experience.

I don't have a full-blown solution to this challenge, and I suspect this wish has the smallest chance of coming true this year. Contractor opposition is likely to be significant, and there's no clear model for how to make it happen. Should a few projects be managed in-house? Should agency personnel be involved in some coding or project management teams rather than simply receiving reports from contractors?

We need a discussion in the coming year about how to proceed. Both 18F and the U.S. Digital Service have put the issue of government technical expertise on the agenda, but it appears the infusion of expertise they bring, however welcome, is likely to be short-term. ■

BOB STEVENS is vice president of federal systems at Lookout.

Why shadow BYOD is your next big problem

Mobile might not be the most serious security risk, but it needs far more attention than it has been getting

It's nearly impossible to find a recent article about federal cybersecurity that doesn't mention the Office of Personnel Management hack — and for good reason: It has raised some very serious questions about our nation's cybersecurity practices or, more accurately, the lack thereof.

Without question, there is massive room for improvement. Yet recent discussions have all but overlooked one critical piece of the federal security puzzle: mobile devices.

Some might ask, "Why focus on mobile when in many areas of government, smartphones aren't even allowed?" After all, there's no reason to believe the OPM hack involved a mobile component. Yet for that very reason, mobile devices remain sitting ducks as entry points for similar attacks in the future.

In fact, after analyzing 20 federal agencies, Lookout recently discovered 14,622 personal devices associated with government networks. That means people, permitted or not, are connecting their smartphones and tablets to federal systems. In this sample, those devices encountered an astounding 1,781 app-based threats such as spyware or Trojans.

So government employees are not only using their smartphones to regularly access potentially sensitive government data and their agencies' Wi-Fi networks, but those devices are encountering threats that could put the devices and the data they access at risk.

Adding more fuel to the fire, a recent survey of more than 1,000 federal government employees (also commissioned by Lookout) revealed a sobering set of statistics:

- 58 percent of federal employees are aware of the security consequences of using their personal mobile phones for work, yet 85 percent will use their phones for potentially risky activities anyway.
- 50 percent of federal employees access work email on their personal devices, and another 49 percent use their personal devices to download work documents.
- 7 percent of federal employees claim they jailbreak or root a device they bring to or use at work. Those practices introduce vulnerabilities that attackers can exploit, and they make it easier to download apps from third-party marketplaces that tend to have a higher number of malicious apps.
- 18 percent of employees claim to have encountered malware on their mobile devices, including both personal and government-issued devices.

> All federal agencies have some level of BYOD taking place, whether officially sanctioned or not.

Clearly, all federal agencies have some level of bring-your-own-device activity taking place, whether officially sanctioned or not. And this shadow BYOD introduces countless risks for sensitive data leakage. This is not to say that more traditional entry points no longer pose risks or that mobile is a greater threat — but mobile is being completely overlooked.

So how do you address shadow BYOD and minimize potential risks? For many government agencies, the answer is to institute more policies. But policies alone won't address the underlying issues of why shadow BYOD is happening in the first place.

In the aforementioned survey, nearly 40 percent of employees who work at agencies that have rules prohibiting personal smartphone use at work said those rules have little or no impact on their behavior. Employees want access to mobile technology to do their jobs, but the government is not moving at the speed of technology.

The answer lies in embracing BYOD programs wholeheartedly, which involves having the tools and technologies in place that provide visibility into what's really happening on federal networks and offer protection against potential harm. If we wait for a mobile attack to cause a devastating government data breach before we start considering how to tackle the significant mobile security challenge, it will already be too late. ■

6 hidden costs of continuing resolutions

BY ADAM MAZMANIAN

No one really expects the appropriations process to function seamlessly these days. Congress and the president have produced full appropriations for all branches of government only four times in the past 40 years. This year looks like no exception.

Barring an unlikely outbreak of bipartisanship, there doesn't appear to be enough time left in the fiscal year and the congressional calendar to enact all the appropriations bills before fiscal 2016 begins Oct. 1. That means either a continuing resolution or a shutdown.

Missing the fiscal year deadline isn't anything to be too alarmed about, said Doug Criscitello, who served as chief financial officer at the Department of Housing and Urban Development and the Small Business Administration and is now executive director of MIT's Center for Finance and Policy.

It's fairly routine for Congress to pass a six-week continuing resolution early in the fall session to provide time to resolve outstanding budget issues before the Thanksgiving recess. However, sometimes multiple CRs are required to keep the government open. There were seven in 2011 and five in 2012.

Although multiple short-term CRs are less disruptive than a full or partial government shutdown, they do carry costs borne by agency officials, including:

2015 Federal List

1. OMB's scrutiny

Relationships between agencies and the Office of Management and Budget can be strained in the best of times. But during a continuing resolution, OMB handles the tricky business of apportionment — doling out funds to agencies in a way consistent with the length and terms of the CR. If an agency has an expense that is outside the ordinary, OMB must approve it.

During a CR, OMB can "take on an aura of the trustees' role in a corporate bankruptcy," Criscitello said.

OMB's guidance makes the point painfully clear: "Because of the nature of CRs, you should operate at a minimal level until after your regular fiscal year appropriation is enacted."

2. Lost productivity

For each short-term CR, agencies must conduct a great deal of compliance activity. "From a management perspective, it's a lot of paperwork," said John Palguta, a longtime government human resource manager and currently vice president for policy at the Partnership for Public Service. "That's certainly a big headache for CFOs and others. You feel like you're spinning your wheels sometimes."

The activity includes creating guidance for programs and offices, making and disseminating new spending plans for each CR, and responding to congressional and intergovernmental requests for information. The FBI estimated that its accountants and others spent 600 hours on CR-related management activity in 2009, according to a Government Accountability Office study.

3. De facto hiring freeze

The hiring cycle for college students begins in the fall as major recruiters make the rounds of career fairs to find promising job candidates. Agencies have a harder time competing with companies when their funding is mired in a series of short-term spending bills, Palguta said.

By the time an agency gets its full-year funding, "some of the best talent is already taken," he added.

And the problem isn't just at the entry level. "The whole process of filling jobs becomes more complicated," Palguta said.

Sometimes an agency with a high-level vacancy will issue a job announcement in the hope that by the time applications are screened and interviews are conducted, the money will be available to make a hire.

Sometimes, however, "you may have someone you want to hire but you can't make an offer yet," Palguta said. The most sought-after candidates aren't likely to be available for long. "Those are people who have options. They're not waiting around for Congress to get its act together."

4. Delayed procurement and training

Under a CR, IT upgrades, training and other optional expenditures can often get kicked to the curb. Agencies have already adjusted in some ways to the inevitable funding delays by trying to push spending to later in the fiscal year. "The first quarter is a terrible time to plan conferences and training," Criscitello said.

The constraints also take a toll on acquisition because program managers don't know how much they'll end up having to spend for the full year.

Delays in training can diminish an agency's core mission delivery. In one instance noted in the GAO report, a Food and Drug Administration official reported that the agency wasn't able to meet targets for inspections because of a lack of trained personnel.

"The biggest hidden cost is from a management perspective," Palguta said. "You do not know how much you're going to be able to spend to manage your organization."

According to the GAO report, agencies have already begun backloading essential annual services contracts into the third and fourth quarters, such as janitorial services and maintenance. But managing contracts is difficult under a CR because of the necessity to perform administrative tasks associated with spending for each short-term measure.

5. The mad dash once funding comes

When a real appropriation or full-year CR is in place, activity ramps up, but the frenetic pace to finish agency work on a compressed schedule can result in sub-optimal performance.

Acquisition professionals who are juggling a number of procurements "may not have time to negotiate the best deals," Palguta said. "It increases the odds that both the government and the taxpayer are losing out a bit."

6. Morale

Careering from one short-term CR to the next takes a toll on personnel. "The psychic costs are probably higher than the actual costs," Criscitello said.

The cycle of responding to CRs and then ramping up activity once funding comes through can be dispiriting, and it certainly doesn't resemble the image of government service that drew employees to federal careers.

Moreover, agency employees are personally under the gun to make sure they comply with the limitations in place during a CR. The Antideficiency Act, which governs how federal agencies comply with appropriations, contains criminal penalties for individuals who spend government money that is not properly appropriated and programmed.

"I don't know if anyone has gone to budget jail," Criscitello joked. Most violations are accidental or technical, but the law looms over any agency employee tasked with implementing spending restraints during a CR.

In short, there is no upside. It's not as though agencies are freed from their obligations to Congress during a CR. All the policy riders, requests for information and reports, and other demands contained in appropriations bills and reports from the previous year carry over during CRs until they are supplanted by new legislation. ■

> "The biggest hidden cost is from a management perspective. You do not know how much you're going to be able to spend to manage your organization."
>
> **JOHN PALGUTA, PARTNERSHIP FOR PUBLIC SERVICE**

16 firms to turn to for agile

BY ZACH NOBLE

After a long wait and multiple delays, the General Services Administration's 18F agile blanket purchase agreement is up and running.

In announcing the awards in late August, 18F's consulting team praised 16 successful vendors for their delivery of "amazing, working software" in response to a request for quotations.

Unlike typical contract vehicles, the agile BPA sought to pool GSA Schedule 70 vendors for rapid agile or DevOps work on 18F and partner agency projects, and would-be vendors had to offer a functional project, not just a proposal, to seal the deal.

The 16 vendors to win a slot on the BPA are:

1. Acumen Solutions
2. Applied Information Sciences
3. Booz Allen Hamilton
4. DSoft Technology
5. Environmental Systems Research Institute
6. Flexion
7. NCI Information Systems
8. PricewaterhouseCoopers Public Sector
9. SemanticBits
10. TechFlow
11. TeraLogics
12. Three Wire Systems
13. True Tandem
14. Vencore Services and Solutions
15. Ventera
16. World Wide Technology

The process was not entirely smooth, however. Overwhelmed by questions about the novel BPA, 18F pushed back the deadline for the RFQ not once but twice.

"Before the RFQ release, we held a presolicitation conference so we could preview the RFQ to vendors and answer questions, with the goal of reducing the questions during the official Q&A period," the 18F team wrote. "Despite that, after the release, hundreds more questions still poured in — mostly on technical or contracting issues. To respond to this volume, we missed our own answer deadline, and that ended up pushing back the vendors' deadline to respond."

The team thanked the Federal Acquisition Service for working through the issues with them.

18F officials admitted to being frustrated by the delay but claimed to have learned valuable lessons from the process.

"We think we were successful in demonstrating some solid innovation with the award process, but we've got a long way to go now before we can declare success on what really matters: demonstrating the ability to partner with industry to deliver successful digital services to our customers using agile delivery practices," they wrote. "In other words, as with the rest of 18F, delivery is the strategy, and now we're looking forward to shipping under the BPA."

Officials also pledged that other vendors would be afforded on-boarding opportunities in the future. ■

2015 Federal List

LIVE! 360

TECH EVENTS WITH PERSPECTIVE

2015 Orlando

ROYAL PACIFIC RESORT AT UNIVERSAL

November 16-20

Visual Studio LIVE! | SharePoint LIVE! | SQL Server LIVE! | Modern Apps LIVE! | TECHMENTOR

The Ultimate Education Destination

Live! 360 is a unique conference where the IT and Developer community converge to test-drive leading edge technologies and fuel up on current ones. These five co-located events incorporate knowledge transfer and networking, along with finely tuned education and training, as you create your own custom conference, mixing and matching sessions and workshops to best suit your needs. All roads lead to Live! 360: **the ultimate education destination.**

REGISTER BY OCTOBER 14 AND **SAVE $300!**

Use promo code L360OCT1

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

5 Great Conferences

1 Great Price

LIVE360EVENTS.COM

EVENT PARTNERS

Microsoft Magenic

PLATINUM SPONSORS

GRIDSTORE PLURALSIGHT

GOLD SPONSORS

e-SignLive by Silanis GitHub

PRODUCED BY

1105 MEDIA INC

YOUR GROWTH. OUR BUSINESS.

16.7

16.7 reasons to watch the CSC/SRA deal (and 2.7 billion small causes for concern)

BY NICK WAKEMAN

In a summer of blockbuster deals, Computer Sciences Corp. and SRA International might have pulled off the biggest of the bunch.

CSC is buying SRA for $390 million and the assumption of $1 billion in debt. The deal will close when CSC splits into two companies by the end of November. SRA will be integrated into CSC's public-sector business, to be known as Computer Sciences Government Services.

The combination will create a new business with $5.5 billion in revenue and 19,000 employees. SRA is contributing $1.4 billion in revenue and 5,600 employees to those totals.

Larry Prior, currently the leader of CSC North American Public Sector, will be CEO of the combined SRA/CSC government business. Current CSC President Mike Lawrie will be chairman of both CSC and CS Government Services after the split.

SRA CEO Bill Ballhaus has agreed to stay on through at least the end of November, Lawrie said during an investor call in August.

Impressive profit margins

Obviously, Lawrie and other CSC leaders are excited about the deal, and they've released some impressive numbers to support their enthusiasm.

The margins are attention-getting. Both companies boast adjusted earnings before interest, taxes, depreciation and amortization that are well above the industry average. While most companies are struggling to report EBITDA in the mid to high single digits, CSC reported that the EBITDA for its government business is 16.4 percent and SRA's is 14 percent. Officials expect the combination of the two companies to have EBITDA of 16.7 percent.

Lawrie said the companies have been on parallel paths in recent years to transform their respective businesses. "Each has become extremely cost competitive and highly tuned to the current market environment," he said. "We'll have industry-leading profit margins and strong cash flow to support dividends and to deleverage."

SRA founder Ernst Volgenau built a business that is now poised for a lucrative and industry-shifting merger.

2015 Federal List

Deleveraging will likely be a priority because CS Government Services will have $2.7 billion in debt when it completes the twin transactions of splitting from CSC and acquiring SRA. The debt includes a $10.50 per share special dividend that will be paid to each CSC shareholder as part of the split.

SRA's shareholders — which are primarily Providence Equity Partners, SRA founder Ernst Volgenau and SRA management — will receive $390 million in cash.

The $2.7 billion also includes refinancing SRA's $1 billion in debt.

Once the deal is completed, CS Government Services shareholders will own 84.7 percent of the company and SRA shareholders will own 15.3 percent.

'Playing the role of consolidator'

The acquisition of SRA should also dispel the rumors that CSC was splitting off its government business to make it an easier takeover target for other buyers. "With this move with SRA, we are really playing the role of consolidator," Lawrie said. "You can't make a stronger statement than that.... We are not running the commercial business and the [North American Public Sector] business with the idea of positioning them for sale."

SRA was attractive because it "was a clean asset, well managed, well disciplined with good cost controls, and we had very little overlap," Lawrie said.

CSC has gone through its cost-control phase and is now ready to pivot toward growth. To acquire another company that needed to go through its own cost-control phase would likely have slowed that momentum, he added.

"I think this industry is going to consolidate, and scale is increasingly important for next-generation solutions and strategies," Lawrie said. "We wanted to be an early mover in creating a platform solely dedicated to IT services."

The CSC split also played a role because the acquisition of SRA likely would not have happened if CSC had remained in its current structure with two-thirds of the business being commercial, he said.

With the acquisition of SRA, CS Government Services' business mix will be about 52 percent defense and intelligence, 30 percent health and civilian, and 13 percent from the Department of Homeland Security.

Lawrie said the acquisition will combine the technical capabilities and solutions that CSC has developed in recent years — particularly around the cloud and managed services — with SRA's focus on the customer and the mission.

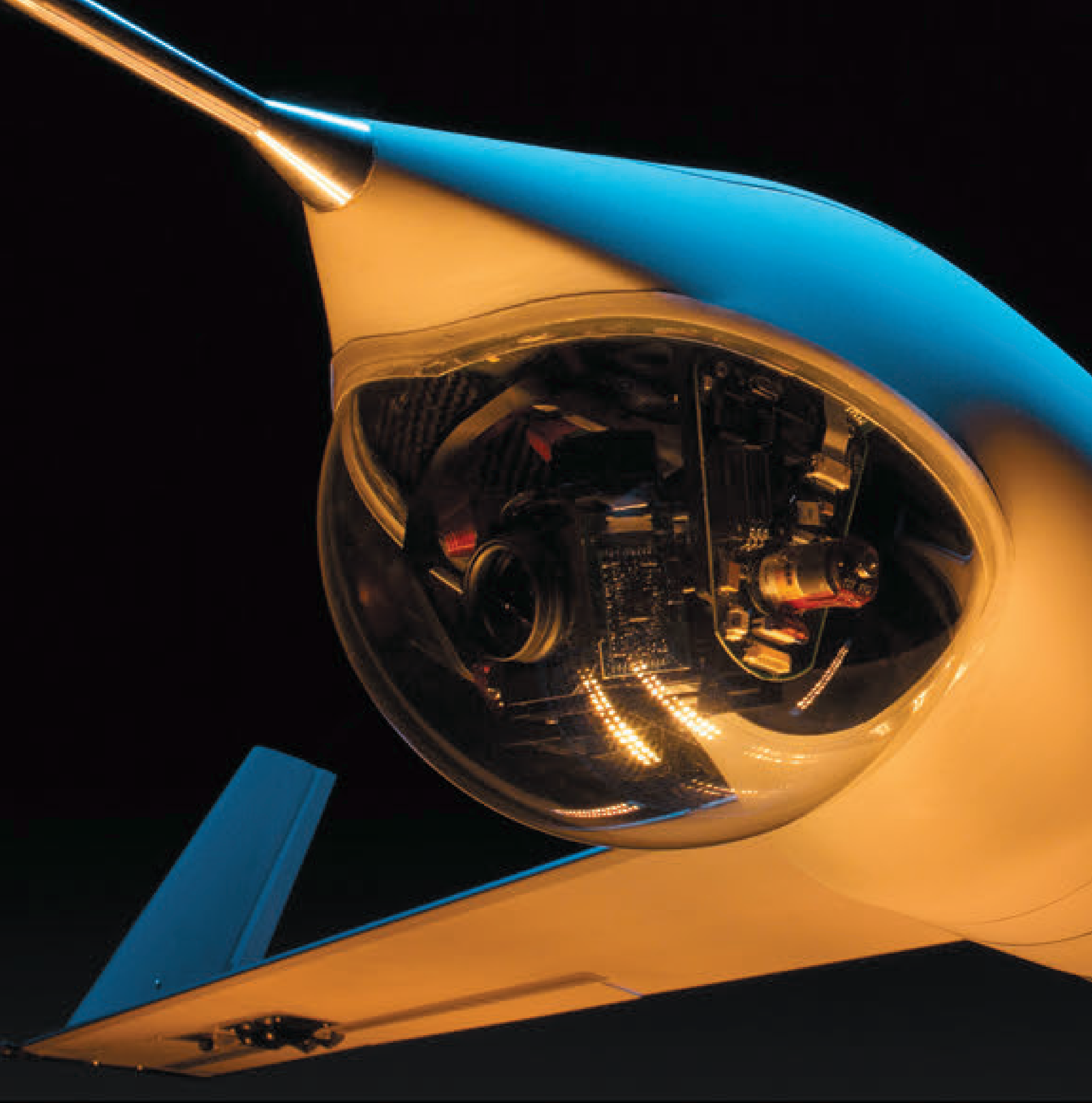
"This will drive significant value for clients, shareholders and employees," he said.

A great example is CSC's recent win of a $109 million Federal Aviation Administration cloud contract. "We partnered with Amazon and Microsoft and developed a world-class hybrid cloud solution, and we see more opportunities like that," he said.

Specifically, the combined

"This will drive significant value for clients, shareholders and employees."

MIKE LAWRIE, CSC



Intelligence, Surveillance & Reconnaissance

Network Systems

Secure Communications

Command & Control

ENDURING AWARENESS

BOEING

companies will have IT capabilities such as cybersecurity, software development, cloud and IT infrastructure. Those areas will represent about three-quarters of revenues, Lawrie said.

Other revenue sources include domain-specific professional services such as intelligence analysis, bioinformatics and health sciences, energy and environmental consulting, and enterprise planning and resource management.

A market in transition

The CSC/SRA deal is one of the most transformative of the several transformative acquisitions that have hit the market in recent months, particularly for pure IT companies.

We've seen deals by Engility and PAE add scale and new capabilities through acquisitions. We've seen several other deals in which companies were acquired by private equity groups looking for a platform as the government services market heads deeper into a period of consolidation.

I put CSC and SRA at the top of the heap because of the struggles both companies have gone through in recent years. In many ways, their combination validates the value of what they've been doing.

SRA also is a legendary company in the market because of Volgenau, one of the pioneers of the government services business. He founded SRA in 1978 and grew it to nearly $2 billion in revenue and a successful initial public offering.

The government IT services market is going through a period of transition. There is overcapacity. The customer is hyper-focused on cost because of budget and resource constraints. There is also a revolution in technology being driven by the adoption of cloud and managed services, which is breaking down traditional business models. Companies are scrambling to adjust, survive and find a way forward.

The CSC/SRA deal will not be the last big one to hit the market. Still to come is how Lockheed Martin will divest itself of its IT business. I've also heard rumors that major divestitures by other companies are in the works.

In many ways, companies like Lockheed Martin are trying to move away from the IT services business while others are embracing it, particularly when they have the cost model in place to make it profitable.

Lawrie and CSC believe they have the cost model to make being a pure-play IT services company work for its employees, customers and investors. Right now, they have the numbers to back it up. ■

2015 Federal List

14 rising stars in federal IT

Each year, FCW recognizes individuals who are in the first 10 years of their federal IT careers yet are already having an outsized impact in the community. These women and men are not only making a difference today — they are put forth by their peers and managers as the likely leaders of tomorrow.

Perhaps unsurprisingly in a year dominated by data breaches, this year's class of Rising Stars is weighted heavily toward cybersecurity. But other innovators are working on everything from acquisition to website development.

Full profiles will run in an upcoming issue of FCW, and the winners will be honored in person at the Oct. 14 GCN Awards gala. Until then, here's a quick preview of the 2015 Rising Stars — 14 people you'll be hearing about for years to come:

RISINGSTAR

Akosua Ali
Department of Homeland Security

Michael H. Brody
Department of Homeland Security

Lindsay Burack
Sapient Government Services

Evan Chan
Jet Propulsion Laboratory, NASA

Regina Kassar
Red Team Consulting

Nicholas Keshavarz-Nia
Noblis

Alexander Lin
TCG

Erica McCann
Information Technology Alliance for Public Sector

Katherine Mullins
Department of Homeland Security

Mark Naggar
Department of Health and Human Services

Christina Prat
Customs and Border Protection

Teresa Rodriguez
U.S. Forest Service

Michael Wheeless
Oceus Networks Inc.

Andrew Yuen
Environmental Protection Agency

Top 10 stories on FCW.com

Most FCW readers strive to make government work better, but they're only human. And 12 months of web traffic proves yet again that conflict drives clicks.

1. Continued turmoil at the Department of Veterans Affairs

Whether it was the departure of Deputy CIO Steph Warren or congressional inquiries into the department's reform efforts, VA IT was far and away the most popular topic.

2. What really happened in the OPM breach

Readers naturally wanted to know what the Office of Personnel Management breach meant for them — and FCW's exclusive report in August on the official timeline of hacker activity and federal response was deemed a must-read.

3. Former DISA comptroller alleges retaliation

The standoff between then-DISA Director Lt. Gen. Ronnie Hawkins and former Comptroller Jimaye Sones even drew congressional attention.

4. Bad news about the Internet of Things

When National Institute of Standards and Technology Fellow Ron Ross declared the Internet of Things essentially indefensible, the Internet took notice.

5. DHMSM: DOD's massive electronic health records contract

The July 29 announcement that a team led by Leidos, Accenture and Cerner would get the multibillion-dollar contract drew top-five traffic numbers by itself. If this were a top 20 list, several other stories related to the acquisition would be on the list as well.

6. The future of FedRAMP

More than three years after the Federal Risk and Authorization Management Program was first floated, the federal IT community is still carefully parsing its progress.

7. Understanding State's big database crash

FCW published a Q&A with Greg Ambrose at the beginning of fiscal 2015 and found that lots of people wanted to know how passport and visa services could just stop.

8. What program management really means

Drama and conflict didn't have a complete monopoly on page views: This April package on program management proved that substance sells, too.

9. NASA's SEWP V

The announcement of contract winners last October drew serious traffic, and the continued coverage of protests, additional awards and SEWP V finally opening for business kept FCW readers coming back.

10. The disappearance of TaxmanKeith

Who knew that an anonymous Reddit poster — believed to be an Internal Revenue Service employee — would spark such widespread reader interest?

5 reasons shared services are slow to stick

BY CAROLYN DUFFY MARSAN

2015 Federal List

With its brilliant photography and educational videos, NASA.gov attracts 600,000 unique visits per day. Thanks to a new cloud-based, shared-services approach to its web infrastructure, the agency is saving 25 percent to 30 percent a month on the cost of operating NASA.gov and 125 other websites.

"NASA wanted to centralize all the Web applications that are external to the enterprise…and move them to an enterprise-managed cloud solution," said Raj Ananthanpillai, CEO of InfoZen, an independent cloud broker that is the prime contractor on NASA's Web Enterprise Service Technologies contract.

NASA's five-year WEST contract involves centralized web hosting, operations and security for external and internal websites and web applications, including content management. So far, InfoZen has migrated 1 million pieces of content to the new cloud environment, which features a Drupal open-source architecture that allows NASA to update content on its websites in minutes rather than hours.

NASA's approach, however, is an anomaly. Despite mandates to choose cloud and shared services first, successful projects in the federal government are few and far between.

Cloud-based shared services offer proven cost savings and time-to-market advantages, but the biggest obstacle to adoption is cultural. Agencies have many fears, including losing control of data and applications, meeting federal standards for information security and adopting new methods of acquisition.

"We're on a very slow path," said Kevin Greer, managing director of shared-services operations at Accenture Federal Services. "While they say it's cloud first and shared first, it's not operational for most back-office applications. The government lacks an overall framework and governing body to move this initiative forward."

Although email migrations to the cloud have garnered attention, experts say the majority of savings will come when the 200-plus federal agencies adopt shared services for back-office applications, including financial management, human resources, supply chain and IT administration.

Many agencies understand the benefits. In a message to employees in November 2014, Department of Veterans Affairs Secretary Robert McDonald listed shared services — with their potential to improve efficiency, reduce cost and increase productivity — as one of his top priorities.

"Right now, we're looking at options used in the private sector to enhance our rapid delivery of services and also at our own business processes that are suited for shared services," McDonald said.

Accenture has documented savings ranging from 20 percent to 45 percent with the shared-services projects that it has conducted for states. Ohio, for example, anticipates $145 million in net savings over 20 years after moving accounts payable, travel reimbursement and other back-office applications to a cloud-based, shared-services model that supports 17,000 employees.

"The benefits are clear," Greer said. "Shared services drive standard business processes and result in operating with fewer errors, the delivery of better customer service and, most importantly, significant cost savings through eliminating redundant operations.... We came up with an estimate of $20 billion in savings if all federal agencies were to migrate to shared services on back-office operations."

Off to a slow start

Accelerating the deployment of shared services has been a priority of the Obama administration for five years. They are part of the president's 25-Point Implementation Plan to Reform Federal IT Management, which was released in December 2010. Cloud services and shared solutions "will result in substantial cost savings, allowing agencies to optimize spending and allowing agencies to reinvest in their most critical mission needs," the plan states.

In 2012, the White House released a follow-up report called the Federal IT Shared Services Strategy, which was designed to eliminate waste and duplication. The strategy identified 34 areas where federal agencies provide similar services and could adopt a shared-services model. Agencies need to use shared services to deliver solutions "faster, for less money and with fewer resources," the strategy states.

Since then, several agencies have successfully adopted cloud-based platforms for email, collaboration, mobile device management, software testing, websites and web services. The National Oceanic and Atmospheric Administration moved its 25,000 users to Google Apps for Government as did the National Archives and Records Administration with its 5,000 users. The Army, meanwhile, has licenses for 50,000 Microsoft Office 365 users.

A handful of back-office migrations are also underway, with the Treasury's Administrative Resource Center running an Oracle-based cloud platform and the Agriculture Department using SAP's cloud-based infrastructure.

Nevertheless, Greer said agency CIOs are concerned about giving up control over their back-office systems and information security due to auditing and regulatory requirements.

"We did a survey with the Association of Government Accountants, and we talked to 200 government officials," he said. "Seventy percent of the people were very afraid of migrating to the cloud not knowing if their data is safe or met security requirements. That's one of the major concerns."

The survey identified other barriers to cloud-based shared services, including concerns about effective

"We came up with an estimate of $20 billion in savings if all federal agencies were to migrate to shared services on back-office operations."

— KEVIN GREER, ACCENTURE

governance, paying for the transition, the lack of providers that meet federal regulations and the need to develop a strategy for employees.

Agencies "don't want to be the first mover," Greer said. "They are very skeptical and question the amount of successful implementations. Forty-two percent of respondents said that it is not in their culture to give up a function if done cheaper or better."

And even when an agency wants to adopt cloud-based shared services, standardizing data and processes is a time-consuming prerequisite.

"It's about getting ready for central or shared services. That's the big issue," said Bill Beyer, a partner at Deloitte who is responsible for shared-services projects. "You can't go from vision to implementation without setting the table properly. You have to do data cleanup before you throw everything up into the cloud. You can save anywhere from 17 percent to 30 percent in the cloud, but you don't want to throw junk up into the cloud."

Another issue is funding. For example, federal agencies already consolidated 26 payroll systems into four back in 2009, an initiative that the Office of Personnel Management said would save $1 billion in a decade. Now those four payroll systems must be migrated to the cloud, but funding is necessary to pay for that upgrade.

"The government didn't bank these savings from the payroll systems," Beyer said. "Now they have antiquated payroll systems that need to be upgraded and migrated to the cloud. They don't know where the money is coming from."

He added that migrating to the cloud requires agencies to staff up and run duplicative systems for a period of time. So extra funding is needed until the savings of a cloud-based system kick in. "There is a funding issue, and [the Office of Management and Budget] is trying to address it," Beyer said.

Human resources applications are likely to be the next to migrate to the cloud, he added. Pilot projects involving Salesforce.com and Oracle are underway; both companies have received approval under the Federal Risk and Authorization Management Program.

Pushback for Peace Corps' email upgrade

The Peace Corps One offers one example of a cloud-based shared-services project that went awry. The agency came under fire for moving too quickly on a plan to migrate its email, collaboration and document management systems to the cloud through the General Services Administration's shared-services model.

GSA's own cloud-based email system has been extremely successful. In 2011, the agency adopted Google's applications for email and collaboration in a move that is expected to save the agency $15 million over five years. By swapping a legacy IBM Lotus Notes system and replacing it with Google Docs for its 17,000 users, GSA cuts its email costs in half.

Under pressure to migrate its own aging email system to the cloud, the Peace Corps decided to piggyback on GSA's procurement and adopt Google's platform. Sheila Campbell, the Peace Corps' director of digital integration, won a 2015 Federal 100 award for driving that pilot project. However, the Peace Corps' Office of Inspector General issued a report in March questioning whether the agency had followed federal acquisition rules when it signed a memorandum of understanding with GSA to use its cloud-based email service on a pilot basis.

"Before the Peace Corps pursued and entered into a shared-services model, a technology platform should have been researched and identified by the [Office of the CIO]," the IG report states. "There should have been a broad analysis of the different types of cloud platforms... and an analysis to determine if these different platforms would meet the needs of the Peace Corps."

Auditors recognized that the shared services model is beneficial to the government and is being promoted by the Obama administration, but they asserted that the agency did not take the time to evaluate whether the cloud pilot met federal regulations regarding email

2015 Federal List

records or IT security. And the IG recommended that the Peace Corps terminate all pilot users from GSA's Google Apps cloud pilot and start over with a requirements analysis, an acquisition analysis and an IT security assessment before signing any agreement with a cloud services provider.

The Peace Corps is still exploring cloud email solutions, but the shared-services approach with GSA appears to be off the table.

OBSTACLES TO SHARED SERVICES

1. Acquisition processes
2. Data standardization
3. Migration costs
4. Security concerns
5. Questions of control

Steve Kousen, vice president of cloud strategy and integration services at Unisys Federal, acknowledged some bumps along the way with projects like the Peace Corps' email system.

"We have to make the acquisition of cloud-based services easier and more streamlined," he said. "It's about agility, it's about speed, and it's about doing more with less people."

One agency that's tackling the acquisition problem for cloud-based shared services is the Interior Department, which offers what it calls Foundation Cloud Hosting Services. This acquisition vehicle allows customers to purchase cloud-based offerings from Google, Microsoft, Amazon Web Services and others. Ten systems integrators, including Unisys, are on the FCHS deal, which could be worth $10 billion over the next decade.

"This vehicle is alive and going very well," Kousen said, adding that his company is receiving requests from various Interior components and other agencies.

Interior has a history of running shared services through its Interior Business Center, which manages financial systems for 17 agencies. Indeed, experts say such centers are likely to deploy cloud-based offerings in areas such as human resources, payroll, financial management and procurement to ease the acquisition process for smaller agencies.

"Interior is migrating to SAP in the cloud," Kousen said. "Now we're really starting to talk about core enterprise management systems in the cloud. That's the next wave."

OMB mandates expected

One question is whether OMB will outline specific mandates for agencies to migrate to cloud-based shared services.

"Everybody knows shared services are imminent," Beyer said. "The question is what this administration can do over the next 15 to 19 months that leaves a blueprint and legacy to move agencies toward shared services. Any administration that comes in is going to adopt this. It's inevitable. It's going to happen. The issue is what the Obama administration can do to lay a strong foundation for the next public servants."

Greer said OMB is likely to forbid agencies from upgrading their human resources systems and instead require them to adopt a shared service similar to the steps it has taken with financial management applications. Because many agencies have enterprise software licenses that expire in the 2017-2018 timeframe, Greer predicts that there will be a spike in shared-services migrations during that time period.

"If you're a Cabinet-level agency, you can no longer upgrade an old legacy financial management system," he said. "You have to prove why you can't go to a shared-services provider or cloud-based service. OMB is looking to entice or force shared-services consolidation. If HR follows that direction, it will be an important milestone."

He added that he doesn't think the Obama administration's lame-duck status will affect the slow but steady shift to cloud-based shared services because the cost savings are too great.

"Shared services is good government, and it's part of a strategic effort to improve government efficiency," Greer said. "It's a bipartisan issue that I think all parties would want to implement and provide savings to the taxpayers." ■

Top 50 systems integrators

The rankings for the top 50 systems integrators are based on government procurement data for fiscal 2014, which was analyzed using product and service codes for IT, systems integration and other professional services. Dollar amounts are in thousands.

SOURCE: FEDERAL PROCUREMENT DATA SYSTEM

RANK	COMPANY	PRIME CONTRACTS
1	Lockheed Martin Corp.	$9,296,514
2	Northrop Grumman Corp.	$5,171,445
3	Boeing Co.	$5,043,363
4	Leidos Inc.	$3,679,551
5	Raytheon Co.	$3,637,676
6	Booz Allen Hamilton	$3,564,546
7	General Dynamics Corp.	$2,863,739
8	Hewlett-Packard Co.	$2,616,718
9	Computer Sciences Corp.	$2,335,839
10	CACI International Inc.	$2,005,412
11	California Institute of Technology	$1,722,053
12	AECOM Technology Corp.	$1,554,734
13	Lawrence Livermore National Security LLC	$1,458,140
14	IBM Corp.	$1,358,114
15	L-3 Communications Corp.	$1,260,913
16	Mitre Corp.	$1,242,836
17	Battelle Memorial Institute	$1,194,539
18	Accenture	$1,158,775
19	BAE Systems Inc.	$1,135,338
20	Deloitte LLP	$1,119,546
21	Jacobs Engineering Group Inc.	$1,119,170
22	SRA International Inc.	$1,098,369
23	Harris Corp.	$998,435
24	Johns Hopkins University	$993,884
25	Massachusetts Institute of Technology	$963,227
26	DynCorp International LLC	$923,540
27	Fluor Corp.	$908,003
28	Alion Science and Technology Corp.	$881,904
29	ManTech International Corp.	$853,104
30	CGI Group Inc.	$821,810
31	Aerospace Corp.	$779,103
32	Dell Inc.	$767,641
33	Wyle Services Corp.	$669,702
34	Exelis Inc.	$653,313
35	Serco Group PLC	$634,044
36	Verizon Communications Inc.	$630,791
37	Engility Corp.	$619,205
38	CDW Corp.	$589,915
39	At&T Inc.	$543,707
40	PAE	$535,610
41	Sierra Nevada Corp.	$519,486
42	Mythics Inc.	$478,040
43	Iron Bow Technologies LLC	$475,921
44	Vectrus Systems Corp.	$459,765
45	Honeywell International	$447,732
46	Unisys Corp.	$435,673
47	Science Applications International Corp.	$428,662
48	Red River Computer Co. Inc.	$427,092
49	Chemonics International Inc.	$415,488
50	immixGroup Inc.	$414,292

2015 Federal List

Top 20 GSA Schedule 70 companies

The top-selling companies on the General Services Administration's Schedule 70 for IT products and services cover the range of government contractors. The rankings are based on total sales via Schedule 70 in fiscal 2014; dollar amounts are in thousands.

SOURCE: FEDERAL PROCUREMENT DATA SYSTEM

RANK	COMPANY	SCHEDULE 70 SALES
1	Mythics Inc.	$617,788
2	Carahsoft Technology Corp.	$553,665
3	Cellco Partnership (Verizon Wireless)	$547,393
4	Dell Marketing L.P.	$524,584
5	IBM	$519,267
6	Accenture Federal Services LLC	$381,560
7	Insight Public Sector Inc.	$284,359
8	DLT Solutions LLC	$265,777
9	immixTechnology Inc.	$249,723
10	SRA International Inc.	$242,864
11	CGI Federal Inc.	$204,697
12	Softchoice Corp.	$186,649
13	Booz Allen Hamilton Inc.	$178,450
14	EC America Inc.	$169,421
15	Artel LLC	$167,121
16	Northrop Grumman Information Technology	$164,771
17	CDW Government LLC	$149,273
18	CA Inc.	$139,975
19	Leidos Inc.	$139,362
20	At&T Mobility LLC	$133,320

Top 20 service-disabled veteran-owned companies

The 20 top-selling companies owned by service-disabled veterans did an aggregate government business of $2.4 billion in fiscal 2014. And that's just prime contracts; the total does not include subcontracting work. The dollar amounts in the chart are in thousands.

SOURCE: FEDERAL PROCUREMENT DATA SYSTEM

RANK	COMPANY	HEADQUARTERS	2014 OBLIGATIONS
1	Mission Essential Personnel LLC	Columbus, Ohio	$258,253
2	Alvarez and Associates LLC	Tysons Corner, Va.	$235,304
3	MicroTechnologies LLC	Vienna, Va.	$226,096
4	Thundercat Technology LLC	Reston, Va.	$223,222
5	Four Points Technology LLC	Chantilly, Va.	$165,283
6	COLSA Corp.	Huntsville, Ala.	$143,387
7	Three Wire Systems LLC	Falls Church, Va.	$116,585
8	By Light Professional IT Services Inc.	Arlington, Va.	$115,374
9	Defense Engineering Inc.	Alexandria, Va.	$94,128
10	ICI Services Corp.	Virginia Beach, Va.	$92,102
11	Knight Point Systems LLC	Reston, Va.	$84,530
12	OBXtek Inc.	Tysons Corner, Va.	$82,215
13	7 Delta Inc.	Columbia, Md.	$81,585
14	Technatomy Corp.	Fairfax, Va.	$80,965
15	Armed Forces Services Corp.	Arlington, Va.	$80,702
16	FedStore Corp.	Rockville, Md.	$74,988
17	Harding Security Associates Inc.	McLean, Va.	$71,979
18	Military Personnel Services Corp.	Falls Church, Va.	$71,076
19	Veterans Enterprise Technology Solutions Inc.	Clarksville, Va.	$58,441
20	LongView-FedConsulting Joint Venture LLC	Rockville, Md.	$57,851

Top 20 woman-owned companies

The 20 top-selling companies owned by women did an aggregate government business of $2.6 billion in fiscal 2014. And that's just prime contracts; the total does not include subcontracting work. The dollar amounts in the chart are in thousands.

SOURCE: FEDERAL PROCUREMENT DATA SYSTEM

RANK	COMPANY	HEADQUARTERS	2014 OBLIGATIONS
1	Sierra Nevada Corp.	Sparks, Nev.	$571,743
2	ActioNet Inc.	Vienna, Va.	$285,810
3	FCN Inc.	Rockville, Md.	$242,841
4	AASKI Technology Inc	Ocean, N.J.	$176,986
5	Blue Tech Inc.	San Diego	$171,415
6	Four LLC	Centreville, Va.	$120,894
7	Sterling Computers Corp.	Dakota Dunes, S.D.	$102,245
8	CounterTrade Products Inc.	Arvada, Colo.	$89,178
9	FCI Federal Inc.	Ashburn, Va.	$88,274
10	Science Systems and Applications Inc.	Lanham, Md.	$87,099
11	Gryphon Technologies LC	Washington, D.C.	$83,435
12	Medical Science and Computing Inc.	Rockville, Md.	$82,413
13	Global Tech Inc.	Arlington, Va.	$62,389
14	JBS International Inc.	North Bethesda, Md.	$59,824
15	Manufacturing Techniques Inc.	Kilmarnock, Va.	$59,747
16	AI Signal Research Inc.	Huntsville, Ala.	$57,882
17	System Studies and Simulation Inc.	Huntsville, Ala.	$56,694
18	Dynamic Systems Inc.	El Segundo, Calif.	$53,738
19	CSSI Inc.	Washington, D.C.	$49,982
20	Transource Services Corp.	Phoenix	$48,741

Top 20 minority-owned companies

The 20 top-selling companies owned by minorities did an aggregate government business of $3.8 billion in fiscal 2014. And that's just prime contracts; the total does not include subcontracting work. The dollar amounts in the chart are in thousands.

SOURCE: FEDERAL PROCUREMENT DATA SYSTEM

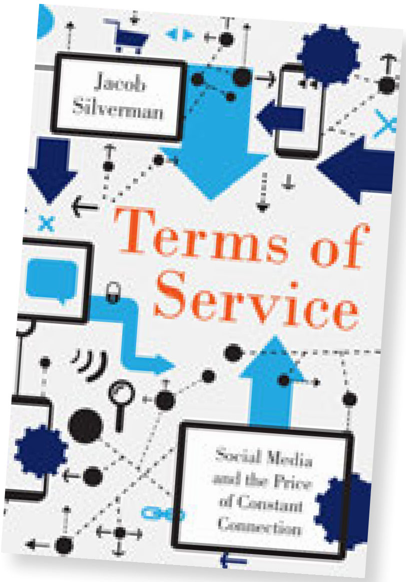
RANK	COMPANY	HEADQUARTERS	2014 OBLIGATIONS
1	World Wide Technology Inc.	Maryland Heights, Mo.	$317,412
2	ActioNet Inc.	Vienna, Va.	$285,810
3	Digital Management Inc.	Bethesda, Md.	$265,684
4	Affigent LLC	Herndon, Va.	$247,281
5	MicroTechnologies LLC	Vienna, Va.	$226,096
6	AASKI Technology Inc.	Ocean, N.J.	$176,986
7	NCS Technologies Inc.	Gainesville, Va.	$175,334
8	Adams Communication and Engineering Technology Inc.	Waldorf, Md.	$174,525
9	STG Inc.	Reston, Va.	$174,454
10	ASRC	Beltsville, Md.	$635,382
11	Colsa Corp.	Huntsville, Ala.	$143,387
12	Tribalco LLC	Bethesda, Md.	$134,001
13	Phacil Inc.	Arlington, Va.	$128,383
14	Four LLC	Centreville, Va.	$120,894
15	Abacus Technology Corp.	Chevy Chase, Md.	$111,686
16	Ace Info Solutions Inc.	Reston, Va.	$101,255
17	Pragmatics Inc.	Reston, Va.	$94,015
18	Cherokee Nation Technology Solutions LLC	Catoosa, Okla.	$90,777
19	Force 3 Inc.	Crofton, Md.	$88,395
20	Science Systems and Applications Inc.	Lanham, Md.	$87,099

2015 Federal List

5 books for your reading list

There are important lessons for federal IT managers in recent fiction and nonfiction books alike

BY FCW STAFF



1. "Terms of Service: Social Media and the Price of Constant Connection"

by Jacob Silverman

Journalist Jacob Silverman applies a corrective critique to the idea that technical progress is inevitably determined by what is possible rather than what might be desirable or useful. He pushes back against the tag of "neo-Luddite," but in a precise sense Silverman's first book embodies some Luddite sensibilities — the idea that there is some logic to smashing up a new machine rather than being rendered disposable or irrelevant.

The book takes a broad look at the development of social media and the corporate ideology that Silverman sees embedded in the growth of connected networks of users sharing their personal information, preferences, desires, thoughts and feelings — not only with their real-life friends and family, but also with a more nebulous array of virtual "contacts" and marketers.

To Silverman, Facebook, Twitter and other networked services — including sharing economy platforms like Uber — are selling "a technocracy of benevolent but total surveillance." His argument is that we have not so much made a decision to buy into this new reality as drifted rudderless into it.

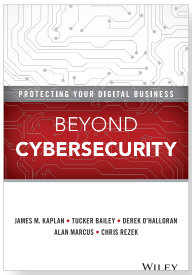
"Terms of Service" can read like a tract at times, but is it also offers a useful perspective as agencies push headlong into "social gov."

2. "Beyond Cybersecurity: Protecting Your Digital Business"

by James M. Kaplan, Tucker Bailey, Derek O'Halloran, Alan Marcus and Chris Rezek

The Andy Ozments of the world might find this to be remedial reading, but "Beyond Cybersecurity" delivers real value for the rest of us.

Written by technologists from McKinsey and Co. and the World Economic Forum, the book targets private-sector executives who aren't giving cybersecurity as much thought as they should. That shortcoming is all too common in government as well, and the authors go deep enough to truly educate without driving away readers who don't make a habit of carefully parsing technology standards.


PROTECTING YOUR DIGITAL BUSINESS
BEYOND CYBERSECURITY
JAMES M. KAPLAN • TUCKER BAILEY • DEREK O'HALLORAN
ALAN MARCUS • CHRIS REZEK
WILEY

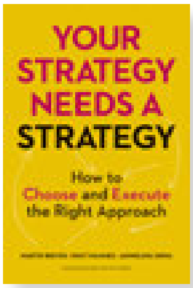
The fundamental message is simple if somewhat distressing: "Cybersecurity, as it is practiced today, is hurting large institutions' ability to derive value from technological innovation and investment," the authors write. And the impact is most keenly felt when it comes to cloud computing and mobile technology.

Over the course of 256 pages, they map the trends that have created this situation and the building blocks required to begin to change it.

3. "Your Strategy Needs a Strategy: How to Choose and Execute the Right Approach"

by Martin Reeves, Knut Haanaes and Janmejaya Sinha

This book takes a meta look at business strategy by exploring five major schools of strategic thinking before proposing the concept of a "strategy palette" in which leaders synthesize elements from each of the offerings.



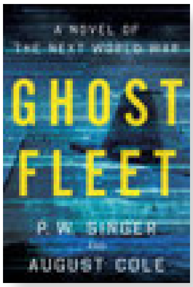
As the authors — all of whom hail from the Boston Consulting Group — break down the pros and cons of myriad business strategies, they sprinkle in accounts of real-world business decisions. Tech giants provide examples of visionary and shaping strategies, while American Express illustrates renewal in action.

In the depths of the 2008 crisis, American Express faced an uncertain future and a cash-strapped environment familiar to many federal leaders. But the company survived and thrived by slashing spending on professional services while maintaining customer service budgets and investing in future growth.

"Your Strategy Needs a Strategy" targets corporate chieftains, not agency CIOs. But the many mini-sagas provide ample inspiration for federal leaders seeking to put their own "strategy palette" to use.

4. "Ghost Fleet: A Novel of the Next World War"

by P.W. Singer and August Cole



This science fiction novel imagines a 21st-century cold war between the United States and Russia that's fought not only on land, air and sea but also online and in outer space — and all with weapons and systems co-developed by the federal government and Silicon Valley.

The book was co-authored by two leading tech experts, P.W. Singer and August Cole, who are on the cutting edge of national security. The science fiction-like trends and technologies in the book are real, according to the authors, and could illustrate the future of a more coherent relationship between Silicon Valley and Washington.

Singer and Cole advocate a closer, more agile partnership between the Defense Department, the federal government and Silicon Valley in developing federal systems and weapons.

5. "There Will Be Cyberwar: How the Move to Network-Centric War Fighting Has Set the Stage for Cyberwar"

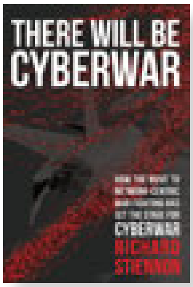
By Richard Stiennon

Richard Stiennon's book opens with an alarming fictional scenario: The Chinese military has used cyber and electronic weapons to disable U.S. naval forces guarding Taiwan. Stiennon scripts a congressional report, dated May 2018, that diagnoses what went wrong. Among the findings is that American spooks were fooled by the intentions of China's alleged state-sponsored hacking of the U.S. industrial base.

"While stealing designs of advanced military systems such as the Joint Strike Fighter and other weapons platforms was evident, it was not clear that the purpose was to discover weaknesses in those systems that the People's Liberation Army could exploit in conflict," he writes.

The implicit warning of this fictional scenario, of course, is that it might not be fiction for long — and that it would be a shame, despite the writing on the wall, to read about it in the dry, post-mortem language of a congressional report.

Stiennon, founder of cybersecurity analysis firm IT-Harvest, has made his case to FCW readers about the cyber vulnerabilities inherent in big Pentagon weapons systems like the F-35 Joint Strike Fighter jet. He expands on that argument in this book and reflects on what is and isn't known about U.S. cyber capabilities.



"We do know, thanks to the numerous breaches and failures of military operations and weapons systems, that the U.S. is woefully unprepared to counter theater cyberwar," he writes.

Although he conjures scenarios that probably aren't far off, Stiennon's prescriptions for bolstering network defenses are focused on present, rather than futuristic, capabilities. He recommends deploying encryption schemes across the battle commands and hardening the Defense Department's IT supply chain.

The book is an enjoyably brisk read that blurs the lines between what's happening in cyberspace and what's on our doorstep. As the author understands, hacking — and defending against it — takes imagination. ■

IT insecurity: Aggressive use of security solutions

To avoid massive data breaches in the future, the government must address its cumbersome acquisition process and misguided IT security practices

BY RICHARD A. SPIRES

In my previous two columns, I described the three primary root causes that have led to the massive data breaches and compromises of core mission IT systems in multiple federal agencies. and provided recommendations for addressing the first cause: lack of IT management best practices.

The remaining two root causes — which are the focus of this column — are misguided IT security practices and a slow and cumbersome acquisition process.

Regarding misguided IT security practices, to the government's credit, there has been a fairly aggressive shift in thinking from the traditional Federal Information Security Management Act reporting approach to continuous monitoring of IT systems and the overall IT environment. I was also pleased to see that Congress passed much-needed reform in the FISMA Modernization Act of 2014, and I hope Congress will work closely with the executive branch to ensure that implementation delivers enhanced security.

Nevertheless, when I look at the current cross-agency priority goals for cybersecurity, I believe the government is still trailing behind current IT security best practices. For example, if you look at the overall objectives, the CAP goals will typically consider objectives of less than 100 percent to be successful, such as 95 percent for automated asset management or 75 percent for strong authentication.

Higher numbers are certainly better than lower ones in those metrics, but we are dealing with adversaries who are advanced and persistent — and who will almost certainly find the holes and exploit them. It is simply a matter of time.

Likewise, the Einstein system can aid agencies in detecting threats, and the promise of Einstein 3 Accelerated is the proactive blocking of malicious traffic. However, Einstein is only helpful if the traffic is actually going through the system. Many agencies have Internet connections that are not monitored by Einstein, and I posit that this is another example of poor IT management.

The government has invested hundreds of millions of dollars in the Einstein program, yet agencies continue to posture and delay implementation. In effect, these approaches have led the federal government to establish a virtual Maginot Line as its key IT security strategy.

Based on the current situation and what I see evolving in the cybersecurity industry, I recommend rethinking how we measure success, with a focus along three lines:

1. Enhance automated protection. There is without a doubt a continuing need to pursue cybersecurity tools to prevent intrusions and, perhaps even more important, detect them quickly when intrusions do occur. The Einstein program identifies and protects against known "signatures" or characteristics of malicious activities, thereby preventing those intrusions. However, more advanced protective capabilities are required to prevent intrusions that the government is not yet aware of, thereby further reducing the government's attack surface.

With enhanced automated protection, network defenders could focus on detecting and remediating only the most sophisticated and potentially

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

dangerous attacks rather than trying to decide which of the seemingly endless alerts to pursue today.

The cybersecurity industry has made great strides in those areas in the past few years, and the government should be using the most advanced tools for prevention and detection that take advantage of threat intelligence from users all over the world.

2. Fully establish and monitor trust. Even with the most advanced prevention tools, the government needs to assume that sophisticated adversaries will gain access. So alternative approaches are needed — particularly ones that rely on creating more trust in online interactions.

The root of all trust is verified identity, and in the online world, multifactor authentication methods are the key to doing that. A plethora of newly available technologies enable multifactor authentication for both internal (government) and external users. And some of the solutions can integrate with antiquated systems. However, the government needs to step back and rethink how it rapidly implements ubiquitous use of multifactor identity authentication.

Even though the root of trust is identity, there is more to the equation. In the physical world, I trust other people because I have high confidence they will act in a manner that I expect. Some of the most damaging data breaches have come from individuals who were properly authenticated and authorized to use systems and access data, but their behavior was not in keeping with what was expected. This is commonly called the insider threat problem.

There are new technologies and capabilities today that can bring in other contexts to assess someone's trustworthiness on a regular basis, such as audit logs or behavioral analysis systems. Those additional factors, beyond those used to assess authenticity, are essential to fully establishing and monitoring trust.

> **When I look at the current cross-agency priority goals for cybersecurity, I believe the government is still trailing behind current IT security best practices.**

3. Focus on protecting the most sensitive information. The government needs to target additional protection of an agency's most sensitive information, whether it is in the form of datasets or documents. Tools and products exist that enable agencies to protect information independent of the likely insecure environment in which they operate.

Agencies should focus on their most valuable information. I recognize that there are limitations because of the antiquated systems in which some of that information resides, but by focusing efforts on the most sensitive information, the government could ensure that only trusted parties would have access to an agency's most sensitive information. That would go a long way toward thwarting additional major and damaging data breaches.

It is difficult to implement state-of-the-art IT cybersecurity solutions if you have no way to rapidly evaluate them and then purchase or license them. The Continuous Diagnostics and Mitigation (CDM) program and Einstein could potentially serve as governmentwide vehicles for that process, but it has taken significant time to put them in place.

I recommend an approach that enables individual agencies to rapidly bring in solutions and try them in a test-bed environment. After thorough testing and based on what works best, agencies should be able to roll security solutions into production. That approach would ideally encompass traditional cybersecurity vendors and new vendors that have little or no government experience. They are an incredible source of technical innovation.

The government is not getting the best solutions through the existing acquisition process. Therefore, I recommend that the Office of Federal Procurement Policy work with the General Services Administration and the Department of Homeland Security to put a more streamlined CDM program in place — one that would enable rapid addition of new capabilities as they become available in the commercial market.

The data breaches at the Office of Personnel Management are terrible for the government and for the millions of us who could be negatively affected in the future. Viewed through the right lens, however, the episode could be the impetus for much-needed and sustained change. And given the need to implement the Federal IT Acquisition Reform Act, the current administration has a golden opportunity to set the correct foundation for success. It is critical to make enough progress in the next 18 months to ensure that leadership commitment to FITARA, FISMA modernization and other needed changes in IT security are sustained into the next administration and Congress.

FCW Index

People

Agencies/Organizations

Advertisers

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

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

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.

1105 PUBLIC SECTOR MEDIA GROUP

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

9 SIGNS YOU'VE BEEN the VICTIM of a BREACH

klossner

- The waiter asks how you could consider that dessert with your medical history.
- Strangers tell you how much better they feel about themselves since they've learned about you.
- When traveling, your hotel bartenders serve you before you order.

- People greet you by your social security number.
- The doctor's office says to come in 15 minutes later because it would be "useless to sign any privacy forms."
- The person on the eliptical next to you says you're pretty relaxed for someone with a mortgage as large as yours.

- A coworker tells you you're not as bad as your personnel file suggests.
- Your children come home crying because the other kids are picking on them about your credit card balance.
- You start receiving birthday cards from China.

The Federal IT Acquisition Summit

October 20, 2015 | Washington Hilton, Washington, DC

Participating Agencies

SEWP V

NITAAC
OMB Authorized GWACs for IT Acquisition

Featured Speakers From

ARMY CHESS
COMPUTER HARDWARE, ENTERPRISE SOFTWARE AND SOLUTIONS

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

TRAINING OPPORTUNITIES :

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

FEATURED PANEL SESSIONS:

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

Free for Government & Military Attendees

FCW GCN Washington Technology DEFENSESYSTEMS Federal SOUP

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

http://FCW.com/FIAS

IBM Hybrid Cloud:

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

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

Smarter clouds are made with IBM.

IBM and Smarter Planet and their logos, ibm.com and made with IBM are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. See current list at ibm.com/trademark. ©International Business Machines Corp. 2015.