FCW

THE BUSINESS OF FEDERAL TECHNOLOGY

BUILDING BETTER OVERSIGHT?

FITARA changes the rules, and Congress has new chairmen in charge.

But will it make any difference?

PAGE 18

+

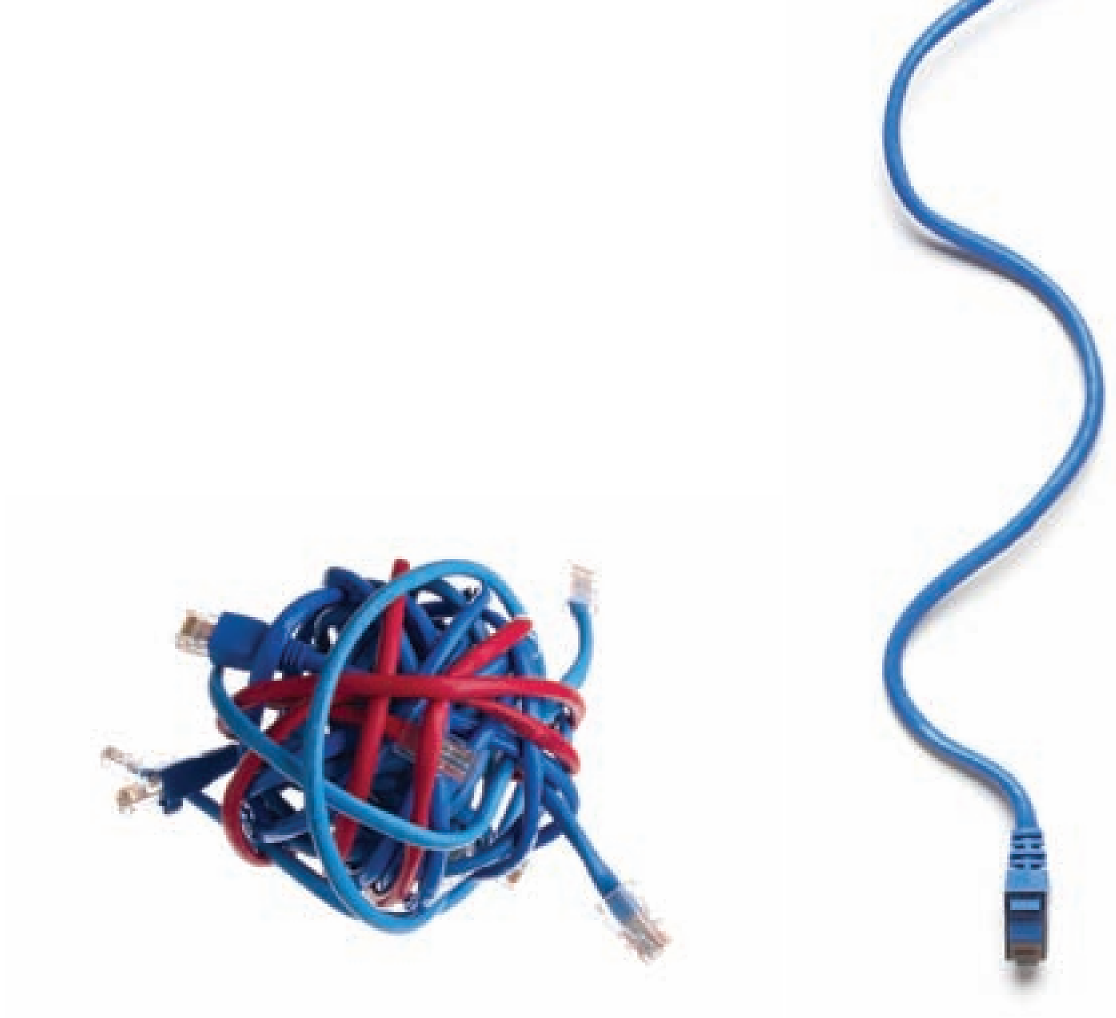
Innovations in acquisition

PAGE 31

Suicide prevention through better data

PAGE 23

FEBRUARY 2015 • VOLUME 29 NUMBER 2



64.4 was the government's score on the 2014 American Customer Satisfaction Index — its lowest ever

Could this be the year for data-breach legislation?

For Republicans in Congress looking for areas of bipartisan cooperation, data-breach notification could prove to be low-hanging fruit. There is widespread support for creating a national standard as an alternative to the 47 state laws that currently govern data breaches, although there are some key details to be ironed out.

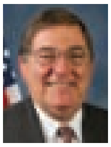
"A single requirement across the states would give companies some confidence that their methods are sound in handling electronic data, an inherently interstate activity," Rep. Michael Burgess (R-Texas), chairman of the Energy and Commerce Committee's Commerce, Manufacturing and Trade Subcommittee, said at a Jan. 27 hearing.

The basics of such legislation would include a standard definition of what constitutes a breach, whether a breach has the potential to cause harm and a minimum time period before consumers are notified. Then there are the more controversial questions of whether companies that notify consumers about data breaches would be indemnified against lawsuits and whether a federal standard would preempt state laws or simply augment them.

If Congress does get into the data-breach business, some federal agency would be charged with overseeing the policy. The Federal Trade Commission is one possible choice. In 2012, the FTC sued Wyndham Hotels and Resorts over a data breach, arguing that the company had failed to take adequate steps to protect customer data. That suit is working its way through appeals, but so far the FTC's jurisdiction over data breaches as a consumer protection matter has been upheld. FTC attorney Lesley Fair wrote in a blog post that so far the agency has settled 53 cases, and that number would "likely go up."

Although a handful of states have relatively minimal or no data-breach reporting requirements, others — including California and Connecticut — demand that their residents be notified within five days of a hack. National firms often adopt the most stringent state standard as a baseline for doing business, a fact not lost on those Democrats who seek tougher federal rules.

"While I clearly believe the federal government should have a role in data breach [reporting requirements]...I also believe that there have been many important protections that are at the state level that we don't want to eliminate when we do federal legislation," said Rep. Jan Schakowsky (D-Ill.), the subcommittee's ranking member.



A single requirement across the states would give companies some confidence that their methods are sound in handling electronic data.

— REP. MICHAEL BURGESS

Some Democrats on the panel cautioned against preempting state laws, but Rep. Peter Welch (D-Vt.) said he has "been persuaded that if we can get the right standard, this is one of those situations where it really makes sense to have preemption."

Welch is working on a bill with Rep. Marsha Blackburn (R-Tenn.), vice chairwoman of the Energy and Commerce Committee. An Obama administration proposal would set a single 30-day national standard for notification that would supersede state laws.

— *Adam Mazmanian*

FCW CALENDAR

3/3 Acquisition Office of Federal Procurement Policy Administrator Anne Rung is among the many invited speakers at Acquisition Excellence 2015. Washington, D.C.
is.gd/FCW_ae2015

3/12 Insider threats This FCW conference will focus on the deployment of analytical tools and training programs to minimize insider threats.
Washington, D.C.
fcw.com/InsiderThreatDetection

3/26 Federal 100 Save the date! The 26th annual Federal 100 Awards Gala will honor 2014's top achievers in the federal IT community.
Washington, D.C.
fcw.com/fed100

BURGESS.HOUSE.GOV

Contents

TRENDING

DEPARTMENTS

Making a Success of CDM

If there is one thing government technology professionals know, it's that no system—no matter how many tools and staff are dedicated to it—is fully secure. Agencies have spent the last two decades working hard to keep up with the changing nature and breadth of cyber-threats, but most acknowledge that it's time for a new approach.

Enter CDM. The Continuous Diagnostics & Mitigation method encourages agencies to approach cybersecurity in a more holistic, automated, measurable, and continuous way. Based on standards from NIST, CDM focuses on providing agencies with comprehensive visibility into assets and activities across the network, the ability to measure all risks, and full accountability of staff to follow plans and policies.

CDM is a deliberate attempt by government to move from the reporting rules of FISMA and the progress made through continuous monitoring to more comprehensive, effective security monitoring and mitigation. Once fully rolled out, all federal agencies will have the tools and processes to protect their networks and infrastructure from cyber-threats.

Even Congress has stressed the importance of CDM as a priority throughout government. The DHS 2015 appropriations bill specifies that part of the $140 billion set aside for the Federal Network Security program should be used "to provide adequate, risk-based and cost-effective cybersecurity to address escalating and rapidly evolving threats to information security, including the acquisition and operation of a continuous monitoring and diagnostics program".

The CDM program will be implemented in three phases. In the first phase, currently in progress, agencies are tasked with satisfying the first four of 15 functional areas: hardware and software asset management, vulnerability management, and configuration-setting compliance. During this phase, agency networks must be scanned at least once every 72 hours for potential attacks or vulnerabilities. Agencies also should install or update their sensors and start performing automated searches for potential vulnerabilities.

CDM makes the difference

Whether it's a security risk to the network, applications, data, an Internet-connected sensor, mobile device with access to network resources or a cloud-based system, CDM controls can make a big difference. They do so by providing a holistic view across the enterprise so you can understand the assets you have, the role of those assets in your organization, and where those risks are arising.

"With that information, you can quickly evaluate potential negative impacts to the organization and make sure you resolve and remediate the most potentially damaging risks first," says Robert Potter, Vice President, US Federal at security, storage and systems management solutions provider Symantec.

The key underlying concept of CDM is to fix the worst problems first, which puts the focus squarely on risk prioritization and management. That means expanding the risk management framework to fully understand critical applications, data sets, personnel and key vulnerabilities. CDM takes that up a notch with real-time monitoring, automation and big data analysis, which allows IT staff to access

From Awareness to Action

CDM isn't a concept that sprouted overnight. Instead, it's the culmination of decades of progress in cybersecurity awareness.

2002	2007	2007	2008	2010
Federal Information Security Management Act (FISMA) is enacted	Department of State initiates the Cyber Security Incident Program (CSIP)	NIST begins working on SCAP (Security Content Automation Protocol)	Department of State launches iPost for automated scanning and continuous monitoring; it is so successful that other agencies begin to take note	OMB issues mandate on continuous monitoring

information and make decisions in real-time.

"If you have visibility into vulnerabilities, patches and activities on the network in real time and can aggregate that information and display it in real time, you can understand the health of the enterprise from a risk management perspective," said Robert Osborn, Chief Technology Officer for Federal at ServiceNow, an enterprise IT cloud company.

Managing risk is the key to successful CDM. Being able to quickly pinpoint behavior or activity inside the network that is inconsistent with your policies or the behavior of the people or devices running on your network is more than half the battle in cybersecurity.

While CDM is just getting off the ground in many agencies, those that have implemented it have already reaped big benefits. The State Department, which led the charge several years ago with the first CDM-type program, reported reductions of up to 90 percent in security risk. A SANS Institute study published in August 2014 found that nearly half experienced better security as a result of the CDM controls.

CDM also has proven to improve security decision-making significantly. A recent MeriTalk study found that at least half of respondents cited improved risk assessment and acceptance, improved decision-making on when to share data with other networks, and better awareness of consequences resulting from the current state of security.

Making sense of it all

A successful CDM approach requires paying full attention to people, processes and technology. In the technology realm, it involves upgrading or adding to the security capabilities many agencies already have in place. Some of the most important areas are:

Automation: Automation is a critical component of CDM because some threats require response within milliseconds—much faster than a human could respond. By automating as many of the known threats as

CDM: Step by Step

The Continuous Diagnostics and Mitigation program covers 15 diagnostic capabilities, which will be rolled out in three phases:

Phase 1: Endpoint integrity

- Hardware asset management
- Software asset management
- Configuration settings management
- Vulnerability management

Phase 2: Least privilege and infrastructure integrity

- Access control management (trust in people granted access)
- Security-related behavior management
- Credentials and authentication management
- Privileges
- Boundary protection (network, physical, virtual)

Phase 3: Boundary protection and event management for managing the security lifecycle

- Plan for events
- Respond to events
- Generic audit/monitoring
- Document requirements, policy, etc.
- Quality management
- Risk management

Source: Department of Homeland Security

CDM promises to take cyber-protection to new heights.

2011	2012	2013	2014	FY2014
NIST publishes SP 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations	OMB identifies continuous monitoring of federal IT networks as one of 14 Cross-Agency Priority goals	OMB issues memo requiring continuous monitoring of security by the end of FY2017	NIST publishes SP 800-53, Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations	Agencies required to finalize CDM strategies

possible, humans only have to be involved when the activity is unexpected. Automation also is the only practical way to meet the CDM requirement of assessing all network assets every 72 hours. "The challenge of doing something 10 times a month instead of once a month when these agencies are already resource-constrained is completely overwhelming for solutions that don't have a high degree of automation," says Keren Cummins, Director, Federal Sales at Tripwire, a provider of risk-based security, compliance and vulnerability management solutions.

Continuous, real-time monitoring: A wide range of research shows that once an advanced persistent threat enters a network, it can quickly compromise dozens of machines, moving laterally. That makes continuous monitoring critical; by spotting breaches quickly, you have a better chance of containing and eradicating them. Most agencies already stress the importance of continuous monitoring. For example, the Defense Department relies on its Continuous Monitoring and Risk Scoring (CMRS) system to meet this goal.

Big Data analytics: Data today comes from many sources—mobile devices, sensors, email and texts, images, phone logs and more. It's critical to examine each and every piece of data interacting with the network to ensure security. With big data analytics, agencies can gain full visibility into everything in the IT infrastructure, allowing them to quickly connect the dots across different systems and applications. Doing that in real-time translates into a powerful CDM capability.

"It doesn't matter the device, or whether the resource is cloud, physical or virtual; if confidential data is involved, it represents a potential risk to the organization and must be monitored," said Joe Goldberg, Security Evangelist at Splunk, a software platform provider for real-time operational intelligence.

Ensuring that all of these capabilities are included and work together—and as required—is a difficult task. The best way to start is with a verified, tested cybersecurity framework. NIST has provided the baseline with its 800 series publications, which outline the technical controls, best practices and processes agencies need, focusing on risk management and continuous monitoring controls required to handle both advanced persistent threats and insider threats. In developing the framework, NIST included input from the public and private sector as well as SANS Institute, which contributed the 20 critical security controls.

The framework is technology-agnostic, giving agencies the freedom to choose which technologies to employ to meet the framework's goals.

The NIST framework itself is a base on which agencies can build their own CDM programs. The Defense Department has chosen to include its Continuous Monitoring and Risk Scoring (CMRS) system as part of the framework, while DHS has chosen to layer its Continuous Diagnostics and Mitigation program on top of the framework. DHS is the lead agency for the federal government on the CDM effort.

A look ahead

Once agencies are finished implementing Phase I, they must turn their attention to the next two phases. Phase II addresses issues around managing people, from training and credentials to account access and privileges. Phase III focuses on event management and boundary protection, employing technology such as forensics analysis and data loss prevention.

Along the way, threats will continue to change and technologies will continue to mature. One of the fastest-growing vulnerabilities is in the area of the Internet of Things, which involves the data sent from a variety of sensors through networks.

"Think about a military base and all of the people who live on it. If they have sensors for temperature control, refrigerators, televisions and many other things on the military network, you are potentially increasing the IP listing of that base by 30 fold," says Potter. "I don't think we have even begun to see the vast increase in sensors and the risks they could cause. That's something both agencies and vendors have to plan for now."

Strengthening the Security Posture of Government Networks

Carahsoft is pleased to support the government's CDM and cybersecurity initiatives through its partnership with a broad range of technology manufacturers, resellers and system integrators.

Akamai
Cloud Security Solutions

AlertEnterprise!
Security Convergence Solutions

CORE SECURITY
Intelligent Network Visibility Platform

CYBERARK
Privileged Account Controls & Monitoring

EMC²
Secure On-Premise Storage Infrastructure

ExtraHop
Wire Data Analytics Platform for Continuous Monitoring

f5
Application Security Testing & Management

FireEye
Cybersecurity and Malware Protection

Gigamon
Intelligent Network Visibility Platform

hp
Integrated Enterprise Security Solutions

HYTRUST Cloud Under Control
Virtualization Security, Compliance & Control

IMPERVA
Data Center Security Solutions

Infoblox CONTROL YOUR NETWORK
Automated Network Control

invincea
Endpoint Security Solution

MarkLogic
NoSQL Platform for Cyber Defense & Analysis

mongoDB
Cross-Platform Database for Big Data Analytics

pentaho
Real-Time Predictive Analytics

redhat
SE Secure Linux

RSA
Security, Risk & Compliance Management

SafeNet The Foundation of Internet Security
Data Protection & Software Monetization

servicenow
Cloud Infrastructure Security Platform

splunk>
Operational Intelligence Software

ssh COMMUNICATIONS SECURITY
Data-in-Transit Security Solutions

Symantec.
Monitoring, Remediation & Compliance Reporting

tripwire
Security Configuration & Vulnerability Management

Trustwave
DbProtect Database Security & Audit Logging

VENAFI
Next-Generation Trust Protection

vmware
Network Virtualization & Security Platform

Vormetric Data Security Simplified
Enterprise Encryption & Key Management

Xceedium
Privileged Identity Management Solutions

CDM System Integrator Partners

Booz Allen Hamilton | CGI Federal | Computer Sciences Corporation | Engility Corp. | General Dynamics Information Technology | HP Enterprise Services
IBM | Knowledge Consulting Group | Kratos | Leidos | Lockheed Martin | ManTech | MicroTech | Northrop Grumman | SRA International | Technica

CDM@carahsoft.com   carahsoft.   carahsoft.com/cdm

FCW
THE BUSINESS OF FEDERAL TECHNOLOGY

Editor-in-Chief Troy K. Schneider
Executive Editor John Bicknell
Managing Editor Terri J. Huck
Staff Writers Colby Hochmuth, Sean Lyngaas, Adam Mazmanian, Mark Rockwell
Editorial Fellow Jonathan Lutton

Vice President, Art and Brand Design Scott Shultz
Creative Director Jeff Langkau
Assistant Art Director Dragutin Cvijanovic
Senior Web Designer Martin Peace
Director, Print Production David Seymour
Print Production Coordinator Lee Alexander
Chief Revenue Officer Dan LaBianca

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**
Director of Sales **David Tucker**
Senior Sales Account Executive **Jean Dellarobba**
Media Consultants **Ted Chase, Bill Cooper, Matt Lally, Mary Martin, Mary Keenan**
Event Sponsorships **Alyce Morrison, Kharry Wolinsky**

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

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

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

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

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

FederalSoup and Washington Technology
General Manager **Kristi Dougherty**

OTHER PSMG BRANDS

Defense Systems
Editor-in-Chief **Kevin McCaney**

GCN
Editor-in-Chief **Paul McCloskey**
Executive Editor **Susan Miller**

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

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
For questions on subscriptions or circulation, contact Annette Levee,
(512) 301-2632 (phone); (512) 301-3361 (fax);
alevee@1105media.com

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

458 controls are included in the draft FedRAMP high-impact baseline

DHA readies $10 billion IT contract

The Defense Health Agency is in the final stages of developing a solicitation for an indefinite-delivery, indefinite-quantity IT services contract worth as much as $10 billion over five years.

The agency will hold its last industry day for the Health Information Technology Services IDIQ contract on Feb. 17, said Col. Scott Svabek, DHA's acting director of procurement, during a Jan. 22 panel discussion on federal procurement and small business sponsored by AFCEA DC. The final solicitation is expected in the third quarter of 2015.

The contract will be a follow-on to an IT support contract called Systems Integration, Design, Development, Operations and Maintenance Services, which expires at the end of 2015.

DHA is responsible for managing enterprisewide support of DOD's medical mission, including the establishment of shared services and the introduction of common business and clinical processes across the Military Health System.

Svabek said he turned to the broad IDIQ contract option rather than an existing governmentwide acquisition contract because of the fees GWACs charge and the fact that he would have to cede control to other agencies whose goals might not match his own.

"I wanted to bring it back in house," he said, noting that DHA spent $14 million in usage fees last year. "It may be arrogance on my part, but I don't want to be held to others' restrictions and protests."

Other panel members said small companies' success in seeking new contracts hinges on their ability to talk specifics with agencies not only about their products but about how those products can be applied to agencies' specific projects.

Mitchell Ross, director of the Acquisition and Grants Office at the National Oceanic and Atmospheric Administration, said small-business contractors "have to provide something of interest" in response to requests for information on projects, instead of supplying canned marketing materials that provide few if any specifics on how their firms' technology could be of use.

Kathleen Gregory, procurement analyst and small-business specialist at the Immigration and Customs Enforcement agency, agreed.

"Everyone does IT," she said. "Match our mission."

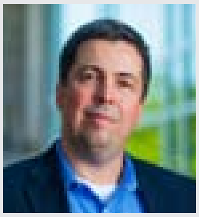
— Mark Rockwell

EDITOR'S NOTE

Should you really care about Congress?

Federal employees who feel like a punching bag when it comes to public opinion can at least be assured of one thing: Americans like Congress even less.

A January Pew Research Center poll, for example, asked about eight well-known agencies, and even the Internal Revenue Service — not exactly known for making citizens' lives easier — was viewed favorably almost as often (45 percent) as unfavorably (48 percent).



When Pew researchers asked the same question about Congress in December, 71 percent had an unfavorable view of the legislative branch. And in a subsequent survey, 71 percent said they expected the two parties to "bicker and oppose one another" even more than usual in 2015.

The dismal approval ratings make sense: Congress hasn't passed a budget or moved real appropriations in years, and "oversight" is too often code for political theater and partisan witness-grilling. For those who need those appropriations and are subject to said oversight, it's all too easy to caricature Congress (as we do on Page 11) as something between a nuisance and a medieval inquisitor.

Agency leaders, however, know that working with Congress is not optional and that the real picture is much more nuanced.

That's why we devoted so much of this issue to IT's intersection with Capitol Hill. The new laws *do* matter — and so does the manner in which they're implemented. Federal IT is also one of the rare areas where partisanship can be muted, allowing real work to still get done.

And most important, there are individuals on the Hill — just as there are throughout federal IT — who care deeply about using technology to make government work better. (Four of this year's Federal 100 winners, in fact, hail from Congress. You can find the full list at FCW.com/fed100.) Those partners, and the possible common ground, are worth the attention.

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

Mobile security: The device decision

Agencies are standardizing on fewer mobile platforms, but device security remains a multilayered challenge

BY CAROLYN DUFFY MARSAN

As agencies grapple with the rapidly evolving universe of mobile devices and applications, they are scrambling to find faster and better ways to determine which devices they will allow on their networks and how best to secure the devices they acquire.

From the Pentagon to the FBI to the Department of Agriculture, agencies are getting newer mobile technology into the hands of their users faster by streamlining acquisition processes and standardizing on fewer mobile platforms. After the devices are selected, agencies are bolting on extra security through containerization technology, mobile device management platforms and application security services.

There is still a ways to go, however, before federal employees have state-of-the-art and secure mobile devices at their disposal.

"We've always seen mobile technology change, but it's happening faster than it ever did before. Just think about the fact that the iPad wasn't even out five years ago," explained Tom Suder, president of Mobilegov, a Washington, D.C., consultancy. "There is a real business case for agencies to solve the mobility problem.... Agencies are trying, but it's still taking too long."

Part of the challenge in mobile security is that the devices themselves are so much more personalized and context-driven than PCs, said Bryan Coapstick, director of mobile innovation for HP Enterprise Services U.S. Public Sector Business.

DISA's short list

Just a handful of devices have been approved under the DOD Mobility Program Management Office's new streamlined process. Approved devices include:

Apple iOS (8.x)

Phones: iPhone 4s, iPhone 5, iPhone 5s, iPhone 6, iPhone 6 Plus

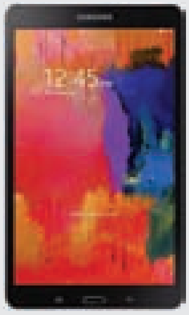
Tablets: iPad mini 2, iPad mini 3, iPad mini 4, iPad mini-R, iPad Air

Android OS (4.4)

Phones: Samsung Galaxy S4, Samsung Galaxy S5, Samsung Galaxy Note 3, Samsung Galaxy Note 4, Samsung Galaxy Note Edge, Samsung Galaxy Alpha

Tablets: Samsung Note 10.1 2014 Edition, Samsung Note Pro 12.2, Samsung Galaxy Tab S 10.5 LTE, Samsung Galaxy Tab S 8.4 LTE, Samsung Galaxy Tab Active

(All with Knox)



Source: Defense Information Systems Agency

"These are different devices and we need to take a fundamentally different approach to security," Coapstick said. "Trust is fundamentally changed with mobile. It's not just can we trust the device, but can we trust the data on the device. These are some of the questions that are becoming part of the dialogue."

Narrowing the options

Many agencies have streamlined the process of approving and purchasing mobile devices so that they are able to put up-to-date technology in the hands of their users.

For example, the Defense Department's Defense Information Services Agency is now publishing Security Requirement Guides for smartphones and tablets, and then letting manufacturers develop a Security Technical Implementation Guide (STIG) for their device as they develop it, submitting a self-certification back to DISA for final approval. Previously, DISA would develop its own STIG for each newly released product, which often took so long that devices were obsolete by the time they were approved for use on DOD networks.

"The problem you had before was demonstrated by the Dell Streak," Suder explained, referring to the tablet that was the first Android device approved by DISA back in 2011. "It took so long to get the Dell Streak certified that by the time it was certified, a week later Dell discontinued the Streak."

With its new streamlined process, DISA has approved several mobile phones, including various Apple iPhones and Samsung Galaxy devices with the Knox security add-on. DISA also has approved five Apple iPad tablets and five Samsung tablets. Two operating systems have been approved by DOD's Mobile Program Management Office: Apple iOS and Android.

When DISA switched to having vendors write their own STIG, "the turnaround time went from a year to more like three months," said Adam Salerno, manager of federal accounts with Veris Group. "It's definitely a boon to getting more devices out there."

Salerno said the old DISA approach was a "very thorough but very time-consuming process. All the work was probably going to one program office that had very limited resources…. They were able to offload that onto the vendor to do a lot of heavy lifting."

DISA's goal is to have mobile devices approved for use on DOD networks at the same time that these devices are brought to the commercial marketplace.

Suder said DISA's new device approval process "is definitely better over the last 18 months or so. But it is not all the way there. They still need to do a better job with mobile device management."

And it's important for federal agencies to deploy mobile platforms rapidly and not allow themselves to get two or three generations behind.

"With cybersecurity these days and zero day vulnerabilities…it actually behooves you to get on the newest stuff as soon as possible," Salerno said. And because commercial providers often aren't willing or able to provide agencies with older, already-approved devices on a large scale, "you are almost forced to make it work on the newer stuff."

The situation at DISA — which declares itself device agnostic, but has largely settled on Apple and Samsung for mobile — reflects a similar trend across government.

"We are seeing strides [toward standardization], and we see many more Samsung deployments than any other Android because of that," Salerno explained. "But even then, those devices ship with different versions and apps depending on the carrier."

The FBI, for example, is standardizing on Samsung Galaxy devices with its Knox security add-on. In July 2014, the FBI purchased 26,500 licenses for Samsung's Knox 2.0 software, which allows users to seamlessly switch from work to personal modes on their smartphones. Samsung is replacing aging BlackBerry smartphones at the law enforcement agency.

David Rubin, the mobility lead for the Justice Department, said in January that the FBI has nearly 30,000 of Samsung's Android-based devices deployed at 56 field offices. He told the crowd at an AFCEA event that the FBI used the Knox containerization technology to profile applications and to encrypt agency communications. The FBI uses the Samsung devices for unclassified communications only, but would like to eventually connect to classified networks using these devices, Rubin said.

One reason that the FBI replaced its BlackBerry devices with Samsung is that it wanted a more commonly used device in the hands of its employees to provide anonymity on the job.

"Walking around with a BlackBerry almost pigeonholes you as working for the U.S. government," Suder said. "Overseas, it's a telling sign. It's almost a physical security issue."

Management platforms proliferate

Device selection alone does not guarantee security, of course. The applications loaded onto the device are also a critical concern. (One recent study of mobile devices that connected to the networks of a major federal agency found that 29 percent of the devices had encountered mobile malware.) More agencies are therefore deploy-

Agencies need to really think about how these devices are being used and how they are employed in the transaction because that's what it's really about. **Users want to access the right information right now and right here.**

— **Bryan Coapstick, HP Enterprise Services**

ing MDM platforms to provide asset management and security functionality across a variety of mobile devices.

Four MDM vendors are at the forefront in the federal market: MobileIron, AirWatch, Fiberlink and XenMobile. AirWatch is owned by VMware, Fiberlink is owned by IBM, and XenMobile is owned by Citrix.

MDM platforms are helping agencies get their mobile devices under control, Salerno said. "We've now moved into applications as the main risk factor. We're looking at how those applications are getting to those devices."

For example, DISA chose MobileIron as its MDM platform and secure mobile app store. A DISA official told FCW that 6,700 unclassified mobile devices were currently under management.

Suder said DISA's rollout of MDM is a step in the right direction but is taking longer than anticipated.

"DISA is having trouble getting devices certified for the MDM," Suder said, adding that other military agencies are looking at getting MDM platforms of their own. "The Navy is looking at an MDM of their own. The Air Force is kicking the tires on MDM. The Marine Corps is looking to go through a carrier."

Coapstick said the DISA MDM deployment is behind schedule because "they are starting to see some of the challenges with mobility and how they do things from a strategy, policy and implementation perspective.... For any large organization, it becomes a big change management problem."

And Salerno noted that, while "most of the MDMs, and in turn a lot of the management applications, are now cross-platform…a homogenous environment is going to work a little more smoothly across the board."

USDA's National Agricultural Statistics Service, for example, has standardized on iPads and MobileIron. Approximately 3,000 NASS employees use iPads to survey and report on agricultural data nationwide.

Last year, USDA selected MobileIron to help secure its mobile devices, data and apps. As an MDM solution, MobileIron provides secure email, automatic device configuration, certificate-based security and remote wipe for lost or stolen devices. The software separates business and personal data, and allows an enterprise to wipe all corporate data off the device when an employee leaves.

On the horizon: App security

The mobile security debate is expected to shift focus in 2015 and beyond from devices to applications. This shift comes at a time when mobile app development is skyrocketing; IDC predicts that enterprises will develop twice as many mobile apps in 2015 as a year earlier.

One sign of this issue's importance is that the National Institute of Standards and Technology has drafted guidelines to help agencies test for vulnerabilities in mobile applications.

Agencies are starting to consider mobile app security with targeted products from such vendors as Barracuda, Appthority and Lookout as well as mobile application management features on MDM platforms. As Lookout's Vice President for Federal Systems Bob Stevens told FCW, "MDM is really good at policy and policy enforcement. But who informs those policies?"

Coapstick said that the biggest challenge in mobile security is that mobile apps are built using a different paradigm than applications built for PCs.

"Mobility isn't always about the consumption of data in a tablet factor. It's about providing data that relates to a location or what I'm doing, what we like to call hyper contextual. It's a fundamentally different experience," Coapstick said.

"It's going to take a security posture and a paradigm shift to think beyond the mobile device," Coapstick said. "Agencies need to really think about how these devices are being used and how they are employed in the transaction because that's what it's really about. Users want to access the right information right now and right here."

Mobility experts say agencies need to think more about the security of data and apps on devices than worrying about the devices themselves.

"App security is the next frontier," Suder said. "An agency has to develop some kind of risk profile of what they can accept in their apps. They can't lock down everything, or nobody can do their job." ■

SAMSUNG
My Workspace
Team Briefing
Travel Schedule Changed
Q4 Dinner
Reimbursement Guidelines
IT upgrade options
Management Survey
Samsung Knox
GALAXY Note 4
GALAXY Tab Active
GALAXY S5

26 data centers have been closed by Lawrence Livermore National Lab, saving nearly $350,000 annually

IG details flaws in HealthCare.gov IT acquisition

It's no secret that HealthCare.gov failed to work as advertised when it launched in October 2013. The site's high-profile flop is cited as part of the recruiting pitch for the government's high-tech rescue squad, the U.S. Digital Service.

Behind the over-stressed, crash-prone website was a rushed procurement strategy that failed to yield meaningful competition, faulty and undocumented acquisition planning, lack of control over and coordination of contractors, and contracting methods that increased the risk of cost overruns, according to a new report from the Department of Health and Human Services Office of Inspector General.

CMS Administrator Marilyn Tavenner concurred with the IG's report on the botched HealthCare.gov acquisition.

AP IMAGES

The result wasn't merely a buggy website, according to the report. Cost estimates on the six largest contracts associated with HealthCare.gov were pegged at $464 million when the awards were made beginning in 2011. By early 2014, the contract value had nearly doubled to $824 million.

One particularly ill-fated move was the decision to conduct the procurement under an existing contract used by the Centers for Medicare and Medicaid Services to acquire IT systems.

The 16 companies on CMS' Enterprise System Development contract were the only firms allowed to bid on developing the five major components of HealthCare.gov. Only one firm — CGI Federal — submitted a qualified bid for the Federally Facilitated Marketplace (FFM), HealthCare.gov's center for insurance plan comparison and shopping. The FFM proved to be particularly problematic at launch and required extensive redesign. During the race to repair the site, CGI Federal was put under the supervision of a lead contractor before being taken off the project in January 2014.

Two other key contracts — for the $68 million Data Services Hub that routed eligibility queries to government databases and the $109 million identity-proofing service — attracted only two qualified bids each.

The IG report states that contracting officials did not consult government databases on vendors' past performance when awarding the FFM and Data Services Hub contracts. And just two of the six biggest contracts got a second look from the CMS Contract Review Board before awards were made.

CMS risked taking on additional costs by using cost-reimbursement for some of the largest contracts. Furthermore, the justification for that decision was limited to "general statements that fixed-price contracts could not be used because costs could not be defined accurately due to uncertainties with the required work," the report states.

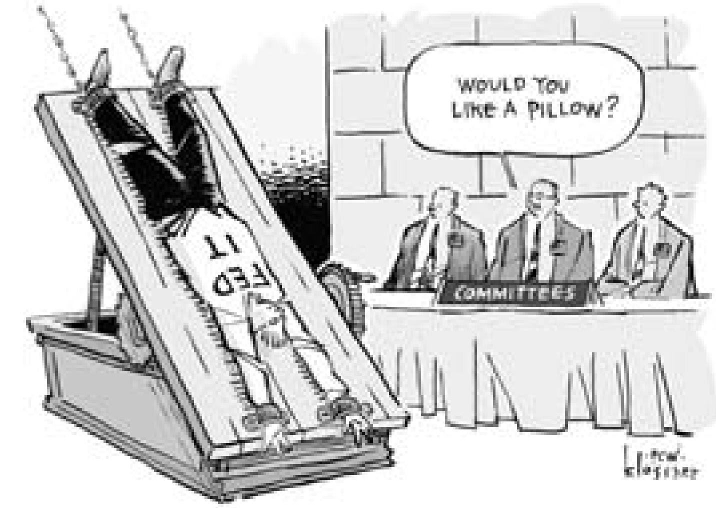
The report is also critical of the decision not to choose a lead integrator for the biggest HealthCare.gov contracts, considering the size and complexity of the project. Former CMS CIO Tony Trenkle told the IG's office that CGI Federal was perceived to be the lead contractor, but the report states that "the company did not have the same understanding of its role."

In reply to comments filed in November 2014, when CMS officials reviewed the report, CMS Administrator Marilyn Tavenner and HHS Chief Financial Officer Ellen Murray concurred with the auditors' conclusions. "CMS is taking the HHS OIG's findings and recommendations seriously and is using the report as an opportunity to make needed change," they wrote.

By most accounts, the HealthCare.gov site is functioning smoothly as the second open-enrollment period winds down. Accenture, the contractor tapped in January 2014 to take over the FFM, recently won a five-year, $563 million contract to run the FFM through 2020.

— Adam Mazmanian

INK TANK



The New Congress

SNAPSHOT

CONVERGED INFRASTRUCTURE

Making the Most of Convergence

Other Converged Infrastructure Report Articles:

- When Moving to a Converged Infrastructure Makes Sense
- HyperConvergence: The Next Wave of Convergence
- The Business Case for Converged Infrastructure
- The Data Center of the Future

FULL REPORT ONLINE

Go to FCW.com/2015CONVERGED INFRASTRUCTURE

Converged infrastructures can help agencies simplify and optimize the IT infrastructure, deliver IT services more quickly and efficiently, and reduce costs. But before jumping on board, it's best to examine your motives for moving to a converged infrastructure in the first place and make sure that you're choosing the right converged solution.

At its core, a converged infrastructure should simplify IT while helping the IT staff achieve its goals—whether it is improving disaster recovery at branch offices, being able to provision virtual machines more quickly or consolidate workloads. With that in mind, it pays to look under the covers at the solution to ensure that it does more than just bundle servers, storage and networking into one package. In addition, it should include comprehensive monitoring, security administration and IT management activities. It should also include tools to analyze potential failures and performance impacts and conduct root cause analysis. Other must-haves include automated patching and updates. And, of course, make sure that the converged infrastructure solution supports the operating systems and applications your organization requires.

In addition to analyzing the bundle's features, it's also important to fully understand the relationship between the technology components. For example, do all components come from one vendor, or is it a package that includes technology from multiple vendors? If it's a multivendor package, make sure the technology stack is fully integrated, and that the hardware vendors and application providers have stronger partnerships with each other. That includes confirming that all software is certified to run on the converged infrastructure hardware.

Once deployed, there are steps agencies can take to get the most out of the solution. For example, by automating the process for deploying both new and legacy applications onto a converged infrastructure, agencies will have a standard way of standing up applications quickly and efficiently.

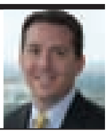
Another way to increase the benefits of a converged infrastructure is by setting up a self-service portal that allows internal users to choose the services they will be using. If, for example, users expect to frequently use a particular Web application service, they can pre-select that service so that IT can deploy it quickly on demand.

Culture and process changes

Choosing the right converged infrastructure is just the first step. Since it's a different deployment model, an IT staff will have to be cross-trained in other disciplines. For example, in the traditional data center model, an agency might have separate server, storage and network specialists. But with converged infrastructure, all of the components are managed together.

The changes in IT culture are permanent. In addition to finding that individual administrators need to know about servers, storage and networking, IDC found that important new skills include the ability to rapidly detect and remediate problems, understand the best way to make effective use of self-service, and understand which types of applications are best suited for converged or integrated systems. •

BRIAN GAGNON is a senior director at CEB.



Why strategies get stuck

Poor execution, not poor planning, derails many new programs, but there are steps agencies can take to stay on track, despite the coming leadership changes

Why do so many sound and meticulously planned strategic efforts go awry? A recent study cited in The Economist concluded that 61 percent of organizational strategies underperform not because of faulty ideas or poor planning, but as a result of poor execution.

Through conversations with hundreds of cross-functional leaders, CEB has identified what the most successful organizations do differently when implementing a new strategy or change initiative: They mobilize their leaders by ensuring that they are aligned on strategy and are able to focus effort on related activities.

In effect, the best organizations go beyond establishing buy-in and an understanding of strategy by unlocking employees' capacity to execute.

The gap between strategy and execution is a challenge in both the private and public sectors. However, the federal government faces an additional risk that will intensify the challenge in the years ahead. Based on our analysis of 2014 Federal Employee Viewpoint Survey results, 48 percent of Senior Executive Service members plan to retire in the next five years. Furthermore, we expect to see a spike in leadership transitions in the next 24 months as executives anticipate the end of the Obama administration.

Key executive sponsors and leaders — those who built the vision and path forward for positive change — will leave the federal workforce. As a result, strategic initiatives could stall and years of investment and hard work could be at risk.

Additionally, as federal agencies continue efforts to enhance evidence-based decision-making and performance management, they will face increasing pressure to link strategic plans to demonstrated results. Many programs that fail to show progress on strategic goals and objectives will face an uncertain future as budgets continue to shrink.

> The best organizations go beyond establishing buy-in by unlocking employees' capacity to execute.

Luckily, there are steps that agencies can take to ensure that they continue to make progress on strategic initiatives:

1. Manage leadership alignment as a continuous process. Rather than taking a room full of head nods as leadership commitment, agencies must focus on generating lasting leadership team alignment. Instead of simply communicating the importance of new strategies, leaders need to actively manage alignment, mitigate resistance to new strategies and continually achieve support across the leadership team.

2. Give program and functional leaders the authority to stop projects. Leaders need to make judgment calls about what initiatives to cut in order to free the capacity and mental bandwidth necessary to execute something new. High-performing agencies give their leaders permission to decide what to stop doing so they can quickly focus their managerial capacity and resources on new initiatives.

3. Eliminate misaligned assumptions and legacy behaviors. Managers across the agency, but particularly those on the frontlines, must model and enable new behaviors to drive better, more sustained effort on new strategic objectives. The best agencies continuously unlock employee capacity and motivate ongoing effort by providing managers with the tools they need to eliminate legacy behaviors that do not directly support the new strategy.

As leadership transitions continue to take center stage, agencies must enable employees to rally around strategic initiatives. Failing to do so could result in months or even years of costly strategy derailment, which could ultimately put mission achievement at risk.

By creating a workforce where leaders and employees are aligned around achieving strategic goals, agencies will reap the benefits of a highly engaged and productive workforce with the ability to successfully achieve targeted results and outcomes. ■

DAVE McCLURE is chief strategist at Veris Group.

How Congress can make cyber reforms real

Congressional oversight is essential to ensuring compliance with cybersecurity legislation. Here are three ways lawmakers can improve that oversight.

In 2014, industry and government were rocked by major cyber breaches and attacks that highlighted continued vulnerabilities in security management. As a result, corporate and agency executives are beginning to pay attention to the business and customer impact rather than assuming security is the narrow and exclusive technical domain of chief information security officers and CIOs.

That change in attitude comes as IT is growing ever more pervasive via the interconnected systems, devices, monitors and sensors that make up the Internet of Things. New business solutions, emerging interactive technologies, innovative data aggregation and delivery options, and hyperscale infrastructure technology all require robust information assurance and privacy protections.

Congress, meanwhile, has passed several reform bills that are moving federal cybersecurity in a similar direction, and no less than eight committees and subcommittees in the House and Senate have announced intentions to hold cybersecurity-related oversight hearings this year.

Congressional oversight is critical to ensuring transparency and accountability for compliance with new legislation. So what can Congress do to more effectively oversee implementation of major cybersecurity reforms? Let me offer three suggestions based on my experience working for and reporting to congressional oversight committees:

1. Focus on fact-based discussions. Oversight is most effective when committees ask agencies for facts that demonstrate how cybersecurity dollars are producing tangible improvements. How have legal, regulatory, economic or mission impact risks been mitigated? Can the agency demonstrate that it is implementing security programs in a cost-effective manner? What is being done to simplify security insights to increase responsiveness and resiliency to changing threats?

> Oversight is most effective when committees ask agencies for facts that demonstrate how cybersecurity dollars are producing tangible improvements.

2. Learn from leading best practices and avoid past mistakes. Security is not a one-size-fits-all affair. There are operational, technical and managerial controls that apply to any effective security program, but risk management frameworks should result in risk profiles that vary across different agency missions.

Furthermore, with so much security now outsourced as managed services, clear contractor accountability for performance is essential. Congress should demand this focus from audit groups and the reports they issue to oversight committees. With governmentwide buy-in from the executive and legislative branches on a baseline set of controls (like the FedRAMP controls for cloud solutions), audits can become less of a guessing game.

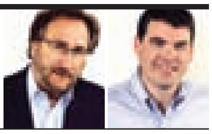
3. Seek consensus on how to prioritize corrective security actions. At the Department of Veterans Affairs, the inspector general reported some 6,000 security risk findings and made 35 recommendations as part of the agency's reporting under the Federal Information Security Management Act.

But how can VA or any agency possibly address the thousands of findings and related recommendations? What is attributable to lack of management support versus inadequate budget resources or poor budgeting practices? Are resources within existing budgets available to shore up weaknesses, and if so, how can they be prioritized?

Given the vast array of policy, process, managerial, technical and operational demands that are in play, at least some degree of consensus on risk-based priorities is paramount. Agency leaders, inspectors general and the Office of Management and Budget all have important parts to play, but Congress can have a special role in ensuring that viable security solutions are put in place. ■

LARRY ROSENFELD AND ALEX MITCHELL

LARRY ROSENFELD is CEO and **ALEX MITCHELL** is an account executive at Sage Communications, a full-service marketing agency.



New policies are cause for contractor optimism

Several activities in the new Congress signal a shift in spending and strategy that will require increased support from contractors

The 114th Congress is underway, and we're beginning to see signs of change for major policy items, a few of which will have a direct and largely favorable impact on the federal IT community.

It's not often that a midterm election can change the outlook for an entire industry. And although Republicans took control of the Senate and extended their majority in the House, it would be simplistic to point to one party as the impetus.

Movement can be seen by policymakers on both sides of the aisle as the zeitgeist slowly evolves from a focus on domestic budgets to concern about international affairs.

This was one of the few elections in which international concerns held center stage, perhaps even outweighing the economy, Affordable Care Act and other domestic agenda items. Several freshman senators spent millions of campaign dollars touting the ways they would strengthen the United States' national security posture.

And it's not just talk. The GOP takeover in the Senate means that veteran lawmakers John McCain, Bob Corker and Richard Burr now lead the Armed Services, Foreign Relations and Intelligence committees, respectively. Those three panels wield significant power over defense legislation, and McCain has said that his first order of business will be to end the sequester.

That budget rule currently requires the military to make across-the-board spending cuts, and along with lowest price, technically acceptable contracts, it has been shaking up the federal IT community for nearly three years. Those policies might or might not have helped ensure the best value for taxpayers, but they have undeniably led to challenges in the industry.

> This was one of the few elections in which international concerns held center stage, perhaps even outweighing the economy.

Then there are matters that are fundamentally foreign policy concerns but might nonetheless alter the IT landscape. One issue that already has Congress stirring, for example, is the expansion of military operations in the Middle East. The shift in the Senate has opened the door to a new authorization for war against the Islamic State group.

The president called for such a measure in his State of the Union address, and if one should pass with bipartisan support, we would likely see a large increase in military and intelligence resources devoted to a campaign that is already being waged with cutting-edge technologies and weapons systems.

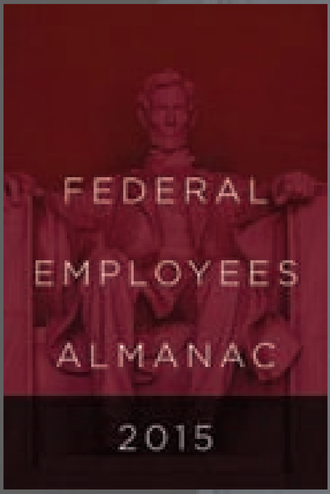
A new war authorization, coupled with Ashton Carter's confirmation as Defense secretary, could signal a shift in strategy that would require increased services from contractors.

Last and perhaps most important, there is cybersecurity legislation. Republicans have been trying to guide the Cyber Intelligence Sharing and Protection Act through Congress for almost four years but have been stymied by some senators' privacy concerns. Although Obama has expressed similar concerns, his recent proposals suggest a desire to break down the barrier that exists between the private sector and the government to make it easier to create cybersecurity solutions that serve everyone.

Passage of CISPA is hardly guaranteed, but it and other key policies will be debated this year — and many, if not all, companies that provide IT products and solutions to the government will have a stake in the importance that is placed on information sharing and privacy.

Any one of those items by itself might not move the needle significantly, but taken together they show a trend toward a normalization of government spending.

There is a great deal of optimism and confidence right now among contractors. As many companies are going through annual planning efforts, our recommendation is to begin thinking about kicking aggressive business development efforts into high gear. ■



FEDERAL EMPLOYEES ALMANAC

2015

More effective oversight. *Maybe.*

FITARA gives Congress new tools for getting answers, and key legislators remain focused.

But will it actually work?

BY ADAM MAZMANIAN

We can thank the HealthCare.gov debacle of 2013 for a new law that concentrates IT spending, planning and hiring in the hands of department-level CIOs. A few advocates on both sides of the aisle in Congress had been pushing for updates to the decades-old Clinger-Cohen Act, but it took the public failure of a key piece of government technology to generate a widespread interest in the bill. It narrowly failed in 2013 and squeaked through in the closing days of the 2014 session as a section of the defense authorization bill.

The Federal IT Acquisition Reform Act — known as FITARA, although its lead sponsors prefer the moniker Issa-Connolly — is designed to give top CIOs authority over IT, and it enshrines a few executive branch technology initiatives, such as data center consolidation and strategic sourcing, into law.

But CIOs aren't the only group empowered by the legislation. The law also has the potential to change the way Congress performs oversight by giving members new tools to make their work more efficient and effective. From that perspective, the law helps Congress get answers.

"Most importantly, FITARA requires single-point accountability," said Rep. Darrell Issa (R-Calif.), the law's top backer. "The CIO under the act has the responsibility to be responsible. We believe that prevents a situation of finger-pointing. CIOs know their responsibility and that they will be held accountable."

That promises to be an improvement over the chaos that seemed to reign in the wake of HealthCare.gov's launch. Issa's committee obtained and released email messages showing that the top tech officials at the Department of Health and Human Services had no visibility into the single biggest application-development project on their watch.

"In the case of HealthCare.gov, you had four people who were theoretically in charge, all of whom said they lacked

A November 2013 hearing on HealthCare.gov was a prime example of the finger-pointing and fuzzy accountability that can surround IT oversight. FITARA supporters say the new law can create more clarity. (Pictured: Centers for Medicare and Medicaid Services Deputy CIO Henry Chao, Health and Human Services Department CIO Frank Baitman, former federal CTO Todd Park and former federal CIO Steven VanRoekel.)

AP IMAGES

the authority to shut it down," Issa said.

Dave McClure, former associate administrator of the General Services Administration's Office of Citizen Services and Innovative Technologies and a former auditor specializing in IT issues at the Government Accountability Office, sees a big opportunity for improved accountability.

"The CIO is going to be the key spokesperson for a Cabinet department on where they are with their IT strategy, IT security and IT spending," he said. "In the past, that's been bifurcated across CIOs, and it's been hard for a departmentwide CIO to answer questions in full compliance because they don't own or control funding, contracting and strategy for the entire entity. That changes a lot under FITARA."

Implementation will be the key to improving governance. Issa and co-sponsor Rep. Gerry Connolly (D-Va.) have pledged to make sure the law's provisions are instituted through guidance from the Office of Management and Budget to the civilian agencies that fall under the FITARA umbrella.

Making implementation work

The law originated in the House Oversight and Government Reform Committee. Issa's memorable tenure as chairman of the panel recently ended, and he has moved on to lead the Judiciary Committee's Courts, Intellectual Property and the Internet Subcommittee. Connolly remains on the oversight committee and will serve as ranking member of the Government Operations Subcommittee, where he plans to keep a hand in IT issues and FITARA implementation in particular.

Connolly told FCW that he will track efforts by OMB and the CIO Council to develop guidance for agencies on FITARA and oversee implementation on an agency-by-agency basis. He wants to make sure that "every agency head is held accountable for establishing ownership over concrete, detailed FITARA implementation plans and policies for his or her given agency."

"I think we have a real opportunity

"This is one of those legacy things, and Gerry Connolly and I will keep our eyes on it and take special interest and work together to see that it's fully implemented."

— Rep. Darrell Issa (R-Calif.)

AP IMAGES

for some very substantive hearings, and I certainly intend to push early on for rigorous oversight hearings on this subject," Connolly said.

He was also blunt about how the oversight panel can use the requirements of the law to spur action. "It sets new metrics that allow us to measure how they're doing. We can push on the personnel piece in terms of CIOs," he said. Given the new range of IT planning, personnel and budget authorities embedded in the CIO role under FITARA, he added that some agencies might "decide that new leadership is required."

Issa and Connolly could do a great deal for FITARA just by sticking around. The Clinger-Cohen Act was implemented without input from its sponsors because soon after its enactment Rep. Bill Clinger (R-Pa.) retired from Congress and Sen. William Cohen (R-Maine) was tapped to serve as secretary of Defense by President Bill Clinton.

"Anytime Congress passes a major management statute, there's an interest especially from the authorizing committee in the first year or two years to see how the statute is being implemented," said Dan Chenok, chair of the Industry Advisory Council and executive director of the IBM Center for the Business of Government. "Most likely Congress will continue to be interested in these issues for the next year to two years and maybe longer."

Paul Brubaker, who helped write the Clinger-Cohen Act as a Senate staffer and later served in leadership roles at the Defense Department, said he is concerned that FITARA implementation could suffer from a brain drain caused by Issa's departure from the committee and the changeover of majority staff under its new chairman, Rep. Jason Chaffetz (R-Utah).

"Oversight is only as good as the knowledge of both the members and the underlying staffers," Brubaker, who is now director of AirWatch's U.S. federal government business, told FCW. "Members don't have the time to dive deep into these issues for the most part — into the nuances and operational aspects of the CIO role. Agencies know that, and they'll take advantage of it."

Issa acknowledged that there might be a lack of institutional knowledge on the Oversight and Government Reform Committee but said many of his former staffers have found new posts on authorizing committees in the House and Senate where they can bring their expertise to bear on IT issues.

And FITARA isn't just a tool for the governmentwide oversight committees. The authorizing committees for individual departments will now have an accountability mechanism for IT projects that fall under their jurisdiction.

The new faces of IT oversight

Chaffetz, who was not interviewed for this article, is reviving the IT Subcommittee that was shelved by Issa, who preferred to handle IT issues at the full committee level. Rep. Will Hurd, a GOP freshman from Texas, has been tapped as chairman. Although committee sources say the Government Operations Subcommittee will take the lead in terms of staff resources and personnel, the IT Subcommittee will play a big role in overseeing federal technology.

Hurd served for nine years as an undercover officer in the CIA in the Middle East, South Asia and elsewhere. He also has a background in IT, including a degree in computer science from Texas A&M University and a stint at cybersecurity firm FusionX. Hurd resists the tag of "IT vendor" because he mostly worked on penetration testing for companies. Still, he's a rare technologist in a Congress that is made up largely of lawyers, businesspeople and career politicians.

Hurd downplayed his technical chops in an interview with FCW, saying, "I may be able to bang out some Fortran 77 code right now." But more important, he said, he could "understand and articulate technical issues

— a skill set that is lacking here in Washington, and I'm looking forward to playing a part and using that background."

As a new member, he's still getting up to speed on the folkways of Congress and working through a pile of GAO and inspector general reports on IT topics that he might want his subcommittee to explore. He's also familiarizing himself with the impressive raft of IT-related legislation, including FITARA, enacted at the tail end of the 113th Congress.

Hurd plans to cut a wide swath across tech issues, including federal cloud implementation, procurement, data breaches and cybersecurity in general. And because his district contains 825 miles of the U.S./Mexico border, Hurd takes a special interest in how technology can be used to make border protection smarter and more effective.

"My role in Oversight and Government Reform is to shine the flashlight on some of these issues and work with the authorizing committees — Homeland Security, Armed Services, Judiciary — as well as with Appropriations to help propose solutions," he said.

Connolly hopes to serve on Hurd's subcommittee but said he plans to focus his efforts on the Government Operations Subcommittee. Highlighting IT issues can be helpful, Connolly said, "but the risk is that we stovepipe it."

A lead Democrat for the IT subcommittee had not been named when this issue went to press.

Obstacles remain

FITARA's sponsors are bullish on the prospects for improvement. "There's $20 billion to be had here," Connolly said. "Issa-Connolly can effectuate very substantial savings." More than just saving money, he added, it can focus government technologists on achieving the best outcomes.

Connolly said he hopes the law will "foster a change in attitude [about] how we approach the transformative power of technology. Too often technology is treated as just a commodity. We are hoping these reforms will be a catalyst to get government to address the underutilization of technology in the public sector."

Brubaker, however, is concerned that the concepts embedded in the legislation won't find their way into federal practice. "Many agencies did not embrace the concepts in Clinger-Cohen," he said, but instead took cover in over-prescriptive guidance from OMB. Often there was resistance from leadership at the secretary and deputy secretary level.

Can FITARA surmount similar obstacles? "My guess is that it will make some incremental improvements, but achieving Information Age outcomes in this construct is not going to happen," Brubaker said.

McClure, who is now chief strategist at the Veris Group, agreed that leadership buy-in is essential for the timely implementation of FITARA, especially "the support the CIO gets from the non-IT executives within the agency." Often, he added, "the CIO's success is dependent on productive working relationships with the [chief financial officer] and the leaders of the mission-delivery arms of the agency."

Furthermore, lawmakers hoping to use the statute to improve oversight face built-in obstacles. Congress is outstaffed and outspent by the federal bureaucracy it is charged with overseeing, and it faces the perennial problem of attracting and retaining talented subject-matter specialists at the derisory rates typically offered for legislative staff work.

Nevertheless, Issa and Connolly could prove to be the best advocates for the law's success. "The biggest stakeholders are still here," Connolly said. "Darrell's around. I'm around. And I am tenacious."

"This is one of those legacy things," Issa said, "and Gerry Connolly and I will keep our eyes on it and take special interest and work together to see that it's fully implemented." ■

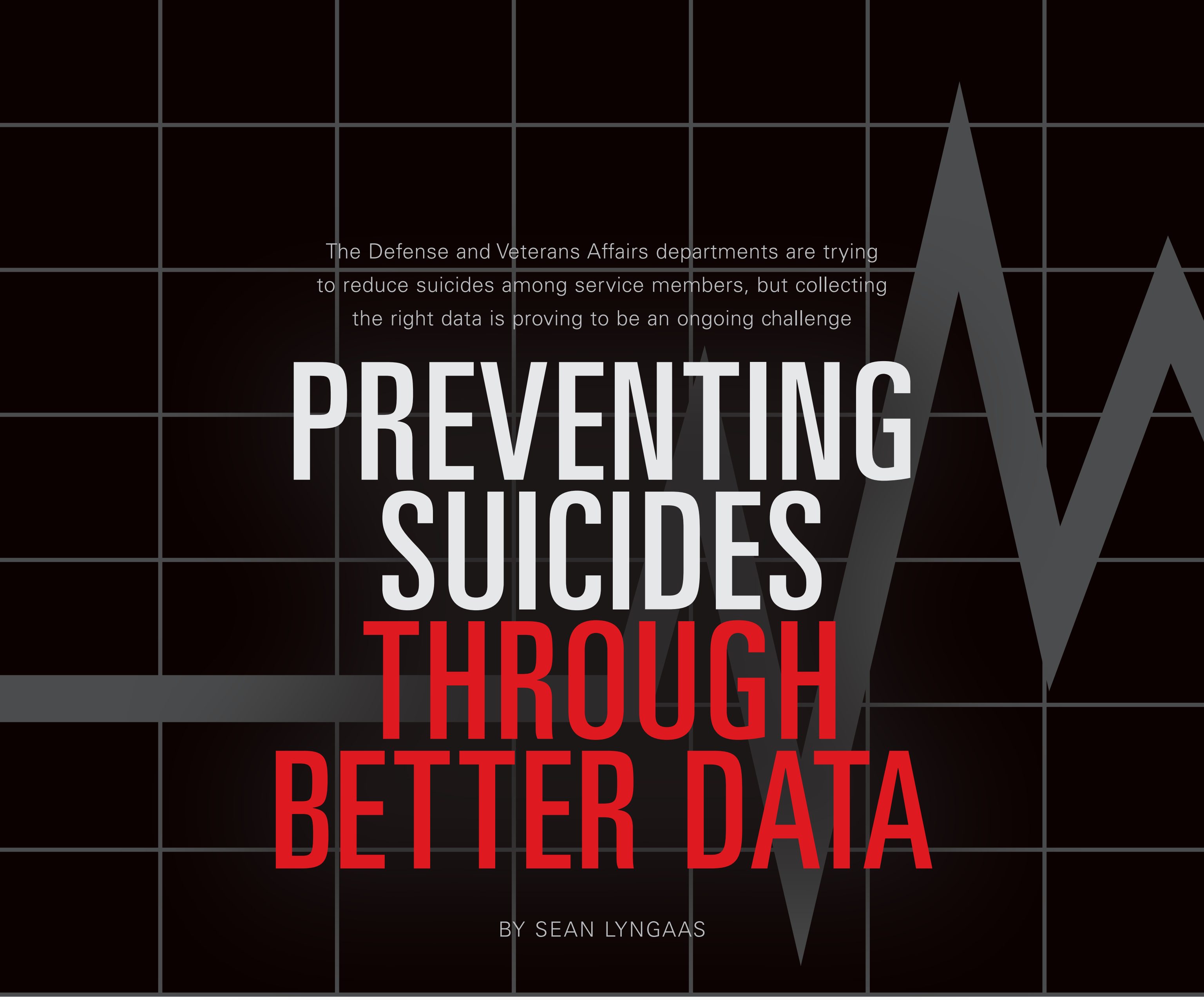
Beyond FITARA

These newly passed measures will also be part of Congress' IT oversight agenda:

- **The Federal Information Security Modernization Act** is designed to streamline federal network security policy, practice and oversight. It codifies the current division of labor for protecting federal networks, with the Office of Management and Budget responsible for policy and the Department of Homeland Security focusing on implementation. The law also requires OMB and DHS to report on adoption of continuous monitoring technologies, including commercial products offered under the Continuous Diagnostics and Mitigation program run by DHS.
- **The Digital Accountability and Transparency Act** isn't exactly a tech bill, but it does require federal budget and spending information to be published in machine-readable form. That might not sound exciting, but it gives public interest groups, businesses and Congress a chance to visualize and understand the federal balance sheet in new and potentially enlightening ways.
- **The Border Patrol Agent Pay Reform Act** authorizes DHS to hire senior-level cybersecurity specialists at pay grades comparable to the military or spy agencies, while also taking inventory of the agency's cybersecurity workforce.
- **The Transportation Security Acquisition Reform Act** puts the Transportation Security Administration on a short leash when it comes to tech procurement and requires TSA to develop and update a five-year strategic IT spending plan.

— Adam Mazmanian

FCW
Patient data the next IT frontier at VA
OMB offers advice for fiscal 2016
Lawmaker voices concern about possible DIA nominee
MANAGING THE NETWORKED ENTERPRISE
SPECIAL REPORT
Cloud in 2014
DOWNLOAD THE
CompTIA acquires TechAmerica
MEASURE TO MANAGE



The Defense and Veterans Affairs departments are trying to reduce suicides among service members, but collecting the right data is proving to be an ongoing challenge

PREVENTING SUICIDES THROUGH BETTER DATA

BY SEAN LYNGAAS

Something as impersonal and mundane as incomplete datasets could be exacerbating a national tragedy: the suicides of thousands of veterans and hundreds of active-duty service members every year.

Preventing such suicides depends in part on the quality of the government's data on potential contributing factors such as mental health and disciplinary history. Officials at the departments of Defense and Veterans Affairs have underlined that point by making improved data management one of the bedrocks of their suicide-prevention strategies in recent years.

Interviews with DOD and VA officials reveal a joint data policy to track suicides that is gradually getting off the ground and overcoming bureaucratic inertia. At the same time, however, a recent report by DOD's inspector general revealed that the information in the department's main collection system for suicide data — recent improvements notwithstanding — is often incomplete.

The IG investigation, published last month, made clear the potential consequences of flawed reporting of suicides and called inadequate suicide-prevention programs "a substantial and specific danger to public health and safety."

The technology at issue is a DOD-wide database created in 2008 for reporting service-member suicides and suicide attempts: the DOD Suicide Event Report (DODSER). Information on those deaths is used by military officials to try to make the next suicide less likely. The data includes medical history, military history (such as demotions, disciplinary cases and deployments) and demographic data. The report also covers contextual details such as where and in what environment the suicide took place.

The IG analyzed the 287 suicide cases reported through the database in 2011, the most recent annual data available at the time, and found that nearly a quarter of them had answers marked “don’t know” or “data unavailable” in 50 percent to 100 percent of the data fields.

The most common fields marked unknown or unavailable were whether the deceased was a victim of emotional abuse (missing 61 percent of the time), whether he or she had visited chaplain services (57 percent) and whether the deceased had a family history of mental illness (57 percent).

It is important to note, however, that the IG study did not include the 2012 DODSER annual report, which was released on April 25. An appendix to the IG report notes “several areas of marked improvement” in DODSER data collection in 2012. The rate of “unknown” or “unavailable” answers to question of emotional abuse, for example, dropped from 61 percent to 35 percent.

Nonetheless, the 2012 report shows a significant degree of incomplete DODSER data. The IG’s report notes that one reason for the missing information in 2011 is that many of the DODSER questions had medical jargon that only an expert could answer. If reports are incomplete or inaccessible to some, officials are working with an incomplete picture in devising mental health policies.

Picking up missing data pieces

The database is managed by the National Center for Telehealth and Technology (known as T2), a DOD organization charged with applying technology to mental health problems.

T2’s fiscal 2015 budget for managing the DODSER database and generating an annual report from it is $500,000, which does not include the military services’ budgets for using the database.

There are two parts to the training an officer receives to learn how to fill out a DODSER. The first is an online evaluation, and the second is the specific DODSER training administered by each of the military services, said T2 Deputy Director Mark Reger, who leads the DODSER program.

He said user training for DODSER is adequate, but no one is going to be an expert in every aspect of what DODSER requires. For example, a military commander might know a soldier’s deployment history but not his medical diagnosis.

The IG report recommends that DOD take a more multidisciplinary approach to reporting suicides, with each suicide triggering a local review board made up of unit leaders, medical professionals and military investigators. That approach would help deliver more complete and accurate data to the DODSER database, the IG said.

Rajeev Ramchand, a senior behavioral and social scientist at Rand Corp. who studies suicide-prevention strategies for service members, offered an additional remedy to the problem of inexpert DODSER users. He called for a team of trained data experts at DOD to handle the data input for every case of suicide rather than relying on a wide range of officers who might have very little experience with the database.

“Are we looking for somebody who’s an expert in every single field or are we looking for somebody who’s an expert in collecting the data?” Ramchand asked. “I would always go with someone who is [an expert in] collecting the data.”

Ramchand said the DODSER database is an effective and comprehensive means of tracking military suicides and suicide attempts but pointed out what he said is a blemish: The input fields do not leave much room to explain the source of the information. For example, if an entry notes that a soldier had trouble in a romantic relationship, it might simply cite the commander as the source of that information.

Ramchand said limited information in that case might misidentify a contributing factor to suicide. “The point of surveillance is to identify trends so that we can intervene, and we need to make sure that we’re intervening on the right things,” he said.

Although DODSER matches up closely with many of the Centers for Disease Control and Prevention’s recommendations for compiling suicide data, one area where it does not is in detailing the source of the information, Ramchand added.

The hunt for better data is not likely to ever be fully satisfied, but the previous approach puts things in perspective. Before the DODSER database began to offer a standard method of suicide surveillance in 2008, the military services “each had their own [systems] for analyzing and understanding the characteristics and nature of suicide in their service,” Reger said.

DODSER offers a more complete picture of suicide across the services, one that DOD is trying to combine with data provided by VA.

The promise of data sharing

Reports from military bases around the world are one piece of suicide-prevention policy. Another is sharing that data with VA as soldiers retire and become veterans. To that end, the two agencies set up a joint Suicide Data Repository (SDR) in fiscal

2013 by acquiring mortality data from the CDC on veterans and active-duty service members.

VA had been working with the CDC since 2006 to collect suicide data on users of Veterans Health Administration services, said Robert Bossarte, co-director of the SDR and director of the Epidemiology Program in VA's Office of Public Health.

But that approach gave a startlingly incomplete picture of the problem because many veterans do not use VHA services.

When you run a veteran's name and Social Security number through the nascent repository, it matches that information up with the CDC's National Death Index and then returns a probabilistic score of matching records. A 99 percent score would indicate a near-certain match.

"The clinical and public health importance [of data from the repository] can't be understated," Bossarte said. "Understanding…increased risk following separation from service, understanding the impact of VA and DOD prevention and transition programs, and understanding new opportunities for intervention [are] only [possible] if we understand the epidemiology of risk in this population."

"One of the things that [the repository] did was allow for VA and DOD to agree upon a matching algorithm to identify when a case is a case," he added.

Bossarte said the SDR currently holds about 25 million personal records, including some duplicates. Of those, the system has identified 2 million veteran deaths since 1979, which is how far back the data goes. Bossarte said he and his colleagues are looking for other sources of data to track veterans who died before 1979. That is another chapter in the endless hunt for data to help prevent future suicides.

DOD and VA will open the SDR to public viewing when they release the first annual report on the database in the coming months, Bossarte said, adding that he hopes the report will help researchers understand what percentage of the total veteran population has been included in suicide data over the years.

For independent researchers like Ramchand who want to review the data, that annual report can't come soon enough. He said he would like to see those in charge of the SDR be more specific and public about their goals for the database and a timeline for achieving them.

SDR data has been made available to researchers for 51 studies, but all those researchers are affiliated with VA or DOD.

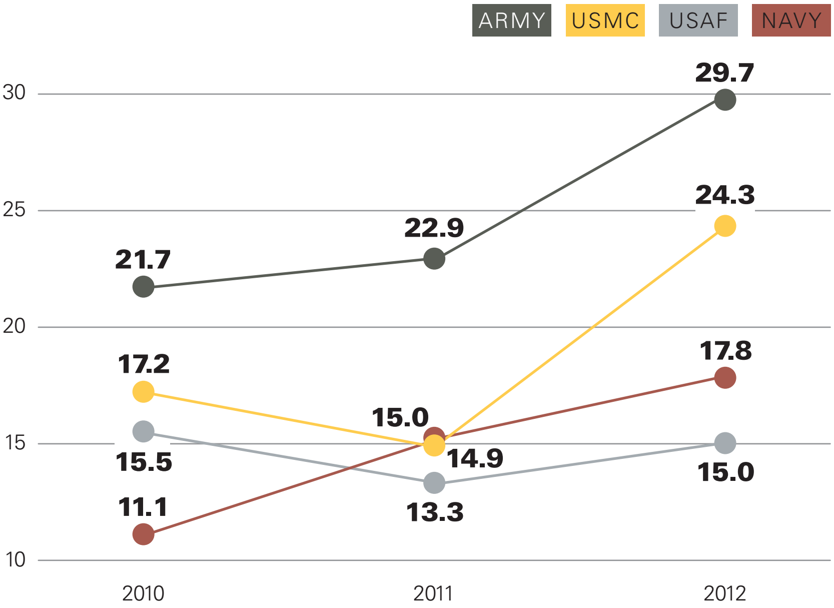
Key piece of DOD/VA repository untapped

DOD and VA have given the cause of suicide prevention significant attention and resources in recent years. "Increasing data fidelity" was one of the nine priorities identified by the Suicide Prevention General Officer Steering Committee, a group of flag officers, Senior Executive Service members and other officials in charge of implementing DOD's suicide-prevention strategy.

At times, the challenges of harnessing the two vast bureaucracies of DOD and VA toward a common goal have been plain. In August 2010, a DOD task force recommended a revised, standardized suicide-reporting methodology. But it was another three

Suicide rates among active-duty service members

The most recent data available shows a steady uptick in the number of suicides among service members.



*Rates per 100,000 service members per year

Source: Defense Department Suicide Event Report Data Quality Assessment and half years before the department formally implemented that methodology in the form of a March 2014 memo.

When FCW asked Jackie Garrick, acting director of the Defense Suicide Prevention Office, why it took so long to implement the new methodology, she said officials needed time to include new data for the National Guard and Reserves and to test large datasets.

With that revised methodology, DOD can now compare factors that potentially increase the risk of suicide for active-duty and reserve service members and, in turn, "do more to target our policies and our programs…specific to those different populations," she said.

Perhaps an even more important hurdle for improved data policy will be getting the joint VA/DOD repository to actually share records, as it is intended to do. Right now, although data from the DODSER database and the VA equivalent is in the joint SDR, Bossarte said it is not being shared back and forth.

The repository's current focus is on mortality, whereas its mandate includes sharing data on possible suicides. If one wants to track a recently retired service member, now a veteran, using the SDR, "you would have to piece the data together, but all of the elements are included that would make that possible," Bossarte said.

DOD and VA officials say they will work in the coming months to reap more from predictive analytics for their suicide-prevention programs. Garrick said the Defense Suicide Prevention Office is tapping into the resources of the Defense Manpower Data Center, the Pentagon's data hub for military personnel, to turn data into a "predictive lens" to spot suicide risk among service members.

The point of surveillance is to identify trends so that we can intervene, and we need to make sure that we're intervening on the right things.

— RAJEEV RAMCHAND, RAND CORP.

As for DODSER, Reger said T2 will seek to implement the IG recommendations for improving the database and its management. He added that many of the recommendations were not news to T2 and the agency has been already addressing them.

For example, the IG report notes that the software used by DODSER automatically archives a record 180 days after it has been entered and prevents it from being updated. The deadline stems from a regulatory mandate to protect service members' privacy, Reger said. But that rigidity prompts some DODSER users to submit a report before the medical examiner's investigation is finished, resulting in incomplete information.

"We have already begun coordination of documents to change those regulatory requirements," Reger said, adding that he expects the change to be made this year.

The quality of DODSER submissions has improved since September 2013, when T2 began providing feedback to the services on their submissions, according to the IG report. For example, in the third quarter of 2012, "the average DODSER submission for the Army and Navy was less than 70 percent complete," the report states, but by the first quarter of 2014, "both services had increased to an average of more than 90 percent."

An invisible finish line

Improving the quality of data on suicide attempts among service members and veterans will likely be an endless task. Given advances in big-data analytics, improvements will always be possible. As Reger said, "I think the challenge of ensuring the highest quality data that you can will be an ongoing process."

Congress is also playing a part in suicide data policy. Lawmakers have included a provision to improve suicide data collection in the $585 billion defense authorization bill for fiscal 2015. The bill tasks DOD with developing "a standard method for collecting, reporting and assessing information regarding" suicide and suicide attempts, something the department has already committed to doing.

A critical challenge for DOD, VA and Capitol Hill will be to ensure that too many cooks don't spoil the broth. All the working groups, task forces and memos in the world will matter little if they do not lead to a drop in suicides. And, of course, improving data is but a piece of policy efforts to prevent military and veteran suicides. More important to the cause is the quality of mental health care that service members and veterans receive.

But data is a window into the problem, and the sharper that view comes into focus, the better off America's uniformed and retired military men and women will be. ■

The uncertain marriage of CDM and FedRAMP

Two vast risk management programs are gradually converging. How smoothly and quickly they can do so remains an open question.

BY SEAN LYNGAAS

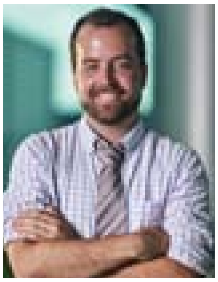
The government has gone all in on Continuous Diagnostics and Mitigation (CDM), a wide-ranging and ambitious program to guard agency networks against cyber threats. Run by the Department of Homeland Security, the program addresses 15 types of continuous diagnostics and pairs a dedicated acquisition vehicle with expert guidance and even DHS dollars for agencies seeking to improve their monitoring.

The first phase, which focuses on endpoint device security, has drawn widespread interest, and managers who have implemented CDM have said the system of dashboards provides a revealing view of vulnerabilities — many of which had gone unnoticed under previous monitoring regimes.

A big question looms over the future of CDM, however: Can the program accommodate agencies' increasing demand for cloud computing and the Federal Risk and Authorization Management Program (FedRAMP) that was designed to accelerate the shift to the cloud?

"I think [continuous monitoring in FedRAMP is] solid. But it's largely compliance-based. **I'd like to make it more risk-based."**

— Matthew Goodrich, director, FedRAMP



Why it matters

It is a truism that bears repeating: Cyber threats to federal networks are a clear and present danger. In recent months, cyberattacks have hit agencies ranging from the Office of Personnel Management to the State Department.

And although the structures and scopes differ greatly, CDM and FedRAMP share a broad goal: to use a standardized and repeatable security process to make damaging intrusions to federal networks significantly less likely. But absent a clear road map for coordinating the two initiatives, agencies risk adding compliance hoop-jumping and unnecessary complexity to their cloud security efforts when the goal is to streamline and focus on risk.

The fundamentals

At the core of CDM is a contract vehicle that currently involves blanket purchase agreements with 17 vendors for a wide range of equipment and consulting and other services that contribute to a holistic view of network vulnerabilities. It provides agencies with a means to not only meet the continuous monitoring mandates that are part of the Federal Information Security Management Act, but to move beyond compliance-driven monitoring to the truly dynamic and risk-based approach demanded by a November 2013 Office of Management and Budget policy memo.

FedRAMP is based in the General Services Administration and steered by GSA, DHS and the Defense Department. The program mandates agencies' adoption of common cloud security standards and seeks to streamline that process by reusing the costly assessments and authorizations of various cloud services. It, too, is mandatory for all agencies, thanks to OMB's December 2011 directive, and it has continuous monitoring provisions of its own. But integration with CDM is not explicitly part of the framework.

Key challenges

The first hurdle in the marriage between FedRAMP and CDM is a fundamental one: The latter's complex structure, which includes a phased model for agency rollouts and types of monitoring, makes wedding it to FedRAMP no easy task.

Officially, all agency cloud projects are now supposed to be FedRAMP-compliant (though there is no clear penalty for missing the June 2014 deadline). CDM is still barely into the second of its three phases. Attention shifted to key components such as access control, credentials and boundary protection — all integral to FedRAMP's requirements — only last summer.

FedRAMP, meanwhile, also continues to evolve. A draft baseline for cloud computing systems that require security at FISMA's high-impact level was released on Jan. 27, and better continuous monitoring is one of nine strategic goals in the two-year road map that FedRAMP Director Matthew Goodrich outlined at a Jan. 22 event sponsored by FCW.

The continuous monitoring that is currently part of FedRAMP is good, Goodrich said, adding, "I think it's solid. But it's largely compliance-based. I'd like to make it more risk-based."

FedRAMP and CDM "already align programmatically and will continue to grow strategically in the same path to move continuous diagnostics and mitigation programs to the cloud," a GSA spokesperson told FCW via email. "Privacy concerns prevent a complete marriage between the two, but [do] not impede progress."

Just what are those privacy concerns? Goodrich said the union of FedRAMP and CDM means dealing with blurred lines between government and private-sector assets. "When you're looking at rolling up reporting into a dashboard with government data, there are a lot of legal and policy and privacy implications for that for private-sector companies versus government assets," he told FCW.

According to Nick Son, Coalfire Public Sector's managing director for technology advisory and assessment services, "It's really about the data input. We need to make sure that the monitoring information [FedRAMP requires] is formatted and standardized" so that it can flow into the CDM program.

There is also the small matter of scale. As Tom DeBiase, chief information security officer at DHS' Immigration and Customs Enforcement, said in October, when his agency took inventory of endpoint devices for CDM's first phase, "we had a lot more technology than we realized." ■

Next steps

The extent to which the Continuous Diagnostics and Mitigation program can benefit from industry-provided cloud services depends on clearing up some ambiguities, vendors say.

Ken Durbin, manager of Symantec's Continuous Monitoring and Cybersecurity Practice, said it might take time for industry and government to get on the same page when it comes to CDM and the cloud.

"I have a concern that [the Department of Homeland Security and General Services Administration] may be assuming that vendors have products teed up, ready to go, to be delivered as a service," he said in an interview. "They may or may not, depending on how 'as a service' is defined."

If DHS were to publish its vision of "as a service" for industry feedback, the two sides could come closer together, he added.

When it began, "the CDM program didn't really come out with [the cloud] as part of its thought process," said Ken Ammon, chief strategy officer at Xceedium. "They started that process before cloud and FedRAMP really had moved forward."

Ammon said that if a product is already deployed through the CDM contract vehicle, there is no way to price additional cloud-computing capacity into the contract. As a result, vendors have so far not "been able to bring their cloud security components to the [CDM] vehicle."

"The biggest challenge that I've seen — considering that both [programs] are supposed to be advancing security — is that the buyers of FedRAMP-approved services still, I think, have a huge gap in their understanding of what their responsibilities are and will continue to be when implementing and utilizing those cloud services," he added.

One of the next signals from government to industry on CDM and the cloud might come from the National Institute of Standards and Technology. It is developing a Cloud Risk Management Framework that will offer detailed guidance on the security risks posed by cloud computing.

Although the guidance might not specifically mention CDM, its language covering the broader topic of "continuous monitoring" would apply to CDM, said Kelley Dempsey, a senior information security specialist at NIST.

The agency generally likes to keep its guidance broad rather than issuing technology-specific documents, but the multitude of applications for cloud computing prompted NIST to develop cloud-specific guidance, which will probably be released by the end of the summer, she said.

— Sean Lyngaas

Get out of the weeds and lead

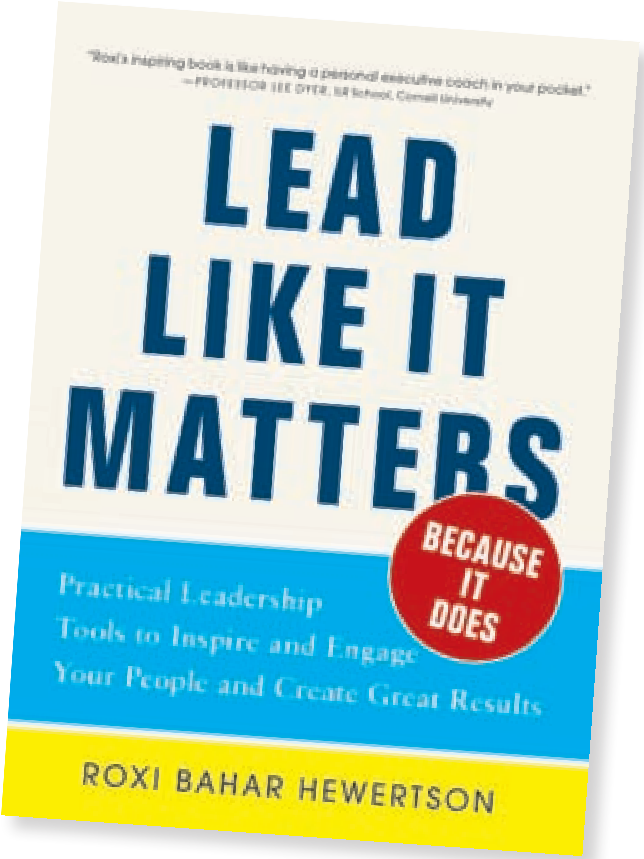
Excelling at a particular activity does not necessarily prepare you to lead a team — just as playing the violin well doesn't prepare you to be the orchestra's conductor

BY ROXI BAHAR HEWERTSON

From the day we were born, all the applause has been about "what I have done well," not "what *we* have done well." Look at your life and your experiences and then fast-forward to where you are today. I think you'll agree that for most of your life, your personal performance generated the lion's share of your positive rewards or negative consequences. It wasn't a group of people; it was you, you and more you.

The exception is teamwork within or outside your family. If you have been a member of a real team of any kind, you may have picked up some insight into the way teams work and even into the way good leadership works. Whether you were on a great team or a lousy team, you learned something about leading and teams. Unfortunately, few people integrate those lessons when they become leaders at work. The fallback position for most of us is what we know best and can count on the most — and that is *me*.

The skills and attributes required to lead people successfully are entirely opposite from the skills and attributes required to be a successful individual contributor. The work, rewards and impact are 180 degrees from each other. Consider this: If the roles and skills weren't so opposite, it would be a walk in the park for someone to move seamlessly from being a great violin player to being a great conductor. Knowing how to play one instrument flawlessly requires one skill set. Knowing how to create harmony from a symphony of people playing


"Roxi's inspiring book is like having a personal executive coach in your pocket."
—PROFESSOR LEE DYER, ILR School, Cornell University
LEAD LIKE IT MATTERS
BECAUSE IT DOES
Practical Leadership Tools to Inspire and Engage Your People and Create Great Results
ROXI BAHAR HEWERTSON

> Leading others is an emotional and intellectual seismic shift that will quickly separate effective leaders from ineffective ones.

This article is excerpted with permission from "Lead Like It Matters...Because It Does."

many varied instruments requires additional, different and opposite skill sets.

In the first case, the violin player is responsible for his performance. The conductor is responsible for knowing what the violin player is capable of and is meant to do, and understanding the job of every other performer in the orchestra. It is also the conductor's job to get the most out of each person and his or her instrument so that everyone will blend well together to produce magnificent music. While the soloists may be appreciated, the audience will remember the performance as a whole. The leader is responsible for the quality of the results. She and they succeed only when the entire orchestra succeeds.

For some people, this transition in roles may come more easily; for most of us, however, it's not a seamless shift because we have not learned how we can most effectively lead others to do their best work. We tend to come at leadership as though it were no big deal: "Hey, I'll get the hang of it — it's just like falling off a log." Or we may consider leading as just another line on our job description, equal or even subordinate to all the other duties and responsibilities listed there. The supervisor role is slapped on, and suddenly you find you still have most, if not all, of your old job and now you are expected to help others create good results.

There might be time cards to approve, vacation schedules, health issues, and messy interpersonal conflicts to deal with, all without getting much, if any, information about how to manage any of those new responsibilities gracefully. Talk about setting up people to fail! This is rarely intentional, and nevertheless, it happens far too often.

Leading others is an emotional and intellectual seismic shift that will quickly separate effective leaders from ineffective ones. Making the transition from being an individual contributor to being a leader can seem as difficult as swimming from New York to London alone, without a life jacket.

How can you make the leadership leap gracefully, you might ask. Of course I'm going to tell you to read my book and do every exercise in it at least once, if not multiple times! Here are some other suggestions: Take a really good leadership development course, find a willing and seasoned mentor who is a good leader, observe other good leaders around you to see how they behave and what they do, observe bad or mediocre leaders around you, [and] finally, regularly ask for and listen carefully to constructive feedback from your direct reports, your stakeholders, your peers and your boss.

Get out of the weeds and *lead*. When you have your entire team fired up and producing great results, you can be far more strategic, including ensuring a sustainable future for your "pond." At long last, there will be time and space for you to be proactive rather than reactive. When you get it right, you will be amazed at how much more time you have to think, to create and to have fun at work. This is not a wild theory, an empty promise, or even wishful thinking. It's real — and it's a beautiful thing. ■

Exercise 1: Three leaders who mattered to you

Think of three leaders who have had a big impact on your life, for good or for ill. Remember their faces, remember their voices, and consider how you feel about each leader's impact on you and why. They could be parents, teachers, mentors, coaches, bosses, someone you read or heard about, someone in a movie that you saw, or someone else. You know who they are.

Write down your answers. I'd like you to get quite specific about each leader's direct or even indirect impact on you and your life.

Who are they?

Name 1: ______________________________

Name 2: ______________________________

Name 3: ______________________________

In how many ways did each of these leaders affect your life? How do you feel about each of them and why?

____

____

____

____

____

AcquisitionMatters

Previewing the future of acquisition

Today's pockets of innovation and IT buying experiments give glimpses of tomorrow's federal buyers and marketplace

BY KYMM McCABE

Acquisition of the Future is an initiative that seeks to frame a vision in which acquisition creates significant new value for the government through fresh approaches, modern technologies and a new generation's capabilities.

Participants include a growing number of federal executives, industry leaders, notable academics and rising acquisition professionals who have been meeting since 2013 to create a framework for what federal acquisition can become to meet the demands of the Collaboration Age — and beyond.

Supporters are continuing their quest to find and capture real-world examples that uncover emerging trends. AOF capitalizes on those initiatives to demonstrate the value that vibrant, forward-focused federal acquisition can provide and to model the strategic decision-making and investments required now to transform the future.

Such experiments are emerging everywhere, especially in the realm of IT. Because technology is evolving so rapidly, the government has difficulty acquiring, modernizing and maintaining it in a way that keeps pace with innovation and commercial best practices. Current government buying processes and culture also make it hard for agencies to take advantage of the pace of technological innovation. Consequently, IT is a hotbed of acquisition experimentation.

> AOF offers a different perspective: Let's stop trying to fix the current, antiquated system. Instead, let's build in a new direction through common goals to create more value, modern technologies and business models.

A common language

We have entered another of the perennial seasons of teeth-gnashing over the government's inability to buy quickly and creatively enough to capture technology's promise. Predictably, calls for acquisition reform are also reaching a crescendo.

Rather than joining that chorus, AOF offers a different perspective: Let's stop trying to fix the current, antiquated system. Instead, let's build in a new direction through common goals to create more value, modern technologies and business models, and a work environment that will draw talented professionals to perform some of the most complex, important and impactful jobs in our country.

To support this undertaking, AOF features a free, open and sharable Transformation Framework and Guide.

The guide puts forth a much-needed common language describing stages of development. It allows users to assess, plan, experiment and share. Specifically, the AOF Transformation Guide describes, rather than prescribes, options at five levels of evolution in five critical dimensions: buyers (the acquiring team), culture, acquisition methods, marketplace and external forces.

To help users focus on the most important activities of envisioning, experimenting and collaborating, the guide was designed to incorporate everything needed to enable application today. It takes account of evolving global and federal dynamics, new opportunities presented by this changed environment, a vision of alternative directions for federal acquisition, a menu of strategic choices that we can begin making now in order to set the necessary changes in motion, and a way to measure and share ideas and progress.

People across the federal community are beginning to use the guide as they plan and work toward their envisioned futures. And because sharing examples of AOF-like initiatives already in development will help illuminate what the future might look like and successful ways to proceed, everyone is invited to capture his or her journey and findings on the soon-to-be-launched AOF Transformation Collaboration website.

Heightened expectations

The guide envisions a marketplace that uses open architecture, open business practices and transparency to attract new companies and innovation to government. The Defense Information Systems Agency's app store is an example of this new approach. The store will allow employees to download and use apps immediately — even some they'd have to pay for on their personal devices.

Today, we all use smartphone apps for a range of activities, including banking, news, entertainment and health care. But it's important to note that young people entering the military and federal workforce who grew up as digital natives expect to find the speed, simplicity and immediacy of apps where they serve and work.

Constant connectivity offers app users new ways to co-create, buy, find, meet and interact, and even enables service members in harm's way to exchange views of the battlefield and other intelligence. Offering a marketplace with commercial and military-developed apps allows users to vote on the most useful apps with their downloads and comments, and to send clear, direct signals about what else they need.

In addition to the app store, DISA is unveiling an IT storefront that will allow users to securely buy IT as they would online: directly, easily and quickly. The user experience will be frictionless, and little procurement processing will be involved, which means DISA will have added relatively little strain to the already stretched contracting corps.

Office of Federal Procurement Policy Administrator Anne Rung and Federal Acquisition Service Commissioner Tom Sharpe are working together on initiatives to provide full-service strategic sourcing and category management capabilities. Those efforts dovetail with the AOF guide's description of future buyers. AOF anticipates a data-enabled team freed by vastly expanded strategic sourcing and category management to focus on mission outcomes rather than just support and process.

Rung leads the Strategic Sourcing Leadership Council, which is made up of the federal agencies that are the biggest buyers. The group has approved 10 "super categories" of commonly bought products and services for management — including IT, transportation, travel and professional services — in an effort to broaden strategic sourcing.

By managing those categories from a governmentwide perspective, the goal is to use data and greater demand to drive down prices and eliminate duplicative contracts. Senior executives will manage categories that focus on price, buying trends, cost drivers, innovation, and emerging companies and capabilities in their markets.

That approach aligns with the AOF guide's vision of future acquisition teams that are aware of market conditions, understand supplier capabilities and incentives, are immersed in their agency's mission, and consider all the external forces shaping it. This vision of highly sophisticated buyers also includes fingertip access to clean, accurate, governmentwide acquisition data already analyzed and visualized using artificial intelligence to support decision-making.

It is encouraging to observe that OFPP and the General Services Administration already are working on making this future a reality.

Other instances of forward-leaning IT buying techniques abound. They include the National Geospatial-Intelligence Agency's GEOINT App Store; the Defense Department's forthcoming marketplace for ground control systems for unmanned aerial vehicles; and 3D printing in medical, military and space programs.

Seeing tomorrow

Isolated experiments, of course, have come and gone for decades while federal acquisition remains data-deprived, rule-bound, risk-averse, overly regulated, and unable to consistently meet expectations for delivering new and expanded types of mission value. But with a vision, a common language, a guide, and a place to collaborate and share, today's experiments have a real shot at evolving into what the acquisition community truly aspires to deliver.

So that brings us back to AOF and its continuously adapting, annotatable guide that enables leaders to chart their course rather than impose static conditions on acquisition's evolution.

Soon the AOF Transformation Guide and collaboration site will be available for public view, comment, annotation, and posting of examples and lessons learned on a website hosted by ACT-IAC. If you'd like an early glimpse and want to be notified of the launch date, sign up at AcquisitionoftheFuture.org.

It's time to build the future of federal acquisition — together. ■

Kymm McCabe is CEO of ASI Government, which provides support, research, education, news and tools to more than 45,000 federal acquisition professionals at 130 organizations through the company's Virtual Acquisition Office and Applied Learning Online.

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.

PUBLIC SECTOR
MEDIA GROUP

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

BackStory

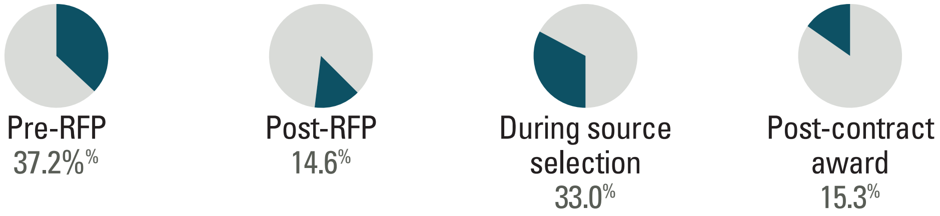
Hurry up and wait

Most agencies are all too familiar with the pain of procurement delays. Here's what they look like from industry's perspective.

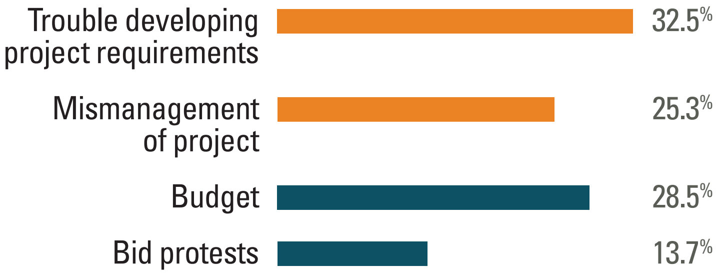
88.5%

of companies say their projects are frequently delayed.

The delays pop up at every stage of the process...



...and poor project management is the most common cause.



The end result?

- Layoffs
- Starting the discussions sooner
- Putting off investments
- Building delays into the planning process
- Shuffling staff between projects
- Scaling back on government bids
- "You really can't do anything but wait"

Washington Technology

This data is drawn from Washington Technology's most recent Insider Report, "The Pain and Peril of Procurement Delays." The full report is available to WT Insider subscribers at WashingtonTechnology.com.