



THE BUSINESS OF FEDERAL TECHNOLOGY



## Help secure your world using the power of the AT&T network

Innovative and comprehensive security services

- Increase situational awareness
- Monitor and identify threats/vulnerabilities
- Gain actionable cyber intelligence

For cyber protection from a trusted source, visit [att.com/gov/cyber](http://att.com/gov/cyber)



© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the Globe logo and all other AT&T marks are trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.



# Investing in innovation to support your mission success...



and empowering government with integrated solutions to connect, protect, virtualize and manage

- Mobility services and applications
- Internet of Things (IoT) solutions
- IP-VPN
- Network on Demand
- Cloud
- Cybersecurity
- Voice over IP
- Unified Communications

For more information, go to [att.com/gov](http://att.com/gov)



- 12** NASA brand management
- 14** CMS' open-data strategy
- 15** Recruiting like Google
- 16** Enterprise risk management
- 17** Interior's Instagram success
- 19** US-CERT's rapid response
- 20** GSA's telecom plan
- 21** Online accessibility standards
- 22** Spectrum sharing
- 23** IFTTT in practice
- 24** Fog computing
- 25** Derived credentials



## How it works

To thrive in federal IT, you need to know more than technology







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

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

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



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

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

WALTER E. WASHINGTON CONVENTION CENTER

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

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

**EDUCATION TRACKS INCLUDE:**

- Achieve Mission Outcomes
- Strengthen Enterprise Management

**SESSION TOPICS WILL INCLUDE:**

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

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

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

**GovEAconference.com**

USE PRIORITY CODE: EAE15

PRESENTING SPONSORS



EVENT SPONSORS



PARTNERING MEDIA



PRODUCED BY



## Untold lines of code make Pentagon weapons vulnerable

Weapons systems remain vulnerable to hacking despite the billions of dollars the Defense Department spends annually on cybersecurity, Pentagon officials have acknowledged.

There are 9 million lines of code in the F-35 joint strike fighter jet, plus 15 million lines in support systems, said Richard Stiennon, chief research analyst at IT-Harvest. Cleaning up all the code in the weapons systems being produced for DOD would cost hundreds of billions of dollars, he added.

"In other words, if we ever go to war with a sophisticated adversary or have a battle, they could pull out their cyber weapons and make us look pretty foolish," he said.

Big weapons are, in essence, big computers because of their reliance on IT, and that reliance is a boon for potential adversaries, said Carl Herberger, a former electronic warfare officer in the Air Force.

"From an adversarial perspective, [what is] really wonderful about this issue is that they really get to level the playing field in a way" that would not otherwise be possible, added Herberger, who is now vice president of security solutions at Radware.

Furthermore, a U.S. government document leaked by former National Security Agency contractor Edward Snowden alleges that Chinese hackers have stolen terabytes of data on the F-35.

Frank Kendall, undersecretary of Defense for acquisition, technology and logistics, has made cybersecurity in weapons a key piece of Better Buying Power 3.0, the latest round of acquisi-



"Many of the things that are in the field today **were not developed and fielded with cybersecurity in mind.**"

— FRANK KENDALL, DEFENSE DEPARTMENT

tion guidance to all DOD components.

"Each service, each program has got to go through and ensure that the fielded systems, as well as the ones in development, are as secure as we can reasonably make them," he told reporters recently. "Many of the things that are in the field today were not developed and fielded with cybersecurity in mind."

Each military branch's component of Cyber Command has a role in trying to make weapons systems more secure. Lt. Gen. Edward Cardon, head of Army Cyber Command, said in a

recent interview that he was concerned by the cyber vulnerabilities inherent in weapons systems. However, many Army systems, such as tanks, can still operate in a "degraded mode" if hacked, Cardon said, adding that the same might not be true for aircraft and ships.

"There's growing recognition that [we, as a society, are] hooking things up to the Internet that we never intended to

hook up to the Internet," Cardon said.

Monetary help could be on the way from Congress. The Senate Armed Services Committee recently approved a fiscal 2016 defense policy bill that would authorize \$200 million for "a new initiative to enable the services to begin evaluating all major weapons systems for cyber vulnerabilities," according to a markup summary.

Faced with such a daunting challenge, the operative word might be "begin."

— Sean Lyngaas

### FCW CALENDAR

**7/23** **Defense IT**  
Washington Technology's DOD Industry Day will explore the top 10 defense opportunities and detail the major acquisition vehicles for 2015 and beyond. Falls Church, Va.  
[http://is.gd/WT\\_DOD\\_IT](http://is.gd/WT_DOD_IT)

**7/29** **Data Act**  
ACT-IAC will host a professional development event focused on the technical and cultural challenges — and performance and open-data benefits — of implementing the Data Act. Washington, D.C.  
[http://is.gd/FCW\\_DataAct](http://is.gd/FCW_DataAct)

**RISEINGSTAR**  
AWARDS

### FINAL DAYS!

Nominations for the 2015 Rising Star awards are due July 9. Submit yours at [fcw.com/2015risingstars](http://fcw.com/2015risingstars).

# Contents



## 12 **COVER STORY** How it works

To thrive in federal IT, you need to know more than technology

- 12 **NASA: A good story well told**
- 14 **Better health care by way of open data**
- 15 **Google-style recruiting — even in government**
- 16 **What exactly is enterprise risk management?**
- 17 **The secret of Interior's Instagram success**
- 19 **How US-CERT gets the word out**
- 20 **How EIS will address increasing telecom complexity**
- 21 **How online accessibility standards should get set**
- 22 **A short history of spectrum sharing**
- 23 **IFTTT: Your digital duct tape**
- 24 **Why 'fog computing' is key to the IoT**
- 25 **How derived credentials make real mobility work**

## TRENDING

### 3 **DEFENSE**

Untold lines of code make Pentagon weapons vulnerable

### **FCW CALENDAR**

Where you need to be next

### 6 **OVERSIGHT**

Acting IGs run the risk of being 'more lapdog than watchdog,' and DISA is redoing content delivery

### 7 **PROCUREMENT**

OFPP issues guidance on reverse auctions. Plus, Editor's Note: The final days for Rising Star nominations.

## DEPARTMENTS

### 10 **COMMENTARY**

What smart succession planning requires

BY PAUL WILSON

What cyber insurance can do for contractors

BY JUSTIN CHIARODO AND PHILIP BESHARA

### 26 **CIO PERSPECTIVE**

Improving the skills of your IT staff

BY RICHARD A. SPIRES

### 41 **FCW INDEX**

### 42 **BACK STORY**

Worth a thousand words

### **SPECIAL REPORT FROM WASHINGTON TECHNOLOGY**

## **How the biggest contractors have adapted**

Acquisitions, reorganizations and investments are everywhere as key companies prepare for a return to growth in federal IT

**Page 28**



**Editor-in-Chief** Troy K. Schneider

**Executive Editor** John Bicknell

**Managing Editor** Terri J. Huck

**Senior Staff Writer** Adam Mazmanian

**Staff Writers** Sean Lyngaas, Zach Noble,  
Mark Rockwell

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

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

**Vice President, Art and Brand Design**

Scott Shultz

**Creative Director** Jeff Langkau

**Assistant Art Director** Dragutin Cvijanovic

**Senior Web Designer** Martin Peace

**Director, Print Production** David Seymour

**Print Production Coordinator** Lee Alexander

**Chief Revenue Officer** Dan LaBianca

## PUBLIC SECTOR MEDIA GROUP

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

**Co-President and Chief Content Officer**  
Anne A. Armstrong

**Chief Revenue Officer**  
Dan LaBianca

**Chief Marketing Officer**  
Carmel McDonagh

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

### Art Staff

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

### Print Production Staff

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

### Online/Digital Media (Technical)

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

### Lead Services

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

### Marketing

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

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

### OTHER PSMG BRANDS

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

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

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

**Federal Soup**  
*Managing Editors* Phil Piemonte,  
Sherkiya Wedgeworth

**THE Journal**  
*Editor-in-Chief* Christopher Piehler

**Campus Technology**  
*Executive Editor* Rhea Kelly



**Chief Executive Officer**  
Rajeev Kapur

**Chief Operating Officer**  
Henry Allain

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

**Executive Vice President**  
Michael J. Valenti

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

**Chairman of the Board**  
Jeffrey S. Klein

## SALES CONTACT INFORMATION

### MEDIA CONSULTANTS

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

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

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

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

### EVENT SPONSORSHIP CONSULTANTS

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

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

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

### MEDIA KITS

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

### REPRINTS

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

### PARS International

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

### LIST RENTALS

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

### SUBSCRIPTIONS

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

### REACHING THE STAFF

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

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

### CORPORATE OFFICE

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

## DISA is redoing content delivery

The Defense Information Systems Agency is gradually changing the way it delivers Web content across the global Defense Department telecommunications network, starting with a recently awarded contract to Hewlett-Packard and Akamai.

The new contract will help DISA begin to transition from the Global Content Delivery Service to a system that uses a unified platform, DISA Team Lead Terrace McCaa told FCW earlier this month.

The agency is still working out the requirements and funding for the new system, dubbed the Universal Content Delivery Service.

The contract with HP and Akamai, which DISA announced in April, has a \$469 million ceiling and will run through 2018 with an option for a three-year extension.

GCDS taps into hundreds of specially equipped servers to deliver Web content and applications across the department's unclassified, classified and coalition networks, according to DISA.

Meanwhile, UCDS will serve as a "unified platform that can accelerate and secure" all the content it delivers and will unite a diverse set of stakeholders within DOD's IT ecosystem, which includes end users, enterprise application owners and those in charge of cyber defense, said Larry Underhill, Akamai's director of custom government engineering.

He added that the goal of UCDS is to unite two key sets of technologies into a single service offering: content delivery networks and secure Web gateways. The gateways filter potentially harmful content, and the CDNs are a distributed set of servers that seek to deliver content smoothly to users.

— Sean Lyngaas

## Acting IGs: 'More lapdog than watchdog'

Extended vacancies in agencies' inspector general offices can put acting IGs in a difficult position, watchdog groups told lawmakers earlier this month.

Without a Senate-confirmed IG, agencies must make do with acting IGs, who can end up being "more lapdog than watchdog," Danielle Brian, executive director of the Project on Government Oversight, told members of the Senate Homeland Security and Governmental Affairs Committee.

Acting IGs have fewer protections and safeguards against being shuttled from one department to another, for example. Consequently, they might try to curry favor with agency leaders, which can undermine the independence that is essential for IGs to conduct effective oversight, Brian said.

The uncertain tenure of acting IGs can also lead to an avoidance of long-term investigations.

The Department of Veterans Affairs has been without a Senate-confirmed IG for more than a year and a half, the Labor Department for more than four

years and the Interior Department for more than six.

Daniel Epstein, executive director of Cause of Action, raised the question of whether IG positions have been left open for political reasons.

Having fewer independent IGs could enable the Obama administration to

pressure acting IGs into not pursuing investigations that could lead to embarrassing revelations.

The speakers at the hearing stressed the urgent need to streamline the recommendation and confirmation process, and Brian referred to the current administration's "general ambivalence" toward IGs.

The confirmation process takes far too long, said Michael Horowitz, IG at the

Justice Department and chair of the Council of the Inspectors General on Integrity and Efficiency.

He added that a simple title change from acting IG to deputy IG could extend an individual's tenure past the mandated 210-day limit, which has contributed to extended vacancies.

— Eli Gorski



The Project on Government Oversight's Danielle Brian told lawmakers that acting IGs lack the power of their Senate-confirmed counterparts.



**Phaedra Chrousos**  
@PSChrousos

So close @marydavie @cscairns! GSA agile RFP expected this week <http://fcw.com/articles/2015/06/02/gsa-agile-rfp.aspx> ... via @FCWnow

Reply Retweet Favorite

1:12 PM - 2 Jun 2015

### Join the conversation

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

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



## OFPP issues guidance on reverse auctions

The Office of Federal Procurement Policy has issued guidance reminding federal chief acquisition officers that although reverse auctions can result in lower prices for common goods and services, they must be used carefully.

In a six-page memo to senior procurement executives, OFPP Administrator Anne Rung described how best to apply the acquisition technique.

She promised to work with agencies to gather information — including prices paid for items, fees, number of bidders and levels of interactive bidding — to help build a digital library on reverse auctions for acquisition officers.

The memo also starts the ball rolling on incorporating information on the use of reverse auctions in the Federal Acquisition Regulation.

The guidance follows a December 2014 request from Reps. Jeff Miller (R-Fla.) and Sam Graves (R-Mo.) that OFPP look into opening a FAR case to address reverse auctions. Current House Small Business Committee Chairman Steve Chabot (R-Ohio) introduced legislation in March aimed at protecting small companies by requiring formal training for contracting officers who use reverse auctions, and prohibiting the use of reverse auctions for sole-source contracts.

In the past year, use of the General Services Administration's reverse-auction platform surged 1,000 percent, wrote Joan Kornblith, communications manager at GSA's Federal Acquisition Service, in a February blog post. From the first quarter of fiscal 2014 to the first quarter of fiscal 2015, auc-

tion sales rose from \$737,000 to \$10.8 million.

Studies by the Government Accountability Office have shown that reverse auctions have not been used effectively in some instances. Accordingly, Rung's memo advises that CAOs follow a number of best practices, such as determining whether reverse auctions are the best fit for a given acquisition, making sure to review data from prior auctions and addressing small-business participation.

She also recommends that procurement officers be aware of fees charged by third-party auction providers and work with them to set a fair fee structure, which could be based on a percentage of the transaction, a percentage of the savings or a flat amount.

— Mark Rockwell

### EDITOR'S NOTE

## Rising Star nominations: The final days

**Do you know someone** who is a Rising Star in federal IT? If so, be sure to nominate that individual today because we have extended the deadline for 2015 Rising Star nominations — but only by a week! And when the window for nominations closes at midnight ET on July 9, we want to have the best possible candidates for our judges to consider.

The Rising Star awards spotlight women and men who are having an outsized impact on federal IT and who show clear signs of being leaders in the community in the years to come. Nominees can work in federal agencies, private companies, academia or the nonprofit world. The only

restrictions are that they be actively involved in the community and in the first 10 years of their federal IT careers.

What makes for a winner? In

many ways, we follow the same criteria we use for the Federal 100 awards. We are seeking people whose leadership, innovation and all-around extra effort are having a powerful and positive impact on federal IT.

Here are some additional guidelines to keep in mind:

- This is an individual award. Teams are important, too, but we're looking for the women and men who power that collaboration.
- Winners go above and beyond, whatever their level or rank. A fancy job title is not required, and doing

one's job well is not enough.

- Impact matters. The judges need to know not only what a nominee did but also what all that work accomplished.
- The award is for work done in the past year. Future leadership potential is important, too, but one must have had clear accomplishments in the past 12 months.
- You can nominate multiple people, but only if you move fast!

So gather your information and supporting nominators, and get those nominations in by July 9.

Go to [FCW.com/2015risingstars](http://FCW.com/2015risingstars) to learn more, and then let us know where to find the leaders of tomorrow — and the rising stars of today.

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



# Software-Defined Storage: An Answer to Growing Data Needs

**A**s the volume of data explodes, and looks set to continue to grow for a long time to come, finding solutions for how to manage and store that data has become a major headache for organizations. Simply adding capacity is no longer an answer, and the turn to cloud computing and the use of more dynamic applications is clearly outstripping the capabilities of current storage arrays.

Software-defined storage (SDS) is one emerging answer. It provides the flexibility and automated management required in modern data center environments, while enabling IT managers to hold down costs by allowing them to use both existing systems and new commodity hardware to boost storage capacity.

As a part of the “software-defined everything” universe it’s suffered a bit from the hype associated with that term, but it’s a real technology and management model that already has a substantial base. Researcher Market and Markets put the global 2014 market for SDS at \$1.41 billion, and expects a yearly average growth of nearly 35 percent for a total of \$6.22 billion in 2019.

In the past it’s been confused with storage virtualization, with which it shares some characteristics. However, whereas storage virtualization is used simply to pool storage resources so that all of an organization’s various systems are made to appear as a single storage resource, SDS goes several steps further by adding automation and monitoring tools. Many of the services now done in the storage hardware itself—such as deduplication, replication, snapshots,



encryption and thin provisioning—are in SDS, handled in software.

The Storage Networking Industry Association (SNIA) says SDS products need four specific capabilities in order for them to be worthy of the name:

- **Automation:** Simplified management that reduces the cost of maintaining the storage infrastructure.
- **Standard interfaces:** APIs for the management, provisioning and maintenance of storage devices and data.
- **Virtualized data path:** Block, file and object interfaces that support applications written to these interfaces.
- **Scalability:** Seamless ability to scale the storage infrastructure without disruption to availability or performance.

Ideally, the SNIA says, SDS solutions will allow applications and data producers to manage the treatment of their data by the storage infrastructure without storage administrators having to intervene, and will do it without any explicit provisioning operations and with automatic service level management.

## MANY DEFINITIONS, SAME MODEL

As with any new technology model, there are many ideas of what constitutes an SDS solution, but all of them are built on the same three, reinforcing principles: They can abstract data from the hardware they are stored on; they can integrate all of the storage, computing and networking environments they operate in; and they can manage everything through software.

The most popular definitions of an SDS solution all have the same two components: a control plane, and a data plane. The control plane understands those application-specific policies that govern such things as performance and availability, and then can migrate those down into the infrastructure without a storage administrator needing to get involved. Data planes usually contain both the familiar, decades-old external storage array technologies and the much newer software-based storage products.

The state of storage in most enterprises today can best be described as a mixed bag. Typically, storage has been acquired and assembled

without an overall plan, over time and according to the needs of various segments of the business or agency. By themselves, storage arrays will have the capability to store, manage and protect data. But, unless they all use the same proprietary technology, they don't have the same features and management models, and they can't interoperate.

That poses a big problem for modern enterprises, which require seamless, end-to-end IT environments that can manage the complex applications and services that users increasingly need to do business. That, in turn, requires a consistent operational model across all of the enterprise storage resources, something that will be even more important as organizations turn to the cloud to deliver those applications and services. In particular, they are expected to mainly use public-private hybrid clouds that will continually shift data from internal to external clouds, and that won't work without a common storage environment that works consistently across the two.

Providing for this as well as future storage demands will depend on how particular SDS solutions are implemented. VMware provides many of the server and network virtualization solutions employed by both industry and government, for example, and uses the same kind of techniques for abstracting the data in its SDS model, with storage services dynamically composed, aligned with changing application needs, and driven by policies surrounding those applications.

In that way, the company says, applications and what's needed to deliver them to users are paramount, and storage is managed in such a way as to respond to the dynamic requirements of those applications. Its SDS solution uses a "just-in-time" model where, unlike with traditional techniques that assign pre-provisioned storage to specific applications, storage and capabilities aren't provided until they are needed. The storage environment can change dynamically and automatically should the service level requested also change.

## COST, MANDATES ADD URGENCY

The truth is organizations are under both external and business-driven needs and internal cost-driven pressures to consolidate IT infrastructures, while also providing flexible environments that can meet both current and future user requirements.

Federal government agencies, in particular, are mandated to cut the number of data centers they operate, as a way to slash overall IT operating costs. The Obama administration's 2010 Federal Data Center Consolidation Initiative (FDCCI) required 1,200 government data centers to close by 2015. At the same time, however, data volumes and storage demands continue only to grow. Another government mandate, requiring agencies to think "Cloud First" for any new application or service they acquire, will also add to storage requirements.

Overall, the information that's being created by digital technologies is roughly doubling every 18-24 months, and storage needs are growing anywhere between 20-40 percent a year. Meantime, the budgets set aside to cope with these storage demands are growing by single digits, if at all. Marrying cost-effectiveness with sophisticated management and capacity techniques has become the paramount need for storage.

SDS is drawing increased interest because its attributes span the full breadth of these needs:

- **Cost:** SDS is fully automated so requires no manual intervention by IT staff, which allows organizations to more effectively use those resources. Head count is typically the largest cost for any IT organization, so the constant push is to produce simpler environments that require less people to manage. They can also use their existing storage hardware while incrementally adding capacity with low-cost commodity hardware, and thus keep a handle on capital expenditures.

- **Efficiency:** SDS significantly reduces the number of steps needed to operate traditional storage environments because of its embedded automation. It improves the stability of that environment since the management software is no longer linked to any specific piece of hardware that may fail. As capacity can be more finely matched to demand, that cuts down on over-provisioning which frees unused storage capacity for other needs.

- **Flexibility:** Application storage requirements change over time, sometimes dramatically given what the application is used for, and SDS environments can respond to that immediately and automatically. New applications will only become more dynamic, requiring faster and more frequent reactions from IT environments than legacy applications have typically needed, which SDS can seamlessly provide.

SDS also speaks directly to changes in storage technology itself, with flash storage getting cheaper and, at least for some uses, quickly replacing disk-based storage. It's also migrating out of the traditional storage array, onto the server bus and from there onto the server motherboard. This kind of storage can cost a half to one-third that of array-based storage and organizations are starting to understand the attraction of this kind of server-based storage.

"Software-defined" may be a buzz phrase, but in fact it describes very well what will have to become the standard for most IT environments, because traditional static technologies and models simply can't keep pace with increasing—and increasingly variable—demands. With the amount of data being created, it's no coincidence that storage is typically the number one IT expense for any organization. Software-defined storage is well positioned to be the solution to that.

vmware®

For more information on VMware Virtual SAN, please visit [www.vmware.com/go/VSAN](http://www.vmware.com/go/VSAN)



# What smart succession planning requires

Leadership changes don't have to be painful.  
Here are some tips for easing the transition.

President Barack Obama is pushing to attain next year's agency priority goals before the end of his presidency, but the administration's succession planning actually began more than two years ago.

Although change is not always ideal, having a framework in place to successfully transition critical roles continues to be a key consideration for government agencies and leaders.

Think about the following hypothetical case study: The branch leader for financial analysis at an agency office announces his intention to retire in two years. A year before the retirement date, a succession analysis reveals that performance would improve if the next branch leader possessed advanced data analytics skills and cloud-sharing abilities.

Therefore, a list of succession candidates is generated with a focus on that particular skills gap.

Ultimately, an individual is selected for promotion. However, when the branch leader retires, the selected successor is transitioning out of the government workforce. The exit interview reveals that the employee would have stayed had she known about the potential promotion.

What went wrong? Simply put, there was a communication failure. Because the agency did not tell the employee about its intention to promote her, she was unaware of the potential and thought she had to leave the agency to take the desired next step in her career.

The communication gap resulted in the agency having an undesired staffing vacancy and potentially hiring a less skilled or less recognized person for the role.

Organizational and leadership change is inevitable; therefore, it is crucial to have a succession strategy in place that meets the needs of

Employee engagement, retention and recruiting are just a few areas of concern associated with major organizational transitions.

your organization while maintaining high-level productivity and mission-critical success.

To create a successful succession plan:

- Clarify the organization's mission and future service needs.
- Identify competencies required to support the vision.
- Develop a set of successors based on the current leadership structure.
- Assess and analyze critical skills gaps and flight risk.
- Monitor and evaluate organization and succession candidates.
- Create a training and development process.
- Outline, implement and evaluate

the transition plan on an ongoing basis.

Yet while preparing those key elements can alleviate pain points in organizational transitions, there are also caveats to be aware of when implementing an effective plan. Especially within the federal government, leadership changes happen more often than not. Employee engagement, retention and recruiting are just a few areas of concern associated with major organizational transitions.

It is important to also consider these lessons learned:

- **Don't keep secrets.** As stated in the case study, let employees know of any happenings within the organization, especially involving leadership. Change provides a chance to build a trusting, committed and confident workforce.
- **Stick with the plan.** Time and budgets are precious, so if you dedicate time to developing a transition plan and communicating goals internally, don't deviate unless organizational requirements change.
- **Develop talent pools.** Strong talent pipelines are the best way to retain top talent and improve recruitment efforts. By neglecting potential candidates, agencies risk missing out on the most qualified applicants.
- **Build successors in all roles.** A change in top leadership is not the only thing to consider. Other transformational roles are equally important to remain a high-performing agency. ■





# What cyber insurance can do for contractors

When it comes to cybersecurity, the SAFETY Act deserves a second look, but companies should also consider commercial coverage

Cybersecurity compliance for government contractors is an ever-growing challenge. Companies face current and emerging obligations arising from a patchwork of executive orders, standards from the Office of Management and Budget and the National Institute of Standards and Technology, rulemaking in the Federal Acquisition Regulation and agency supplements, contract terms, and legislative action (and inaction).

But how well is your business financially protected in the event of a cybersecurity incident? (Or if you are on the government side, how safe are your industry partners?)

The financial costs of cyber events can be staggering. The highly publicized attack on Target cost the retailer and financial institutions a reported \$348 million. And for government contractors, the implications can be existential. In 2014, a high-profile provider of background checks to the Office of Personnel Management fell victim to a suspected state-sponsored cyberattack that potentially exposed confidential information regarding 27,000 government employees.

OPM not only declined to renew the company's contracts (which in one year totaled \$417 million in revenue), but the contractor's parent company filed for bankruptcy, citing the cyberattack as a key cause.

Following a 2011 data breach at a major contractor for the military's Tricare health benefits program, the government required the company

to pay the costs of notifying 5 million affected Tricare recipients. On top of that, the contractor faced years of class-action litigation.

Those numbers reinforce the notion that contractors should focus not only on cyber compliance practices but also on ways to mitigate the financial impacts of inevitable cyber incidents. Those investments should complement more traditional cyber compliance measures (e.g., system security and training).

**Companies should take every advantage of the financial and liability safeguards currently at their disposal.**

Two such measures in particular are worth a closer look: corporate insurance and liability protections under the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002.

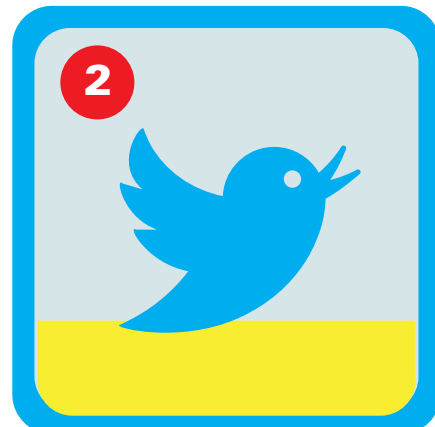
Although the cybersecurity insurance market is still evolving, contractors would be well-served to review their current policies. Advance review and planning will help identify potential coverage issues and gaps before a cyber event takes place, position contractors to maximize their potential recoveries in the event of a cyber incident and

even enable contractors to negotiate more favorable policy language to maximize their liability protections.

The SAFETY Act might also provide liability protections to approved businesses that use or provide approved products or services that can reach cybersecurity vulnerabilities. For example, FireEye recently announced that the Department of Homeland Security had certified two of the company's cybersecurity products as "qualified anti-terrorism technologies" under the SAFETY Act.

Government contractors and other businesses that use DHS-certified technology may cloak themselves in the law's protections, effectively avoiding the tort liability that can arise from a cyberattack when such technology is used. FireEye's DHS approval further confirms that the SAFETY Act's protections extend beyond terrorism concerns to include the cybersecurity threats facing American companies and, through them, U.S. economic and national security interests.

Those threats — particularly for government contractors — show no signs of abating. Contractors that are waiting for financial protection from federal regulators or Congress will likely be disappointed. Therefore, companies should take every advantage of the financial and liability safeguards currently at their disposal and include the assessment of those safeguards as an integral part of their cybersecurity strategies. ■



# NASA: A good story *well told*

The space agency's PR machine is second to none in the federal government.

The secret:  
"Don't suck all the fun out of what you do."

BY ZACH NOBLE

When it comes to connecting with the public — be it on Facebook, Twitter or the silver screen — there might be no federal organization that can equal NASA's success.

How does the agency generate so much goodwill on a relatively tight budget?

The answer lies in a bit of a paradox: following the rules but being flexible enough to roll with hashtags on Twitter and Michael Bay's leaps of logic.

## The power of saying 'yes' to Hollywood

"Don't suck all the fun out of what you do," said Bob Jacobs, deputy associate administrator for communications at NASA.

When it comes to movies, NASA

might have the cachet of space, but it lacks the outreach budget of, say, the Pentagon. Therefore, Jacobs said NASA's cinematic power lies not in aggressive outreach but in saying yes to almost everything it can.

Although the military is picky about the films it cooperates with, NASA has lent advice and support to a slew of movies that feature questionable — or flat-out wrong — science.

For instance, NASA helped with "Armageddon," the over-the-top asteroid movie that starts with the premise that it's easier to retrain oil drillers to be astronauts than it is to retrain astronauts to be drillers.

The wormhole adventure "Interstellar," "The Avengers," time-traveling "Men in Black 3" and cartoon "Planet



51” all received some support from NASA.

Even films that seem to feature hard, genuine science have their flaws, but refusing to let the perfect be the enemy of the good, NASA lends a hand.

“The science of ‘Gravity’ was way off,” Jacobs said, adding that NASA connected actress Sandra Bullock with an astronaut and talked up the movie on social media during the 2014 Academy Awards event despite the film’s imperfect science.

There are, of course, limits. NASA approves three to five scripts a year, Jacobs said, and rejects projects that don’t yet have funding lined up. Filmmakers can’t use a NASA endorsement to raise money.

When it can, however, NASA gives scientific input, its logo and other support to films, be they documentaries or superhero flicks, because “there’s value in the inspiration and excitement they create,” Jacobs said.

### Keeping the ‘social’ in ‘social media’

“I bet we have more [social media accounts] than anyone,” Jacobs said, citing NASA’s nearly 500 accounts on a

## NASA approves three to five scripts a year and rejects projects that don’t yet have funding lined up. Filmmakers can’t use a NASA endorsement to raise money.

dozen platforms. The agency is “still trying to figure out Snapchat,” he said, but NASA is a popular presence on Flickr (8,800 photos and counting, and that’s just the main account), Twitter (10.3 million followers, again just on the main account) and Reddit.

Separate social media accounts for specific space centers and program offices broaden NASA’s reach.

Just having accounts isn’t enough; you need to use them effectively, which NASA does.

The agency’s accounts participate in popular trends — like the Academy Awards — but its online popularity might have been best demonstrated dur-

ing the partial government shutdown in 2013, when Twitter users took it upon themselves to tweet space updates with the hashtag #ThingsNASAMightTweet.

NASA’s social media culture stands in stark contrast to that of some other government agencies.

The IRS, with the most in-demand website in government, has many social media accounts but only uses them to issue pre-approved information instead of interacting with taxpayers.

Jacobs said it’s important that feds recognize that “people expect to have a conversation [on social media]. It’s not just us transmitting to people.”

Social media is meant for engagement, not just a box to check off or another place to dump press releases, he added.

Before diving into a social media platform, Jacobs said agencies should ask themselves, “What problem am I trying to solve?”

### Following the law

The key to NASA’s social success lies in Section 203 of the National Aeronautics and Space Act of 1958, which requires NASA to “provide for the widest prac-

licable and appropriate dissemination of information concerning its activities and the results thereof.”

That mandate forced NASA to be open in a unique way.

“We were going to show you our successes and our failures,” Jacobs said, citing the televised triumph of the Apollo moon landing and the tragedy of the space shuttle Challenger explosion.

“NASA is practicing pure public affairs,” said Richard Jurek, marketing executive and coauthor of “Marketing the Moon: The Selling of the Apollo Lunar Program.”

Jurek’s obsession with space was fueled by watching rocket launches on TV as a kid, and he said part of the tremendous value of NASA’s successful outreach is that it inspires young people to pursue careers as engineers, scientists and astronauts.

Jacobs was quick to say NASA’s outreach isn’t meant to lobby for cash or even recruit talent. The agency is just following the mission to widely disseminate information about space work.

It’s much like a romantic paradox — your ex only wants you back when you stop trying so hard to win her back — and it’s a valuable lesson for other agencies.

“Every government agency is doing something for an audience,” Jurek said, and he urged agencies to find those audiences and engage dynamically with the public instead of merely promoting pre-approved messages.

“Yes, there’s a coolness factor to space, but there’s also a hell of a lot of wonkiness,” he said, noting that during NASA’s initial marketing push it didn’t benefit from space’s cachet, but rather had to convince a skeptical public.

Jacobs and Jurek said other agencies could find success by adopting open, engaging communication strategies and not being afraid to have a little fun.

“Audiences respond to stories and they respond to content,” Jurek said.

At NASA, “we have exciting, compelling stories to tell,” Jacobs said.

Still, social media success hasn’t been handed to NASA, he added. “A lot of it is elbow grease.” ■

# Better health care by way of open data

BY ADAM MAZMANIAN

Government data is changing what we know about the work doctors do and helping developers transform that data into useful tools.

For the second year in a row, the government has released information on how doctors and other providers are charging Medicare. Physician utilization data from the Centers for Medicare and Medicaid Services covers \$90 billion in payments to 950,000 providers, which gives developers the raw material to build tools that allow users to compare doctors on a number of criteria, such as services delivered and charges submitted.

Niall Brennan, chief data officer and director of the Office of Enterprise Data and

Analytics at CMS, said the data consists of 10 million distinct observations and builds on data released in 2014 to allow for comparisons over time. In addition, CMS released a dataset in April on prescriptions written by providers under Medicare Part D that allows for the comparison of health care providers by prescribing patterns.

“Now you can actually see every piece of care and every drug they prescribe,” Brennan said during the sixth annual Health Datapalooza conference earlier this month. “Is it perfect? No. Is it better than where we’ve been before? Absolutely.”

The push for price and prescription transparency is part of a larger Obama administration open-data policy and is designed to show consumers what health care delivery really costs.

“I’m ready to declare progress but not victory,” Brennan said. “I think a lot

of people think transparency is easy. You just kind of push the big ‘Release Data’ button and it gushes forth and it’s done.”

CMS was only “gingerly dipping its toes” into the open-data world when the first Health Datapalooza took place. That changed in 2013 with the release of the “chargemaster” list that revealed what hospitals were charging for common inpatient procedures and the rates at which Medicare paid claims. The data revealed wide disparities in charges for procedures, even within the same

metropolitan areas, and garnered pop-culture currency with a prominent mention on “The Daily Show.”

Brennan said he encountered some skepticism and fear at CMS as the agency moved to release more and more data. “We’ve deliberately adopted

an incremental strategy where the initial data releases were pretty modest, but we had to almost reassure people that the world wasn’t going to end if dataset x-y-z came out,” he said.

He added that although some data releases made big news, others flew under the radar.

“It’s a very market-driven process,” Brennan said. “We’ve released data that we thought was going to have a wow factor, and people have yawned, and we’ve released data where we thought people would yawn, and they’ve gone ‘Wow.’”

Those unpredictable responses have spurred even more releases.

“You almost have to err on the side of openness because we don’t necessarily know the value that others may derive from the datasets, especially when they’re combined with other data,” Brennan said. ■





# Google-style recruiting — *even in government*

Hire people who are better than you, and make sure they're smart and curious, says Google exec Laszlo Bock

BY BIANCA SPINOSA

Google is famous for its culture of work as play. Employees enjoy free meals, access to laundry facilities, bike repair and on-site doctors at the Googleplex. Not to mention the bouncy balls, Lego sets and bean bag chairs.

But hiring at Google is serious business. More than 2 million people apply each year, and the company selects about 7,000.

And in bad news for government, the battle for talent extends far beyond Google. In CareerBuilder's 2015 job forecast, 54 percent of employers surveyed plan to hire full-time IT employees in 2015. That's up from 29 percent in 2014.

The forecast found especially high demand for workers skilled in cloud, mobile, cybersecurity, and managing and interpreting big data. So agencies are going to have to fight for every candidate and cannot afford to make the wrong hire.

Laszlo Bock, Google's senior vice president of people operations, can't help with federal hiring regulations. But in his book, "Work Rules! Insights From Inside Google That Will Transform How You Live and Lead," Bock shares advice that any agency manager could use to find and hire better tech employees.

**1. Only hire people who are better than you.** Bock says every person he has hired is better than him in some meaningful way, whether it's analytics, counseling or finding cost-effective ways to do things.

## **2. Hire smart, curious people.**

Choose smart people who can learn and adapt to new situations, and don't weed people out based on their GPAs. Bock said good hiring isn't just about the biggest name or most clever software engineers. It's about finding people who will be successful in your organization. Google has shifted from hiring exclusively from elite colleges to accepting top graduates from state schools. "Curious people who are open to learning will figure out the right answers in almost all cases," Bock said.

**3. Give up power when it comes to hiring.** In other words, hire by committee. In a typical interview, a Google candidate meets his or her prospective

manager, a peer, and one or two people who would be working under the candidate. Google looks for qualities such as humility and conscientiousness.

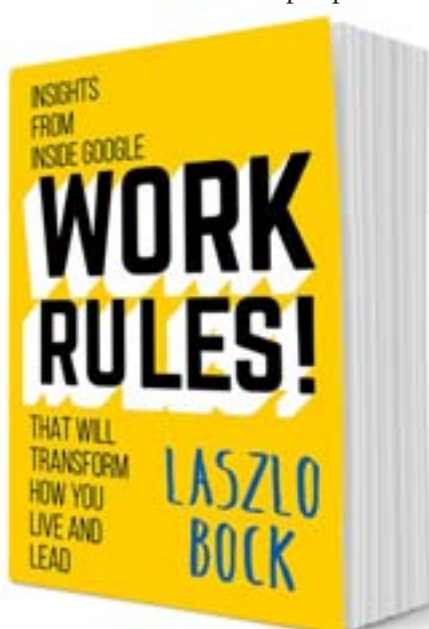
**4. Accept that hiring is an imperfect science.** Bock said most interviews are a waste of time because interviewers make their hiring assessments in the first three to five minutes of an interview or faster. Then they tend to convince themselves that the candidate they've selected is above average.

So what can be done about it? Google has found that behavioral interviews work best. That involves having the interviewer ask all candidates the same set of questions about how he or she has handled specific situations.

## **5. Find your own candidates.**

Social media is your friend! Thanks to LinkedIn, Twitter and other social networking sites, it's easy to find people. Many of the top IT performers are not actively looking for work because they are already employed, so reaching out through social media is an effective way to keep the lines of communication open.

**6. Bag the brain teasers.** Puzzlers such as "How many golf balls fit in a school bus?" or "Why are man-hole covers round?" might make the interviewer feel smart, but they don't necessarily predict anything about the potential employee and how he or she might contribute. Instead, ask questions that deal with problem-solving and leadership. ■





# What exactly is *enterprise risk management?*

It's more than simply rolling up the traditional risk management efforts — and it's increasingly critical for agencies

BY DOUGLAS W. WEBSTER AND THOMAS H. STANTON

*This article is adapted from the IBM Center for the Business of Government's recent report, "Improving Government Decision Making through Enterprise Risk Management."*

Often, the risk that hits an organization hard might not be the one that the organization was anticipating. As they have become more experienced in the application of basic risk management, the shortcomings of the traditional approach to managing risks in functional and programmatic silos have become more obvious. This has led to slow but ongoing progress toward

implementing the principles of enterprise risk management.

One of the earliest formal definitions of ERM was introduced by the Casualty Actuarial Society. In a 2001 report by its Advisory Committee on Enterprise Risk Management, CAS defined ERM as follows: "ERM is the process by which organizations in all industries assess, control, exploit, finance, and monitor risks from all sources for the purpose of increasing the organization's short- and long-term value to its stakeholders."

More recently, the Association for Federal Enterprise Risk Management

(AFERM) defined ERM as "a discipline that addresses the full spectrum of an organization's risks, including challenges and opportunities, and integrates them into an enterprisewide, strategically aligned portfolio view. ERM contributes to improved decision-making and supports the achievement of an organization's mission, goals and objectives."

Those definitions are instructive, in part because they point out that ERM is more than simply "good" risk management as traditionally practiced in silos. AFERM's definition references "the full spectrum of an organization's

However, such a comprehensive view of risk will not emerge simply from a bottom-up aggregation of risks identified within functional and programmatic silos. The need to incorporate risk management into the strategic planning process is an inherent part

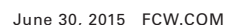
Another shared aspect of those definitions is that they position ERM not as an end unto itself but rather as an element of a broader objective. Risk management is simply an element of effective organizational management, and the AFERM definition reflects the tie of ERM to improved decision-making and

Finally, the AFERM definition indicates that ERM enables a portfolio view of organizational risks. Just as a portfolio of personal financial investments is intended to maximize the risk-adjusted return on investment for retirement planning, so, too, treating an organization's array of products and

Social media is easier said than done for federal agencies, but the Interior Department's Instagram account is the very picture of success

The Instagram account, which had more than 1,800 posts as of press time, is meant to inspire American and foreign tourists to travel to the country's natural wonders.

Interior has also used the Instagram account to make its case for funding in tight fiscal times. "Every dollar invested in the National Park Service returns \$10 to the U.S. economy" reads a caption below a photo of one of the Cathedral Lakes at Yosemite National Park. ■



services — and balancing resources against performance objectives and risks across that portfolio of products and services — serves to maximize long-term organizational stakeholder value.

### **Evolution of ERM in the federal government**

Although the concepts of ERM outlined above have been maturing in the private sector for the past two decades, their introduction into the public sector is more recent. What is believed to have been the first enterprisewide implementation of ERM in the federal government happened at the Office of Federal Student Aid (FSA) in the Education Department.

In 2004, FSA hired a chief risk officer (CRO), Stan Dore, who is believed to have been the first person in the federal government to fill such a position. FSA formally approved the creation of a dedicated ERM office early in 2006. Since those initial efforts, FSA has continued to mature its ERM processes and organization.

In 2008, Doug Webster, a co-author of this report, was serving as the chief financial officer at the Labor Department. With a strong belief in the value of ERM, he reached out to other federal executives who shared that inter-

est. Early in 2008, this informal group established itself as the Federal ERM Steering Group and joined with George Mason University to convene the first Federal ERM Summit.

That annual event has been held every year since and has become the key event for bringing together those interested in ERM in the federal government. In 2011, the Federal ERM Steering Group was formally incorporated as the aforementioned AFERM.

Despite the impetus provided by AFERM and its annual summits, progress in the federal government was initially slow. In the Association of Government Accountants' annual Federal CFO Survey in 2010, five federal executives were noted as having a formal risk management process at their agencies, including the designation of a CRO to facilitate ERM.

Although that certainly represented progress from FSA's initial appointment of a CRO, the surveyed organizations represented a small portion of the federal government. Moreover, meaningful progress was impeded because conflicting messages were being sent about the true meaning of ERM.

For example, in the Association of Government Accountants' 2011 Federal CFO Survey, 50 percent of respondents indicated that they believed that ERM

was adequate at their organizations. However, one respondent said, "We have risk management committees of senior executives and subject-matter experts aligned with each portion of our financial balance sheet. They recommend actions to a national risk committee to evaluate the risks."

That statement reflects a common misunderstanding of the differences between a functional risk (e.g., financial reporting) and meaningful ERM.

Although the principles of ERM may be applied within a functional area to manage risk (such as impacts to reliability in a balance sheet), that approach does not represent the principles of ERM applied across an agency. In that same study, only 29 percent of respondents said there was a designated risk management office or operation at their agencies.

Given the lack of a central coordinating risk management office, this begs the question of whether a meaningful ERM program was in place. As the authors of this report have sought to explain in describing ERM, there is a need for a central office or function generating centralized risk management policy, establishing cross-functional risk management processes, facilitating collaborative risk management discussions and prioritizing risks.

## **Distinguishing characteristics of ERM**

The Risk and Insurance Management Society has identified seven characteristics that yield insight into what constitutes enterprise risk management:

- Encompasses all areas of organizational exposure to risk (financial, operational, reporting, compliance, governance, strategic, reputational, etc.).
- Recognizes that individual risks across the organization are interrelated and can create a

combined exposure that differs from the sum of the individual risks.

- Prioritizes and manages those exposures as an interrelated risk portfolio rather than as individual silos.
- Evaluates the risk portfolio in the context of all significant internal and external environments, systems, circumstances and stakeholders.
- Views the effective management of risk as a competitive advantage.
- Provides a structured process for

the management of all risks, whether those risks are primarily quantitative or qualitative in nature.

- Seeks to embed risk management as a component in all critical decisions throughout the organization.

Those characteristics clearly distinguish ERM from practices that are sometimes incorrectly understood to be ERM.

— Douglas W. Webster and  
Thomas H. Stanton



In 2011, the term ERM might have been more broadly recognized than the understanding of the underlying concepts, but organizations have since sought to improve on that understanding. The winter 2013 edition of the Armed Forces Comptroller, the journal of the American Society of Military Comptrollers, focused largely on ERM, thereby helping to spread the word in that community.

An additional effort aimed at helping inform the federal community about ERM principles and practices was the

publication of the book “Managing Risk and Performance: A Guide for Government Decision Makers” (Wiley, 2014), co-edited by the authors of this report.

Despite the initially slow progress and misunderstanding of the term “ERM,” concrete progress is now demonstrably underway. In the book just referenced, the last of 10 recommendations offered for the federal government was to “incorporate ERM explicitly into Circular A-11 and [Office of Management and Budget] reviews of agencies.”

On July 25, 2014, OMB released an update to Circular A-11 (its annual guidance to agencies on the preparation of their budget submissions) that recognized ERM as an important practice for managing agency risk.

### OMB's efforts to encourage an ERM approach

OMB's current interest in ERM has evolved over time but became more evident early in 2013. OMB began working with the Government Accountability Office to provide input on an update

## How US-CERT gets the word out

The U.S. Computer Emergency Readiness Team collaborates with other federal agencies and industry to quickly disseminate cyberthreat alerts

BY SEAN LYNKAAS

When a major vulnerability hits the Web, it is the U.S. Computer Emergency Readiness Team's job to sound the alarm as quickly and effectively as possible. And given Heartbleed, Shellshock and other menacing revelations, US-CERT has had plenty of clamoring to do in the past year or so.

Internet users can subscribe to four separate US-CERT mailing lists, with “alerts” being the most urgent. Those alerts often include descriptions that are not overly technical so that a non-geek can understand them and take remedial security steps.

For instance, the alert for Heartbleed, the OpenSSL flaw discovered in April 2014, states: “This flaw allows a remote attacker to retrieve private memory of an application that uses the vulnerable OpenSSL library in chunks of 64K at a time.”

Users can rate the helpfulness of the alert as “yes,” “no” or “somewhat” at the bottom of each update. That feedback is presumably factored into how future alerts are crafted.

Although US-CERT is one of the main disseminators of threat information, it does not work alone. As part of the Department of Homeland Security's

National Cybersecurity and Communications Integration Center, the team has tapped the FBI, the Financial Services Information Sharing and Analysis Center, trusted private firms and a Canadian cyber response center for help in preparing alerts.

Like other federal offices that handle cybersecurity, US-CERT's effectiveness rests on breaking down bureaucratic barriers so that it can act more quickly on threats, which can spread like wildfire.

US-CERT Director Ann Barron-DiCamil-

lo said in a recent interview that industry is always interested in getting information more quickly and with greater context. Therefore, her team is working with intelligence agencies to strip relevant data from classified reports, she added.

Top-secret intelligence reports on cyberthreats contain technical data that is not classified, and separating that information “has been a huge focus, and it's really helping with the timeliness as well as richer content associated with what we're sharing,” she said. ■

to Standards for Internal Control in the Federal Government (commonly known as the Green Book) and to consider how evolution of the Green Book might influence internal controls policy reflected in OMB Circular A-123, Management's Responsibility for Internal Control.

With the release of the exposure draft on internal controls by GAO in fall 2013, OMB sought to encourage a more robust consideration of risk management than the check-the-box compliance attitude sometimes seen at federal agencies. The awareness of ERM was at least partly respon-

sible for the effort to move beyond a focus on internal controls in A-123 to a broader view of risk management.

The next version of A-123 (at the time this report was published) is thus expected to broaden the role of A-123 beyond internal controls to include other aspects of risk management.

In parallel with those developments, in 2013, OMB asked the CFO Council for suggestions on what OMB and the CFO Council might focus on as initiatives in the coming year. The No. 1 suggestion from the CFO Council was ERM.

CFOs felt they were doing a good job of financial management and risk management within financial management but were struggling with other types of risk. OMB thus started a working group on ERM under the CFO Council. One result of this working group was to convene a CFO Council forum.

The forum had most of the CFO Council in attendance and was both an educational discussion of the meaning and practices of ERM and a discussion of next steps in the council's engagement with ERM.

In October 2014, OMB Controller David Mader said during a panel discussion that "we have begun talking about how do we think about risk more broadly than just financial risk? I think when you look at [circulars] A-11 and A-123, those were all born out of the CFO Act. So everyone is narrowly focused on 'Well, it's about financial risk and it's about internal controls.' What we are doing now is stepping back and thinking isn't there really a way to take the lessons learned and what we've accomplished with A-11 and A-123 and broaden that perspective across the entire organization, particularly around mission programs?"

Mader went on to state that OMB believes there needs to be an enterprise risk protocol across government and that OMB would provide that guidance late in 2015. ■

*Douglas W. Webster is a senior fellow at George Washington University's Center for Excellence in Public Leadership, where he teaches enterprise risk management. He is also director of government-to-government risk management at the U.S. Agency for International Development and founder and former president of Cambio Consulting Group. Thomas H. Stanton teaches at Johns Hopkins University. He is also president of the Association for Federal Enterprise Risk Management and a former member of the federal Senior Executive Service.*

# How EIS will address increasing telecom complexity

BY MARK ROCKWELL

In 1988, the General Services Administration's Federal Telecommunications System contract incorporated just six services. Its successor, FTS 2001, had more than 20. Now in a sign of how the smartphone has revolutionized telecom services, GSA's next-generation \$50 billion, 15-year Enterprise Infrastructure Solutions contract has 54.

EIS anchors GSA's Network Services 2020 strategy and will replace Networx, which had to connect to 15,000 wire centers in the lower 48 states, said Fred Haines, GSA's program manager for the EIS acquisition. Only a few companies — such as Verizon, AT&T and Century-Link — could make all those physical connections, which limited the pool of providers.

EIS aims to take a different path with NS2020 as telecom continues to evolve from landlines and switching centers to the Internet, IP and beyond.

To make that transition, the EIS contract will have:

- **Fewer entry requirements to attract nontraditional bidders.** Haines said "dark

horse" companies such as Amazon Web Services could be interested in entering the competition because of the looser requirements.

- **Fewer predefined contract line item numbers.** The term is arcane but important because CLINs are central to federal agencies' service ordering. CLINs lock down the services providers must make available and force them to adhere to specific requirements, possibly at the expense of more innovative options.

- **Reduced contract modifications and more flexibility for buyers.** GSA will delegate procurement authority to agency contracting officers, who will be able to create task orders for line items. The move will streamline the process so agencies can get what they need faster. The added authority will also allow providers to more quickly tailor solutions to specific needs.

- **On-ramp capabilities.** The streamlined contracting process will allow vendors to add innovative solutions more quickly, which Haines said might be the path that nontraditional providers take as EIS progresses. ■

# How standards *should* get set

Inside the push to settle on a global standard for online accessibility

BY KAREN S. EVANS

The role of federal CIOs includes a multitude of critical responsibilities: compliance, procurement, records management, privacy and security, as well as bringing mission-supporting technology to employees and the citizens they serve. To deliver on those core obligations, CIOs must ensure that the services they manage are accessible to all, including users with disabilities.

Throughout my 28-year career in government, our commitment to accessibility for all users was unwavering. Yet the alphabet soup of accessibility requirements is complex and slows the ability to provide services that meet the latest standards. Settling on a global accessibility standard would reduce friction between competing standards and create a more efficient path to accessibility, both in the U.S. and abroad.

Section 508 of the Rehabilitation Act seeks to ensure that all the federal government's electronic and information technology is accessible to people with disabilities. It governs any technology the government develops, procures, maintains or uses. Harmonizing our accessibility requirements — specifically the U.S. Access Board's proposed Information and Communication Technology (ICT) Standards and Guidelines with the similar European standard EN 301 549 — would improve accessibility.



**It is time we adjust our policies to reflect the need for strong international standards and meet the evolving needs of today's federal technology landscape.**

It would create a global standard and minimize conflicting interpretations and market confusion while providing cost savings for governments, consumers and industry.

#### **Updating policy for the global stage**

The need to harmonize U.S. and European policies is a product of the growing

international influence of and increased accommodation for those with disabilities. Section 508 of the Rehabilitation Act was adopted in 1986, at a time when the international regulatory climate was far different than it is today. For instance, that was seven years before the establishment of the European Union.

It is time we adjust our policies to reflect the need for strong international standards and meet the evolving needs of today's federal technology landscape.

The European standard went through a rigorous approval process and was developed using recommendations from the Telecommunications and Electronic and Information Technology Advisory Committee. That international committee, founded by the U.S. Access Board, influenced both the European standard and the U.S. Access Board's proposed rule.

The two accessibility standards are closely aligned and seek the same functional outcomes. Yet despite the similarities, there is still room for confusion. In my experience, all it takes are minor differences to increase disparities between interpretation and execution in the ICT community.

#### **Our worldwide presence**

Now that the U.S. Access Board's proposed rule to refresh Section 508 has cleared its 90-day public comment period, the federal government should

consider its global reach and user base. The departments of Homeland Security and State, for example, are just two of the many U.S. government entities with a global presence. Harmonizing our accessibility standards with the European standard would ensure that our outposts abroad are outfitted with ICT infrastructure and services that are fully compatible with local accessibility requirements.

As our world becomes more connected, a universal standard is not only sensible but efficient. In fact, current law and Office of Management and Budget rulemaking support the adoption of such standards.

The National Technology Transfer and Advancement Act of 1995 and revised OMB Circular A-119 mandate the incorporation of voluntary consen-

sus standards as domestic standards where possible.

The use of consensus standards in place of unique standards, unless illegal or impractical, makes maintaining those standards easier for public-sector CIOs and federal government employees while also making it easier for users with disabilities to access information.

### A call to action

The harmonization of the U.S. proposed rule and the European standard would greatly benefit those who need better ICT accessibility. As the U.S. Access Board's proposed rule moves into a review stage, it is critical that federal CIOs and citizens alike support accessibility for all by calling for much-needed global harmony.

With updates to its proposed rule, the

U.S. Access Board could facilitate the creation of a global accessibility standard, thereby ensuring that government employees, people with disabilities and others all over the world can have computing experiences free of barriers and limitations.

The harmonization of standards creates an opportunity for everyone. Most important, it benefits users with disabilities who need and deserve accessible technology. ■

---

*Karen S. Evans is national director of the U.S. Cyber Challenge, a nationwide talent search and skills development program focused on the cyber workforce. She served as administrator for e-government and IT at the Office of Management and Budget under President George W. Bush.*

## A short history of spectrum sharing

BY ADAM MAZMANIAN

The government is eager to make more federal spectrum available on the commercial market to fuel the explosion of data-hungry mobile broadband apps and services. But moving government spectrum to market can be a slog.

A recent auction of 65 MHz of prime spectrum fetched about \$45 billion for federal coffers, but getting the military to agree to vacate most of the highly desirable paired frequency sets (which have uplink and downlink bands) took the better part of a decade and required a lot of political arm twisting.

The concept of sharing spectrum is almost as old as radio. The 1912 Radio Act, passed in the wake of the Titanic's sinking, required private telegraph operators at busy seaports to stay off the air for the first 15 minutes of each hour to give naval and other military stations exclusive use of the airwaves.

One hundred years later, the Federal Communications Commission created rules for Medical Body Area Networks, which give health care facilities access

to a 30 MHz swath of spectrum and reserve 10 MHz for the operation of wireless medical information devices in the home.

To reduce the chances for interference, the MBAN spectrum operates on the ground at very low power and shares frequencies with airborne mobile telemetry systems, which operate in the air at very high power.

In 2015, the FCC approved rules for sharing spectrum in the 3.5 GHz band. The plan allows for incumbent federal users, mostly ship-borne radar systems, to maintain their first rights while creating two other tiers for licensed and unlicensed users.

That approach could be characterized as "cooperative sharing," said Peter Tenhula, deputy associate administrator for spectrum management at the National Telecommunications and Information Administration, which manages federal spectrum holdings.

"The devices are working with each other or are controlled by a centralized

database and sharing information," he added.

A working database is essential for dynamically allocating frequencies and maintaining protocols for user priority. Currently, narrow bands of unlicensed spectrum between licensed TV channels — known as "white spaces" — are allocated by use of an FCC database. Dynamic spectrum access for the 3.5 GHz band would allocate as much as 150 MHz of spectrum in real time based on demand and priority.

As the government tries to get more spectrum to commercial users, sharing has some intriguing possibilities for agencies. For federal users, "the goal is to make sure that there's no need to displace equipment that is still within its useful life," Tenhula told FCW.

Additionally, as large swaths of spectrum open up, there is the potential for agencies to gain access to new frequencies as new regulatory thinking allows for a blurring of the lines between federal and non-federal users. ■



# IFTTT:

## *Your digital duct tape*

BY JUSTIN HERMAN

“If This Then That” (IFTTT) is a social media service that combines 166 channels such as Twitter, Android and iOS location services, and RSS into “recipes” that can integrate government social media, data, location-based services and the Internet of Things.

Now one of nearly 80 social media platforms with federal-friendly terms of service, IFTTT can empower federal managers to operate more effectively, and its developer platform can fuel everything from open archives to wearable devices with government application programming interfaces.

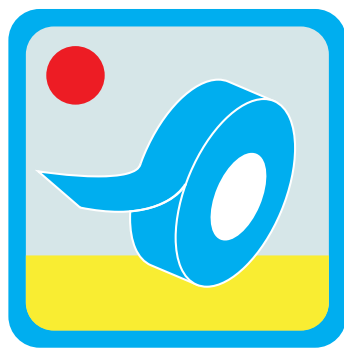
So what does IFTTT mean and how does it work?

If one action is taken on one channel, such as Facebook, you can automatically trigger another action in another channel, such as SMS. For example, you could create a recipe where every Facebook post you send is auto-archived in a document for records management.

Taking the recipe further, you could create triggers where every single social media or blog post sent from any of your approved platforms is auto-archived in a shared Google Calendar that creates an open archive and visual records management system that ensures centralized accountability for any number of satellite offices and agencies. (See [http://is.gd/FCW\\_IFTTT\\_archive\\_tweets](http://is.gd/FCW_IFTTT_archive_tweets).)

And that’s just the beginning. I asked some API enthusiasts in the SocialGov community which of their favorite recipes were must-haves for digital teams or those new to the platform. Although putting government APIs to use for citizens in IFTTT has exciting potential, we focused on recipes that could be used internally for government.

Here are three worth sharing:



**If one action is taken on one channel, such as Facebook, you can automatically trigger another action in another channel, such as SMS.**

### Alerts

As a product manager at 18F, Leah Bannon needs to know when a customer or collaborator wants to take action. The 18F Dashboard, for instance, demonstrates the progress of projects from Discovery > Alpha > Beta > Live and invites people to get involved. She recommends establishing automatic alerts for programs like this to ensure your team is ready to meet them.

**Example:** “Notify me if someone submits a pull request to the 18F Dashboard” ([http://is.gd/FCW\\_IFTTT\\_pull\\_requests](http://is.gd/FCW_IFTTT_pull_requests))

### Notifications

Melody Kramer, an innovation specialist at 18F, has an eye on where the discussions are happening outside government and wants to make sure she’s informed.

She recommends that teams set up notifications that will automatically inform them when a URL from one of their digital properties is shared on another platform. That approach helps her identify where the conversations are happening so she can meet customers where they are.

**Example:** “Notify me if someone submits a link to 18F to Reddit” ([http://is.gd/FCW\\_IFTTT\\_reddit\\_links](http://is.gd/FCW_IFTTT_reddit_links))

### Recruitment

Tim Lowden, a program analyst in the General Services Administration’s Digital Analytics Program, knows that new positions in digital government are rising up across agencies. To help with professional development and recruitment, he recommends using IFTTT to help potential applicants receive alerts when jobs matching specific criteria (such as the positions your department hires) are posted on USAJobs. Such alerts can be customized for keywords, agencies, salary, etc.

**Example:** “Send a daily email digest of new NASA postings on USAJobs” ([http://is.gd/FCW\\_IFTTT\\_jobs](http://is.gd/FCW_IFTTT_jobs))

And that’s just the beginning. We’re planning an API cook-off for later this summer for agencies to explore developing public service channels that would fold government services into IFTTT. So if you’ve got a recipe (or an idea for one), let me know at [justin.herman@gsa.gov](mailto:justin.herman@gsa.gov). ■

*Justin Herman is the General Services Administration’s social media lead and is currently detailed to 18F to focus on talent recruitment. This article is adapted from his IFTTT posts on DigitalGov.gov.*

# Why 'fog computing' *is key to the IoT*

The push to put processing power on the network's edge can be a valuable complement to cloud computing

BY ZACH NOBLE

"Fog computing" describes a way of loading processing power onto devices, from smartphones to simple sensors, at the furthest edges of networks.

On the surface, the core concept seems to be a reversal of the trend toward the cloud because it seeks to restore computing to the periphery of the network.

But instead of being a replacement, it's a developing complement.

Rather than shuttling every scrap of data back to a data center, fog computing allows analysis to take place on the network's edge, saving time and bandwidth and, ideally, optimizing decision-making.

"The usefulness of computing at the edge is manifold, but, for example, ... imagine a network of sensors managing anti-collision capability in a congested airport taxiway system," said Mike Younkens, director of U.S. federal systems engineering at Cisco Systems. "Having decision power within the taxiway instead of at some data center off-site, based on the physics of propagation delay alone, illustrates another tangible use case."

Fog computing is often kicked around in high-level discussions of far-flung Internet of Things or Internet of Everything networks, but there's a more immediate example of the con-



**Fog computing  
provides analytics  
at the edge,  
which allows for  
some very clever  
and innovative  
solutions.**

— MIKE YOUNKERS, CISCO

cept. As the Wall Street Journal's Christopher Mims has noted, smartphone apps showcase the principle underpinning fog computing: The individual device handles some of the data and processing, thereby relieving network stress.

And Gary Hall, chief technology offi-

cer for federal defense at Cisco, said the interplay between fog and cloud is much like an earlier computational disruption.

"Cloud computing has many similarities to mainframe computing, where data is aggregated in centralized locations and accessed from remote devices," Hall said. "Fog computing brings in concepts from distributed computing."

And they don't have to conflict. "When distributed computing via PCs gained prominence, it was highly disruptive to the mainframe computing model," Hall added. "The big difference this time around is that cloud and fog are deeply integrated and complementary."

As the Internet of Things balloons to 50 billion devices by 2020 and data streams threaten to grow faster than the networks that support them, fog computing seems poised to prove a crucial consideration — and not just when it comes to big data.

"Everyone is fixated on 'big data,' which by my definition requires data to be centralized, either physically or virtually, [but big data] analytics does not solve all classes of problems," Younkens said. "Fog computing provides analytics at the edge, which allows for some very clever and innovative solutions." ■

# How derived credentials make real mobility work

BY ELI GORSKI

The use of personal identity verification cards and Common Access Cards for government workers and contractors was mandated by Homeland Security Presidential Directive 12 in 2004. But now as mobile connectivity continues to grow in importance, the need for a new means of authentication has arisen — one that doesn't involve attaching a card reader to every phone and tablet.

Enter derived credentials. This alternate method of verification extracts the credentials on government-issued smart cards and embeds them directly into a mobile device or delivers them via near field communication, microSD cards, USB connections or Universal Integrated Circuit Cards.

In essence, credentials are extended from the card to the device, similar to the way one government-issued ID (e.g.,

a driver's license) can be used to obtain another (e.g., a passport).

The approach allows employees and contractors to use their mobile devices without having their PIV cards handy.

And there are benefits beyond mobility. For example, derived credentials could support automatic desktop locking, which means that if a user's mobile device moves a certain distance from his or her workstation, the desktop PC would lock down and require a password to regain access. Because users are less likely to forget a mobile device than a card when leaving their desks, it could lead to fewer unattended network access points.

There are some trade-offs. Hardware-based derived credentials — those embedded in a device — are more difficult to

use than software-specific solutions, but they are more secure, less susceptible to malware and typically tamper-resistant if a device is lost or stolen.

Software-specific solutions are more flexible and can accommodate multiple device types, but credentials that are stored on a removable card or a device's standard internal storage are an easier target for malware that could crack or compromise the credentials.

Although the solutions are not perfect, competing demands for increased mobile security and improved user experience mean more derived-credential systems are likely.

"The first and next step is derived credentials," Christopher Roberts, vice president of Good Technology's public sector, told FCW. "But we're not done yet" ■

## SPECIAL REPORT

# BREAKING THROUGH THE SECURITY CLOUD

### TOPICS INCLUDE:

SECURITY IS STILL A BARRIER TO CLOUD ADOPTION

HYBRID CLOUD EMERGES AS THE FRONT RUNNER

IAM IS ESSENTIAL FOR HYBRID CLOUDS

ENCRYPTION IS TAGGED FOR DATA SECURITY

COMPLIANCE IS A HEADACHE FOR CLOUD ADOPTION

TO LEARN MORE, VISIT: [FCW.COM/2015SNAPSHOTCYBERSECURITY](http://FCW.COM/2015SNAPSHOTCYBERSECURITY)

SPONSORED BY:



# Improving the skills of your IT staff

Assessing your employees' abilities and identifying skills gaps require a less subjective approach

BY RICHARD A. SPIRES

For those of us who manage others, our effectiveness is largely driven by the skills and motivation of those who report to us. So whether you are a CIO, IT division leader or frontline manager, you need to spend the time to assess your employees in terms of their current skills, abilities and career aspirations, and then help them create the plans that can support their development.

And leaders must do all that in a way that supports the overall near-term objectives of the organization and that properly balances the need for professional development against the organization's day-to-day operational needs.

Yet when it comes to skills assessment, particularly in terms of technical skills, I have always felt that we IT

managers had one hand tied behind our backs. Sure, there are certifications for competence in many different products, and they can be helpful in giving you a sense of an individual's skillset. But how do you assess someone as a journeyman programmer, tester or systems engineer, or perhaps as a master in one's chosen discipline?

It has always struck me that such evaluations are overly subjective and place too much emphasis on "book knowledge" rather than practical applications of that knowledge to develop new, innovative solutions or approaches that the organization truly needs.

The concept of measuring someone's ability to perform in a discipline is captured in Bloom's Taxonomy. "Book knowledge" can only achieve the lowest two levels. However, "synthesis" and above are the only levels at which it is generally accepted that a worker can fully and effectively do the primary roles of their jobs — especially in IT.

This means the assessment problem is twofold. First, for a specific IT discipline, one needs a comprehensive framework by which to understand the types of skills and knowledge an employee should have at each level, from entry level through master.

Second, for each discipline, one also

needs a way to accurately assess the current level of proficiency of one's technical staff members, in order to create the baseline by which to develop their skills so they can move to higher levels of proficiency. That approach not only helps the individual develop a realistic and achievable plan, but it also gives the manager insights into where he or she has significant skills gaps in the organization.

Until recently, it was not easy to address either of those problems. Defining competencies on our own is time-consuming, expensive, frustrating and very likely to be full of inaccuracies.

Fortunately, in 2003 the nonprofit Skills Framework for the Information Age (SFIA) Foundation established a comprehensive framework of skills in IT disciplines based on a broad industry "body of knowledge."

The SFIA currently covers 96 professional IT skills organized into six categories:

- Strategy and architecture
- Business change
- Solution development and implementation
- Service management
- Procurement and management support
- Client interface creation

*Richard A. Spires has been in the IT field for more than 30 years, with eight years in federal govern-*

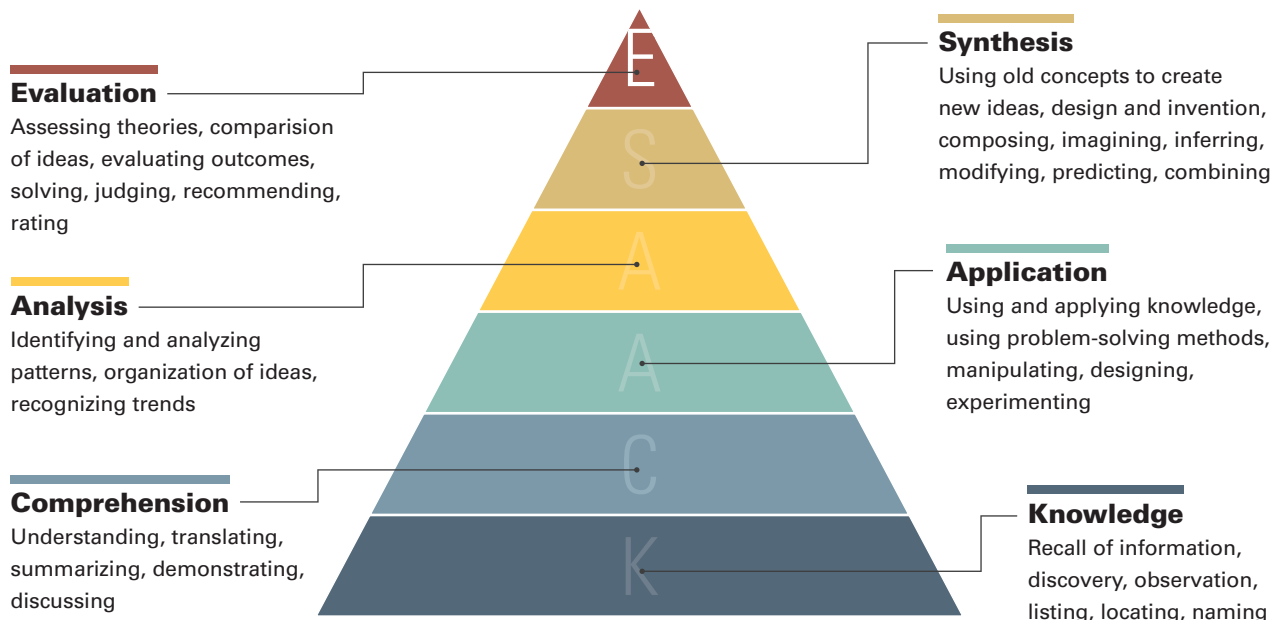
*ment service. Most recently, he served as CIO at the Department of Homeland Security. He is now CEO of Resilient Network Systems.*





# Bloom's Taxonomy

Developed for educators in the 1950s, Bloom's Taxonomy has been adapted to measure individuals' ability to perform in a discipline.



For each of the 96 skills, there are seven levels of attainment that map closely to Bloom's Taxonomy.

The SFIA is updated regularly to account for the rapidly changing IT environment. It is available free of charge for organizations' internal purposes, and it is now used in more than 100 countries. In the United States, the IEEE Computer Society and the Information Systems Audit and Control Association are partners of the SFIA Foundation.

The SFIA is the best way to ensure that the roles and competencies specified for your organization are accurate and complete. But although the framework helps define your needed competencies, it doesn't tell you if your workers have the skills that match them.

Therefore, we need to assess our

employees against the framework and determine what level of attainment they have reached in the specific disciplines in which they work. Then we will be in a good position to help employees develop personal plans to reach higher levels of attainment.

A number of companies are certified to train and coach in the use of the SFIA, including BSMimpact and Learning Tree International in the United States.

The latter company has recently developed an online library of more than 100 skills assessments mapped to the SFIA where appropriate. (In the interests of full disclosure, I serve on the board of directors of Learning Tree International.) Those assessments go beyond just asking questions to measure someone's knowledge of a topic area to evaluate his or her ability to

perform at the synthesis level. They do so by assessing the staff member's ability to perform IT tasks similar to what you would expect him or her to be able to do on the job.

The SFIA and skills assessments can put IT managers in a much better position to understand the actual skills and abilities of their current employees and work with them to address skills gaps and develop individual professional development plans.

Further, by using the framework and assessments throughout one's organization, an IT manager will finally be in a good position to understand and then fill organizational skills gaps that are hindering overall organizational performance. And that's important because as IT managers, we are only as good as the team we develop. ■

Acquisitions,  
reorganizations and  
investments are  
everywhere as key  
companies prepare  
for a return to  
growth in federal IT

# How the biggest contractors have adapted

BY NICK WAKEMAN

**T**he 2015 Washington Technology Top 100 is populated with the largest government contractors in the market, and nearly all are running their businesses on two intertwined tracks.

One track has companies positioning themselves for future growth by making acquisitions, pursuing new markets, restructuring operations and investing in new technologies. At the same time, they are weathering a market that continues to contract.

The total number of prime contracts

measured by the Top 100 fell for the fourth straight year. That continued decline has not been totally unexpected, and many executives are predicting a tight 2015 while looking forward to overall growth returning in 2016.

The market peaked with the 2011 Top 100, when the aggregate prime contracts totaled \$132 billion. For the 2015 Top 100, the aggregate is \$98.5 billion — a 25 percent drop.

The lack of growth mirrors what agencies are experiencing as they continue to face constrained budgets. After several consecutive years of belt tightening, government customers remain focused on reducing costs, increasing efficiency and using new

technologies as a way of boosting effectiveness.

Many executives see that focus on cost, efficiency and effectiveness as a long-term shift in how government buyers view their relationship with contractors, which will continue even when overall spending starts to increase. Much of the repositioning companies have undertaken in the past year or so has been in response to that shift, and some of the moves have been dramatic.

## ACQUISITIONS AND SPLITS

A leading example is the recent announcement by Computer Sciences Corp., No. 10 on this year's list, that it

will divide into two companies: one focused on the commercial market and the other on the public sector.

The company has struggled for several years and has been a turnaround project for CEO Mike Lawrie since he came on board in 2012. Since then, the company has shed business units, restructured to flatten its organization and seen turnover among its senior leaders.

The split, which is expected to be completed by the end of October, might not be the final move that either half of the business will need to make. But the benefit for the commercial and public-sector portions of CSC is that each will be able focus time, financial resources and attention on their respective marketplaces. One will no longer be distracted by the other.

This will likely benefit CSC's public-sector business the most because its financial performance was the quickest to rebound since 2012 and for the most part has held steady.

Another major split, meanwhile, is underway at Hewlett-Packard Co. (No. 6), which is separating its PC, laptop and printer business from its services, software and higher-end hardware business. The move is similar to what IBM Corp. (No. 20) did in 2004. HP's split is expected to be completed by Nov. 1, but the impact on its public-sector business is not clear yet. Both new companies will have substantial government business.

Another dramatic move is the \$4.6 billion acquisition of Exelis by Harris Corp. (No. 9), which closed May 29. Exelis spun off its mission systems business in September 2014 to create Vectrus Inc., which landed at No. 45 on the Top 100. Vectrus took Exelis' IT, infrastructure, logistics and supply chain business, while Exelis retained

Many executives see that focus on cost, efficiency and effectiveness as a long-term shift in how government buyers view their relationship with contractors.

higher-end work focused on critical networks; intelligence, surveillance and reconnaissance; analytics; and electronic warfare.

The idea was to separate the lower-margin work in Vectrus from the higher-margin work held by Exelis. Each company needed different cost structures to remain competitive, and they would be better off as separate companies.

But the repositioning wasn't over. Harris swooped in with a February announcement that it was acquiring Exelis for \$4.6 billion. Harris wanted to add size and scale to its capabilities in ISR, command and control, electronics and other complementary capabilities that Exelis had. The motivation for Harris was to add size, which executives said will make the company more cost-effective and therefore more competitive in the defense and intelligence markets, where Harris expects to grow in the coming years.

That acquisition moved Harris up three spots in the rankings to No. 9.

#### MORE SUBTLE CHANGES

Meanwhile, Raytheon Co. (No. 4) undertook a unique cybersecurity strategy when it acquired a major stake in Websense for \$1.6 billion. It then combined its cyber products business with Websense to create a joint venture focused on the commercial market. The deal allows Raytheon to target the commercial cyber market while still applying those technologies to its defense customers.

That approach differs from other defense companies, which are also

targeting the commercial cyber market but are focused more on adjacent sectors such as energy, utilities and other critical infrastructures.

The size of Raytheon's investment and the structure of the business are unique.

Not all moves to reposition have been so dramatic, though; most are much more subtle. Take Lockheed Martin, No. 1 for 21 consecutive years, which made niche acquisitions in cybersecurity and health care.

Other companies are making strategic hires to increase their intimacy with customers. Several executives described the need to listen to their customers to understand their challenges and needs.

Companies are also actively teaching their customers the art of the possible — not just about new technologies, but about new models of doing business such as cloud computing and everything as a service. They are seeing adoption of those models increase, but there is still a wide gap between early adopters and agencies that are risk averse.

Narrowing that gap is where many government contractors see near-term growth opportunities, so that's where they have targeted their investment strategies. As government buyers remain focused on cost, effectiveness and efficiency, industry leaders believe agencies will turn to new ways of buying goods and services.

And that is when the Top 100 companies' investments, big and small, should pay off, regardless of when overall spending begins to rise. ■

Rank	Company	Headquarters	Prime contracts (in thousands)	2014 rank
1	Lockheed Martin	Bethesda, Md.	\$11,700,962	1
2	Northrop Grumman	Falls Church, Va.	\$6,893,607	2
3	Boeing Co.	Chicago	\$5,256,827	4
4	Raytheon Co.	Waltham, Mass.	\$4,815,472	3
5	General Dynamics	Falls Church, Va.	\$4,071,992	5
6	Hewlett-Packard Co.	Palo Alto, Calif.	\$3,866,791	6
7	Booz Allen Hamilton	McLean, Va.	\$3,665,860	7
8	Science Applications International Corp.	McLean, Va.	\$2,570,645	19
9	Harris Corp.	Melbourne, Fla.	\$2,552,193	12
10	Computer Sciences Corp.	Falls Church, Va.	\$2,379,495	9
11	Verizon Communications	New York City	\$2,029,767	14
12	CACI International	Arlington, Va.	\$2,011,349	13
13	Engility Corp.	Chantilly, Va.	\$1,936,200	30
14	AT&T Inc.	Dallas	\$1,875,331	16
15	L-3 Communications	New York City	\$1,725,575	15
16	Leidos Inc.	Reston, Va.	\$1,642,083	8
17	Accenture	Dublin, Ireland	\$1,599,064	23
18	AECOM Technology Corp.	Los Angeles	\$1,532,825	39
19	BAE Systems	Arlington, Va.	\$1,369,984	20
20	IBM Corp.	Armonk, N.Y.	\$1,349,206	24
21	Dell Inc.	Round Rock, Texas	\$1,325,166	21
22	Jacobs Engineering Group	Pasadena, Calif.	\$1,317,973	22
23	Battelle Memorial Institute	Columbus, Ohio	\$1,198,425	26
24	Fluor	Irving, Texas	\$1,197,994	11
25	Deloitte	New York City	\$1,115,457	27
26	SRA International	Fairfax, Va.	\$1,101,389	29
27	United Technologies Corp.	Hartford, Conn.	\$1,072,515	28
28	ManTech International	Fairfax, Va.	\$1,041,000	18
29	CGI Group	Montreal	\$1,036,025	32
30	PAE	Arlington, Va.	\$1,020,812	31
31	DynCorp International	Falls Church, Va.	\$936,099	10
32	Serco North America	Vienna, Va.	\$794,587	34
33	Vencore	Chantilly, Va.	\$781,700	46
34	Aerospace Corp.	El Segundo, Calif.	\$778,901	33
35	Alion Science and Technology	McLean, Va.	\$702,400	36
36	Wyle	El Segundo, Calif.	\$679,294	35
37	CenturyLink	Monroe, La.	\$654,805	42
38	CDW Government	Vernon Hills, Ill.	\$602,458	51
39	Unisys Corp.	Blue Bell, Pa.	\$529,000	47
40	Iron Bow Technologies	Chantilly, Va.	\$521,113	50
41	Rockwell Collins	Cedar Rapids, Iowa	\$519,960	40
42	Honeywell International	Morristown, N.J.	\$517,992	37
43	Sierra Nevada Corp.	Sparks, Nev.	\$494,808	41
44	Mythics Inc.	Virginia Beach, Va.	\$478,049	57
45	Vectrus Inc.	Colorado Springs, Colo.	\$459,764	17
46	Red River Computer Co.	Claremont, N.H.	\$441,249	68
47	Chemonics International	Washington, D.C.	\$430,530	45
48	Carahsoft Technology Corp.	Reston, Va.	\$416,277	56
49	Parsons Corp.	Pasadena, Calif.	\$412,495	61
50	ImmixGroup Inc.	McLean, Va.	\$408,222	53



Rank	Company	Headquarters	Prime contracts (in thousands)	2014 rank
51	Arctic Slope Regional Corp.	Anchorage, Alaska	\$394,420	55
52	SGT Inc.	Greenbelt, Md.	\$391,434	48
53	DRS Technologies	Arlington, Va.	\$385,172	44
54	ICF International	Fairfax, Va.	\$367,508	52
55	RTI International	Research Triangle Park, N.C.	\$319,204	60
56	World Wide Technology	Maryland Heights, Mo.	\$317,298	62
57	Maximus	Reston, Va.	\$312,038	88
58	Tetra Tech Inc.	Pasadena, Calif.	\$304,273	59
59	DLT Solutions	Herndon, Va.	\$300,333	66
60	Actionet Inc.	Vienna, Va.	\$285,278	71
61	Westat Inc.	Rockville, Md.	\$280,107	82
62	Intuitive Research and Technology Corp.	Huntsville, Ala.	\$276,311	70
63	Insight Enterprises Inc.	Tempe, Ariz.	\$265,906	NA
64	Digital Management Inc.	Bethesda, Md.	\$265,682	74
65	NCI Inc.	Reston, Va.	\$263,440	79
66	Mission Essential	Columbus, Ohio	\$258,251	38
67	Abt Associates	Cambridge, Mass.	\$252,187	78
68	Affigent	Herndon, Va.	\$247,274	NA
69	KPMG LLP	New York City	\$247,148	81
70	Microsoft	Redmond, Wash.	\$240,739	93
71	CH2M Hill Inc.	Englewood, Colo.	\$235,390	86
72	Alvarez and Associates	McLean, Va.	\$234,956	99
73	FCN Inc.	Rockville, Md.	\$233,344	NA
74	MicroTech	Vienna, Va.	\$232,525	89
75	General Atomics Technologies Corp.	San Diego	\$231,976	69
76	Thundercat Technology	Reston, Va.	\$222,993	76
77	Cubic Corp.	San Diego	\$215,165	72
78	Trax International	Las Vegas	\$210,838	NA
79	PricewaterhouseCoopers	London	\$208,400	NA
80	Calibre Systems Inc.	Alexandria, Va.	\$201,143	NA
81	General Electric	Fairfield, Conn.	\$189,679	49
82	Scientific Research Corp.	Atlanta	\$188,336	92
83	SRI International	Menlo Park, Calif.	\$187,205	80
84	John Snow Inc.	Boston	\$185,016	83
85	AASKI Technology	Ocean, N.J.	\$178,299	NA
86	Torch Technologies	Huntsville, Ala.	\$175,954	NA
87	ViaSat	Carlsbad, Calif.	\$175,916	100
88	NCS Technologies	Gainesville, Va.	\$175,109	NA
89	STG Inc.	Reston, Va.	\$174,526	84
90	Adams Communications and Engineering Technology Inc.	Waldorf, Md.	\$174,524	NA
91	New Light Technologies Corp.	Washington, D.C.	\$174,198	NA
92	Development Alternatives Inc.	Bethesda, Md.	\$173,995	64
93	ECS Federal Inc.	Fairfax, Va.	\$173,888	NA
94	Blue Tech Inc.	San Diego	\$171,366	NA
95	Indyne Inc.	Reston, Va.	\$168,838	NA
96	Bechtel Group Inc.	San Francisco	\$166,901	NA
97	Ball Corp.	Broomfield, Colo.	\$166,506	NA
98	Four Points Technology	Chantilly, Va.	\$165,244	NA
99	KeyPoint Government Solutions	Loveland, Colo.	\$162,176	96
100	Camber Corp.	Huntsville, Ala.	\$162,127	94

Sources: Federal Procurement Data System-Next Generation, USAspending.gov, Washington Technology



# FACE OF FACE

## Face-to-Face Event Series

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

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

**FCW.com/events**

### UPCOMING EVENTS

**Cybersecurity: CDM**  
AUGUST 19

**DOD: Joint  
Information  
Environment**  
SEPTEMBER 23

**Cybersecurity**  
OCTOBER 27

**Big Data**  
DECEMBER 2

For event sponsorship information, contact:

**Alyce Morrison**


*Event Sponsorship Consultant*

703.645.7873

amorrison@1105media.com

CONTRACT GUIDE

# UNDERSTANDING CONTINUOUS DIAGNOSTICS & MITIGATION (CDM)



## INSIDE

2

WHAT IS CDM  
AND WHY DO  
YOU NEED IT?

4

CDM  
COULD BE A  
GAME-CHANGER

5

HOW DOES  
CDM WORK?

6

WITH CDM,  
WHAT HAPPENS  
TO FISMA?

8

HOW CDM  
IS ROLLING OUT

# WHAT IS CDM AND WHY DO YOU NEED IT?

**C**ONTINUOUS MONITORING HAS been a long-time staple for organizations looking for ways to more closely track such things as financial and compliance risks. As sophistication of cyberthreats and the risk of damaging breaches increased, so did the relevance for the technique in IT security.

In this sense, continuous monitoring builds on the inherent capability of IT systems to monitor and log network performance. Administrators have used that over the years to periodically check on the health of their systems and networks, and to pick up anomalies that point to a potential security threat, or that a cyberattack might be occurring.

Continuous Diagnostics and Mitigation (CDM) takes that several steps further by combining, in an automated way, the ability to dynamically monitor networks and systems and assess security risks, and then quickly come up with ways to fix holes and vulnerabilities in cyber defenses.

The Office of Management and Budget (OMB) in 2012 made continuous monitoring of federal IT networks one of the now 15 Cross-Agency Priority goals it established to comply with the 2010 Government Performance and Results Modernization Act. Under that, Information Security Continuous Monitoring Mitigation (ISCM) is intended to “provide ongoing observation, assessment, analysis and diagnosis of an organization’s cybersecurity: posture, hygiene, and operational readiness.”

The Department of Homeland Security, in partnership with the General Services Administration, established a formal CDM program as a way to provide agencies with the tools and expertise they would need to implement ISCM. In 2013, 17 companies received awards under a \$6 billion, five-year companion continuous-monitoring-as-a-service (CMaaS) BPA to deliver diagnostic sensors, tools and dashboards to agencies.

Andy Ozment, assistant secretary of the Office of CyberSecurity and Communications (CS&C) in the DHS’ National Protections and Programs Directorate, told Congress in early 2015 that memoranda of agreement with the CDM program encompass over 97 percent of all federal civilian personnel.

The Defense Department is following its own CDM program.

“By the first quarter of FY 2016, 25 agencies and over 95 percent of all federal civilian personnel will have started deploying CDM tools provided by DHS,” Ozment said, “(and) the agency-level dashboards will begin deployment in FY 2015.”

These agency-level dashboards will also feed information to a federal dashboard that the DHS will use to gauge government-wide cyber risks, as well as the progress agencies are making in tackling and reducing risks. It’s expected to be fully operational in FY 2017, Ozment said.

Though a measure of continuous monitoring has been used by government organizations for some time, CDM looks to take that much further with its automated risk and technical assessments. It will also look beyond just device and operating systems to include monitoring of application layer vulnerabilities, an essential these days as some of the more damaging cyberthreats involve errors in software.



As well as the improvements the CDM program itself is expected to bring, the DHS is also touting its ability to complement other major security programs such as the National Cybersecurity Protection Systems, otherwise known as EINSTEIN. That is an integrated intrusion detection, analysis, information sharing, and intrusion prevention system used to provide perimeter defense for government networks.

The DHS also believes the program will make it easier for agency systems administrators to fulfill security requirements set out in OMB’s A-130 circular, and to implement NIST guidelines on continuous monitoring.



# 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.

 Cloud Security Solutions	 Security Convergence Solutions	 Big Data Visualization & Analytics Platform	 Continuous Monitoring of Credential Authorities	 Intelligent Network Visibility Platform	 Biometric Authentication & Access Management
 Privileged Account Controls & Monitoring	 Cyber Visualization, Analytics & Modeling	 Secure On-Premise Storage Infrastructure	 Wire Data Analytics for Continuous Monitoring	 Application Security Testing & Management	 Cybersecurity & Malware Protection
 Intelligent Network Visibility Platform	 Integrated Enterprise Security Solutions	 Virtualization Security, Compliance & Control	 Data Center Security Solutions	 Automated Network Control	 Endpoint Security Solution
 NoSQL Platform for Cyber Defense & Analysis	 Cross-Platform Database for Big Data Analytics	 Real-Time Predictive Analytics	 CAC Authenticator Cases for Smart Phones	 SE Secure Linux	 Security, Risk & Compliance Management
 Data Protection & Software Monetization	 Real-Time Behavior Analysis for Risk Management	 Cloud Infrastructure Security Platform	 Operational Intelligence Software	 Data-in-Transit Security Solutions	 Monitoring, Remediation & Compliance Reporting
 Security Configuration & Vulnerability Management	 DbProtect Database Security & Audit Logging	 Next-Generation Trust Protection	 Network Virtualization & Security Platform	 Enterprise Encryption & Key Management	 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

# CDM COULD BE A GAME-CHANGER

**IT'S NOT AS IF** most government agencies don't already have at least some IT security in place. However, depending on the time and resources each can devote, security can sometimes be more of a patchwork affair that provides uncertain protection. Will CDM change that?

DHS set the CDM program up to be implemented in three distinct phases, each stepping up the extent of the goals that should be met with each:

**1. Endpoint integrity:** The scope of this is the local computing environment, and focuses on the identification and management of agency hardware and software assets, listing known vulnerabilities and malware, and device configuration management.

**2. Least privilege and infrastructure integrity:** This is focused more on the people in the environment, and being able to manage their account and network privileges, and on managing the configuration of network infrastructure devices and services.

**3. Boundary protection and event management:** This encompasses such things as event detection and response, encryption, remote access management and access control, and is aimed at ensuring security is built into networks rather than added on later as an after-thought.

The first phase, which is basically about vulnerability scanning and knowing what's on the network, should be a no-brainer for most agencies since that's the fundamental baseline for any security plan. However, in a survey it conducted in 2014, the SANS Institute found that less than 21 percent of federal government respondents said they had completed a formal gap assessment prior to starting the program.

When SANS asked people to rate the difficulty they faced in classifying assets as a part of their assessments, the most concern was for differentiating between unmanaged and managed, and authorized and unauthorized, devices connecting to the network. Several products offered under the CDM program

can play a key role in addressing this area, SANS said.

The second phase, however, may be of the most immediate interest to agencies since it focuses on managing privileged access to networks and data, which speaks to the insider threats involved with such incidents as the Snowden and WikiLeaks breaches, as well as more mundane issues of data leakage over insecure network links.

It should also help with one of the biggest current threats, the theft of network credentials from agency users or, increasingly, from outside business partners such as government integrators who are given access to agency networks.

Agency-level dashboards could also be transformative for security, but that will depend on how well they are implemented. Most agencies are already familiar with dashboards for other uses, but those used for CDM will have to carry more specific information. It won't be enough to simply give the number of vulnerabilities found and that haven't been patched; agencies will have to know the risk of each so they can prioritize which systems are fixed first.

That will depend on how good the CDM program contractors are since they will be tasked with providing all of the technical services necessary to install, configure and maintain the dashboards, along with the positioning of the sensors that feed data to the dashboards.

It all comes down to the mitigation part of the CDM description, according to John Pescatore, director of emerging security trends at SANS. That's key, he said, since finding vulnerabilities doesn't do any good unless you are also fixing them. Proof of effectiveness will be lacking until the CDM program actually gets to that point.

"Continuous monitoring is just voyeurism unless you are actually changing something," he said.

# HOW DOES CDM WORK?

**T**HE CDM PROGRAM is intended to be a comprehensive push to move all of the federal government to continuous monitoring as the basis for agencies' cybersecurity strategies, and through that to adopt risk-based mitigation practices. Implemented the right way, it will provide critical insight into how agency security systems and processes are working.

Knowing when an agency CDM program is completed is relatively straightforward, according to the US Computer Emergency Readiness Team. A full implementation will be when an agency can use the CDM infrastructure to "automatically test as much of the NIST SP 800-53 control set as possible and efficiently."

The DHS reduced this to a set of 15 capabilities for the CDM which is consistent with the NIST controls, but that have additional requirements such as being able to resist specific attack scenarios, identify the targets that are under attack, and apply a defined Concept of Operation for how continuous monitoring will be used to detect the weaknesses of those targets and prioritize their mitigation.

Together with the agency level dashboards that are also required under the CDM program, when agencies fully implement CDM it will provide them with a suite of capabilities and tools that the DHS says:

- Enables network administrators to know the state of their respective networks at any given time.
- Informs on the relative risks of threats.
- Makes it possible for system personnel to identify and mitigate flaws at near-network speeds.

How well agencies can move forward with this is still a question, however. DHS is planning for a fairly smooth rollout, with Phase 1 of the program focusing on endpoint security and vulnerability scanning, starting in late 2013. Several task orders for that have already been issued.

However, the tools needed for that mostly use known

technology. Phase 2 of the program, which will focus on access and identity management, is likely to need at some new technology and the requirements of that are still under review. The necessary modifications to the GSA's CMaaS BPAs to accommodate them are expected by the end of FY 2015.

But some agencies already have a good baseline understanding of their needs for Phase 1, and would probably be able to already move to Phase 2. DHS, however, though it's defined the CDM capabilities, hasn't given any prioritization schedule for how those capabilities should be implemented, leaving it to the agencies themselves to decide on how and when to do that. They can either use their own funding to buy from the BPA according to their own specific needs, or use DHS funds by signing a Memorandum of Agreement.

In fact, according to Pescatore, things may have slowed even more from the deliberate pace DHS has taken with the CDM program. That could be due to a number of things, such as the budget sequestration limits and change within DHS itself. The DHS also seems to be focusing more on new information intelligence sharing initiatives than it is on CDM, he said.

That shouldn't be the case, he said. The first phase of the program "is pretty basic and not that complicated," he said. Also, there are continuing reports from agency acquisition people that the GSA contract is harder to use than it should be. Meanwhile, the security threats continue to get worse and more frequent.

"The bottom line is that the CDM capabilities are badly needed by government agencies, but (the program) is not moving quickly enough," he said.

# WITH CDM, WHAT HAPPENS TO FISMA?

## THE FEDERAL INFORMATION SYSTEM

**T**he Federal Information System Management Act (FISMA) has been the backbone of federal IT security for more than a decade, but it's come under increasing attack in recent years. With the dynamic nature of security threats today, FISMA's snapshot approach to security assessments is seen as wildly out of date.

The DHS CDM program was created in part to support FISMA reporting, but it could eventually be the key to making FISMA relevant once again. In particular, phase 2 of the program that focuses on identity and network management could be the "realization" of IT security, said Jeff Wagner, director of security operations for the Office of Personnel Management.

It's a sign, he said, that "the federal government finally is taking FISMA seriously," according to a recent story in Government Computer News.

FISMA, enacted in 2002, was a big leap forward for IT security at the time. It focused on a risk-based approach to "cost-effective" security, and required agencies to conduct annual reviews of their security and formally report the results to OMB. The yearly parade of those agencies deemed to be compliant, or not, with FISMA became an anticipated part of the federal IT scene.

However, it only required a yearly statement that the agency systems and networks met FISMA requirements. Agencies were under no compulsion to regularly follow up their assessments to make sure those systems and networks were always in compliance. For that reason, FISMA was increasingly dismissed as a "box-ticking" exercise with little relation to actual agency security.

CDM should put the relevance back into FISMA. Automated, near-real time scanning and validation of network and system security will accomplish many of the things FISMA was intended to deliver. It will also take much of the pain out of the manual, paper-based method of reporting FISMA since much of

the information collected and fed to agency CDM dashboards, and the on from there to the federal dashboard, will meet FISMA requirements.

In fact, CDM-like capabilities are now required by law. In tweaking FISMA to bring it up to date with current security threats, Congress in December 2014 directed DHS as part of the Federal Information Security Modernization Act to "administer procedures to deploy technology, upon request by an agency, to assist the agency to continuously diagnose and mitigate against cyber threats and vulnerabilities."

OMB also has to deliver annual assessments to Congress on the progress of agencies toward adopting "continuous diagnostic technologies" and other advanced security tools.

OMB emphasized the need for agencies to implement CDM capabilities with a memo updating FISMA metrics for FY 2015 that, where possible, used existing federal agency data feeds to automate responses to improve the quality and timeliness of reported data. Agencies "must assess their information security capabilities against these enhanced FISMA metrics at the beginning of FY 2015," OMB said.

If nothing else, there is a cost imperative that will drive that CDM-influenced change in FISMA. When DHS went to the various chief information security officers at agencies and asked them how much time and resources they devoted each year to dealing with FISMA compliance, they said up to 65 percent was spent on the FISMA process and reporting.

In 2013, at the launch of the CDM program, DHS said CDM will cost just \$200 million versus the \$600 million a year spent on current compliance needs, and will use just six percent of each cybersecurity dollar.



# Take the complexity out of CDM.

**Think beyond compliance. Think ahead.** HP Enterprise Security Products offers a complete solution to maintain secure data environments and meet agency missions. Our approach to CDM reduces compliance to four simple, integrated steps. We provide industry leading best-of-breed cybersecurity products to modernize agency infrastructure for improved efficiency and increased protection of networks and information systems.

Our easy to deploy and use security management products test assets for vulnerabilities before they launch, identify evolving risks in assets already in use, find and resolve threats across the network at machine speed, and reduce the number of events requiring manual management.

HP takes the complexity out of CDM. See how it strengthens your mission. To learn more visit: [hp.com/go/pubsecsecurity](https://hp.com/go/pubsecsecurity)



# HOW CDM IS ROLLING OUT

**A** **NNOUNCED IN EARLY 2013**, the \$6 billion DHS CDM program is expected to take around five years to implement completely, with the ability to get a government-wide view of agency security status due by the end of FY 2017, when a federal CDM dashboard should be up and running.

In between then and now, the program will go forward in three separate phases, each one blending into the other. Work on an earlier phase will still go on, even as the next phase begins. Each phase, involving the delivery and integration of commercial-off-the-shelf scanning and security tools to agencies, will be implemented via a number of task orders, which will be met through the CMaaS BPA overseen by the GSA.

Contract awards for CMaaS, which will operate under GSA Schedule 70, were made in August 2013 to 17 companies:

Phase 1—endpoint security/device integrity—kicked off in January 2014 with a \$60 million award for tools needed to provide immediate protection for agency devices such as desktop computers and servers, along with hardware and software inventory tools. A separate contract to begin development of the federal and agency dashboards was made several months later outside of the CMaaS, under the Alliant small business contract.

Task order 2 for Phase 1, which would begin the rollout of planning, management, training, and architecture and engineering tools and services to agencies, is split into six separate groups of differing agency size and missions. The \$29 million contract for task order 2A, involving the DHS itself, was awarded at the end of February 2015.

Task order 2B—intended for the departments of Energy, Transportation, Interior, Agriculture, and Veterans Affairs, along with the Office of Personnel Management—was filled with a \$39 million award in April 2015. Groups C through E task orders are

expected to be awarded by the end of FY 2015 with the remaining group, mainly comprising smaller agencies, to be settled by the end of the calendar year.

When all five awards are made, the CDM program will cover over 98 percent of the federal civilian workforce.

Phase 2 is expected to generate major interest from vendors since it includes five of the CDM's 15 capabilities—access control management, security-related behavior management, credentials and authentication management, privileges, and boundary protection including network, physical and virtual components—that also represent some of the more leading-edge technology areas.

CDM vendors received a RFI for products that could be used in Phase 2, and the necessary modifications needed to the GSA BPA to include these are now being considered. Those modifications could come before the end of FY 2015.

DHS officials have touted the CDM program also for its ability to save agencies money by going through the CMaaS. In remarks to a Senate appropriations panel in April 2015, Ozment said the January 2014 Phase 1 award to purchase continuous monitoring tools for agencies through the CMaaS “demonstrated a 30 percent cost reduction over GSA pricing and resulted in \$26 million in cost avoidance.”

A subsequent award for license maintenance of those tools reflected a 50 percent cost reduction over GSA pricing, he added.

State, local, regional and tribal governments can also buy CDM products and services using the CMaaS BPA, independent of the CDM program itself.

# FCW Index

## People

Bannon, Leah..... 23	Hall, Gary..... 24	Mims, Christopher ..... 24
Barron-DiCamillo, Ann..... 19	Herberger, Carl..... 3	Obama, Barack..... 10
Beshara, Philip..... 11	Herman, Justin..... 23	Roberts, Christopher... 25
Bock, Laszlo..... 15	Horowitz, Michael..... 6	Rung, Anne ..... 7
Brennan, Niall..... 14	Jacobs, Bob ..... 12-14	Snowden, Edward..... 3
Brian, Danielle..... 6	Jurek, Richard..... 14	Spires, Richard ..... 26-27
Cardon, Edward..... 3	Kendall, Frank..... 3	Stanton, Thomas..... 16-20
Chabot, Steve..... 7	Kornblith, Joan..... 7	Stiennon, Richard..... 3
Chiarodo, Justin..... 11	Kramer, Melody..... 23	Tenhula, Peter..... 22
Dore, Stan..... 18	Lawrie, Mike..... 29	Underhill, Larry ..... 6
Epstein, Daniel..... 6	Lowden, Tim ..... 23	Webster, Douglas..... 16-20
Evans, Karen..... 21-22	Mader, David ..... 20	Wilson, Paul..... 10
Graves, Sam ..... 7	Matulka, Rebecca ..... 17	Younkers, Mike..... 24
Haines, Fred..... 20	McCaa, Terrace..... 6	
	Miller, Jeff..... 7	

## Agencies/Organizations

AFERM..... 16-18	Interior ..... 6, 17
Akamai ..... 6	IRS..... 13
American Society of Military Comptrollers..... 19	IT-Harvest..... 3
Army ..... 3	Justice ..... 6
Association of Government Accountants..... 18	Labor..... 18
CareerBuilder..... 15	Ken Blanchard Companies ..... 10
Casualty Actuarial Society..... 16-17	Labor..... 6
Cause of Action..... 6	Learning Tree International..... 27
Cisco ..... 24	Lockheed Martin..... 29
CMS ..... 14	NASA ..... 12-14
Congress ..... 3, 6, 7	NTIA ..... 22
CSC ..... 28-29	OFPP ..... 7
DHS..... 11, 19, 22	OMB..... 19-20, 22
Dickstein Shapiro ..... 11	OPM ..... 11
DISA..... 6	Project on Government Oversight ..... 6
DOD ..... 3, 11, 22	Radware ..... 3
Education ..... 18	Raytheon ..... 29
Exelis ..... 29	Resilient Network Systems ..... 26
FCC..... 22	Risk and Insurance Management Society ..... 18
FireEye..... 11	SFIA Foundation..... 26-27
GAO ..... 7, 20	State..... 22
Good Technology ..... 25	U.S. Access Board ..... 21-22
Google..... 15	U.S. Cyber Challenge..... 22
GSA..... 7, 20, 23	VA..... 6
Harris ..... 29	Vectrus..... 29
Hewlett-Packard..... 6, 29	Wall Street Journal..... 24
IBM..... 16-20, 29	WebSense..... 29
	White House ..... 10, 14

## Advertisers

<b>AT&amp;T Corporation</b> www.att.com/gov/cyber.....	<b>1-2</b>
<b>Enterprise Architecture</b> www.GovEAconference.com.....	<b>2</b>
<b>Face-to-Face Event Series</b> www.fcw.com/events.....	<b>32</b>
<b>InterSystems Corp.</b> www.InterSystems.com/Federal1CC.....	<b>43</b>
<b>QTS</b> www.fcw.com/2015snapshotcybersecurity.....	<b>25</b>
<b>TDWI Boston</b> www.tdwi.org/BOS2015.....	<b>44</b>
<b>VMWARE Inc.</b> www.vmware.com/go/VSAN.....	<b>8-9</b>

**CDM Contract Guide..... 33-40**

**CarahSoft Technology Corp.**  
www.carahsoft.com/cdm..... **35**

**Hewlett Packard**  
www.hp.com/go/pubsecsecurity..... **39**

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](http://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](mailto:FCWmag@1105service.com) or call (866) 293-3194 for U.S. & Canada; (847) 763-9560 for International, fax (847) 763-9564. **POSTMASTER:** Send address changes to FCW, P.O. Box 2166, Skokie, IL 60076-7866. Canada Publications Mail Agreement No: 40612608. Return Undeliverable Canadian Addresses to Circulation Dept. or XPO Returns: P.O. Box 201, Richmond Hill, ON L4B 4R5, Canada.

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

**PUBLIC SECTOR  
MEDIA GROUP**  
CORPORATE HEADQUARTERS  
9201 Oakdale Ave., Suite 101  
Chatsworth, CA 91311  
[www.1105media.com](http://www.1105media.com)

# BackStory



HE DEPARTMENT of the INTERIOR HAS DEVELOPED A SIZEABLE FOLLOWING ON ITS INSTAGRAM ACCOUNT FEATURING PHOTOS OF OUR NATION'S PUBLIC LANDS.

WITH THE BAR NOW RAISED, HOW WILL OTHER AGENCIES MEET THE CHALLENGE?



Environmental Protection Agency



Bureau of Weights and Measures



Internal Revenue Service



Administration on Aging



Office of Personnel Management



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

**“Aggregated and normalized patient data?”  
Sergeant James just feels better.**

HealthShare transforms care by sharing health information.

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

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

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

Learn more at: [InterSystems.com/Federal1CC](https://www.intersystems.com/Federal1CC)

**INTERSYSTEMS®**

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



#### EARLY REGISTRATION DISCOUNT

Register by June 26  
and save up to \$345

USE PRIORITY CODE BOS7

# Boston 2015

## The Analytics Experience

July 26–31, 2015

The Analytics Experience provides comprehensive, end-to-end analytics training on everything you need to build and execute a high-value analytics program. Six action-packed days filled with classes, peer-to-peer sessions, case studies, hands-on training, and networking offer an accelerated learning experience for business and technical leaders and implementers.

### Core Tracks

- // BI & Analytics Foundations
- // Big Data & Data Management
- // Data Visualization & Presentation
- // Advanced Analytics Techniques
- // Big Data & Analytics Technologies
- // Leadership & Management
- // Analytics in Action

### Hot Topics

- // **Big Data Analytics**  
*From data to technologies to business value*
- // **Data Visualization**  
*The language of images*
- // **Advanced Analytics**  
*Predictive, simulation, streaming, social, Internet of things, and more*
- // **The Changing World of Data**  
*Ecosystems, modeling, technologies*
- // **Data Science**  
*Algorithms, techniques, working with data scientists*

### KEYNOTES



**Data to Profit: Revenue Growth through Analytics and Monetization**

**Barbara Wixom, Ph.D.**  
*Principal Research Scientist, MIT Center for Information Systems Research*



**The New BI/Analytics Synergy: How to Align Business and IT around Data**

**Wayne Eckerson**  
*Principal Consultant, Eckerson Group, LLC*

### New!

#### HANDS-ON TRAINING

LEARN HOW TO USE ALL THE LATEST ANALYTICS TOOLS AND TECHNOLOGIES

#### PEER-TO-PEER LEARNING

GAIN TIPS AND TECHNIQUES FOR HIGH-IMPACT AND HIGH-VALUE ANALYTICS



Advancing all things data.