FCW
THE BUSINESS OF FEDERAL TECHNOLOGY

Secure the federal enterprise

JUNE 15, 2015 • VOLUME 29 NUMBER 9

Better security for a better organization.

Are you ready for an end-to-end IT security solution that enables your government agency?

Discover how IT security can enable growth at Dell.com/security.

FCW
THE BUSINESS OF FEDERAL TEC

Wounded warriors' new cyber mission
PAGE 20

What's next for NetCents?
PAGE 30

BRINGING ORDER TO CYBER SPACE

DOD'S QUEST FOR ONLINE COMMAND AND CONTROL

JUNE 15, 2015
VOLUME 29 NUMBER 9

TDWI is your source for in-depth education and research on all things data.

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

tdwi
Advancing all things data.

Trending

80% of public-sector mobile devices activated in the first quarter of 2014 ran on iOS

Teaching contracting officers to buy digital services

The U.S. Digital Service and the Office of Management and Budget's Office of Federal Procurement Policy want someone to teach the proverbial man to fish — for better digital procurements.

The agencies are using Challenge.gov to solicit proposals for the development of a training program, and the winning submission could earn as much as $320,000 in prize money.

The challenge's goal is to create a Digital Service Contracting Professional Training and Development Program.

The program will ideally be no more than six months long and aimed at helping federal contracting officers and contract specialists navigate the procurement of digital services, according to the announcement on Challenge.gov.

A successful program will teach contracting professionals how to:

- Understand and buy digital services and supplies using concepts described in the Digital Services Playbook and TechFAR, which include DevOps, user experience, agile software development, open source, cloud, infrastructure as a service, software as a service and platform as a service).
- Appropriately measure the success of digital services contracts according to industry standards.
- Accurately describe and define the value received.
- Encourage the use of commercial practices and innovative approaches — for example, modular contracting, broad agency announcements, challenges and prizes — to ensure that procurements can capture flexible and rapidly changing technology advancements.

The challenge has three phases. In Phase I, participants will submit white papers detailing their concepts for the training program. Three finalists will be selected and given $20,000 to move forward with their designs.

In Phase II, the finalists will present mock classroom training and the full design of their programs.

One winner will move to Phase III, in which $250,000 in milestone payments will fund a pilot training program.

If the design meets the government's objectives, the winner will be eligible for a final $50,000 prize payment.

Phase I submissions will be accepted through June 23, and the Phase III pilot program should be completed and presented to OMB by Jan. 31, 2016.

— Mark Rockwell

Rising to the challenge

The Digital Service Contracting Professional Training and Development Program must help federal procurement officials:

- Become digital service procurement experts.
- Gain the knowledge necessary to become embedded in agency digital service teams and serve as business advisers to teams, their customers and their stakeholders.
- Learn how to lead agency training, workshops and consultations to expand digital service procurement expertise within their agencies and the government.

Source: Challenge.gov

FCW CALENDAR

6/18 GWACs
ACT-IAC and the NIH IT Acquisition and Assessment Center will host a discussion of governmentwide acquisition contracts' role in "Smarter IT Acquisition." Washington, D.C. http://is.gd/FCW_gwac15

6/30 Open data
AFCEA Bethesda's annual Data Symposium will focus on "impacts in the day and life of the citizen." NIST's Ram Sriram is among the invited speakers. Washington, D.C. http://is.gd/FCW_afcea_data

Contents

TRENDING

DEPARTMENTS

FCW
THE BUSINESS OF FEDERAL TECHNOLOGY

SALES CONTACT INFORMATION

MEDIA CONSULTANTS

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

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

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

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

EVENT SPONSORSHIP CONSULTANTS

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

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

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

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

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

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

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

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

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

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

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

Trending

8% of websites using HTTPS are vulnerable to Logjam, a 20-year-old Transport Layer Security flaw

Contractor IT challenges have a familiar ring

Federal contractors face many of the same nagging questions that their agency customers do in dealing with IT, project management and cybersecurity, according to a new study by Deltek.

The company's sixth annual GovCon Industry Study states that top IT challenges for federal contractors are IT and data security, budget pressures, and managing multiple systems for their own operations. Almost a quarter of the more than 300 companies that responded to the survey ranked IT and data security as their top challenge.

Therefore, as federal vendors move applications into the cloud, their initial efforts have focused on less sensitive data such as social media and human resources applications. Like their government customers, some contractors are struggling with moving more sensitive accounting and finance applications to the cloud, said Kevin Plexico, Deltek's vice president for research.

The study notes that although company executives have been reluctant to put financial data in the cloud, cost savings and other benefits have spurred them on.

Project management, procurement and manufacturing applications were at the bottom of their cloud applications list.

In addition, more than 50 percent of the companies surveyed had no cloud plan, said Warren Linscott Jr., vice president of product strategy and management in Deltek's GovCon group.

That reluctance could be a result of increasing concerns about cybersecurity and confusion about cloud definitions and services such as third-party hosting and software as a service, Linscott said.

— Mark Rockwell

Making the business case for DHS S&T

Representatives of several technology groups told a House panel in May that the Department of Homeland Security's Science and Technology Directorate has taken some shaky first steps toward collaborating with industry.

Although S&T's plans to open up to industry are progressing, witnesses told the Homeland Security Committee's Cybersecurity, Infrastructure Protection and Security Technologies Subcommittee that they had concerns about transparency, return on investments and S&T's apparent lack of influence over DHS component agencies' acquisition efforts.

"Due to the budget cuts, many mid- to large-size companies lost interest in engaging with S&T because it has had difficulty making an attractive business case for their involvement," said Marc Pearl, president and CEO of the Homeland Security and Defense Business Council.

S&T's revised five-year plan, released in late April, helped clarify some of the directorate's goals, said Jake Parker, director of government relations at the Security Industry Association.

However, Parker said S&T has only slight pull with DHS component agencies when it comes to committing to technology acquisitions. "Agencies need to commit to S&T" for acquisitions, he said, noting that currently, "they can go elsewhere."

"While a level of disconnect between S&T and its customers is undoubtedly due in part to the fragmented nature of DHS, it is encouraging to see an acknowledgment of this as an issue and several proposals in the strategic plan on how to improve coordination," Parker added.

Subcommittee Chairman John Ratcliffe (R-Texas) raised concerns about DHS using the Defense Department's defense industrial base as a model for its relationship with industry. "We need to ensure we are addressing the needs of DHS [and] messaging the needs and direction of its components to the small- and medium-size businesses that are interested in doing business in the homeland security ecosystem," he said.

— Mark Rockwell

INK TANK

$320,000 is being offered through Challenge.gov for the best solution to train acquisition officers in digital services procurement

NS2020 RFP probably pushed back

The General Services Administration had been planning to release the request for proposals for the foundation contract of its next-generation Network Services 2020 strategy for telecommunications in July, but a top official said more time will likely be needed as his team gathers input from industry and other interested parties.

Amando Gavino Jr., director of GSA's Office of Network Services Programs, told FCW that his team is sifting through 1,600 comments from vendors and agencies regarding the expansive $50 billion, 15-year Enterprise Infrastructure Solutions (EIS) contracting vehicle that will form the foundation of NS2020.

He said the complex RFP must be released this fiscal year, and in April, he left the door open to pushing back the RFP's July release date.

That is looking even more likely now. "We will still be seeing people until the end of June," Gavino said. "I can't say, 'We're taking your comments' and then three weeks later get out the RFP. That's not going to happen."

He added that even if the RFP is postponed, it would not affect the contract's award target of January 2017.

Several industry sources said the RFP's release would probably edge closer to the end of September to allow maximum time for input and analysis.

Gavino has been taking a diligent approach to gathering feedback, including one-on-one meetings with potential vendors. GSA also unveiled the NS2020 community on its Interact website in April to facilitate more collaboration.

At a Professional Services Council industry forum in May, GSA officials discussed NS2020 and Alliant 2. The event was closed to the press to allow a freer discussion of how the two contracts might align with each other.

— Mark Rockwell

EDITOR'S NOTE

Last call for Rising Star nominations

When an agency or key contractor hires a top executive, that gets plenty of press. Ditto when those senior officials steer a key project to success, change roles, get their team out of trouble or decide to tackle a major problem.

Far less covered, however, is the next generation of leaders in the federal IT community — those who are coming up through the ranks and doing the great work that doesn't include a turn at the podium.

FCW's Rising Star awards are an opportunity to address that inequity — to recognize some of the individuals who are early in their careers and are bringing amazing energy and ideas to the table.

This year's deadline for nominations is fast approaching, and we need your input to be sure we find the best possible candidates for our judges to consider.

Nominees can come from government, the private sector, 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. (That's not just millennials, mind you — a 60-year-old who has embarked on a second career is every bit as eligible.)

What makes for a winner? In many ways, we rely on 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 simple guidelines to keep in mind:

- This is an individual award. Teams are important, but that's what the GCN Awards are for.
- 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 previous year. Future leadership potential is important, too, but one must have had clear accomplishments in the past 12 months.
- You can nominate more than one person. Do so early and often.

So gather your information and supporting nominators, and submit those nominations by July 2. Go to FCW.com/2015risingstars to learn more, then let us know where to find the leaders of tomorrow — and the rising stars of today.

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

1,600 comments were received for GSA's Enterprise Infrastructure Solutions draft RFP

CRITICAL READ

WHAT: "Accelerating Data Innovation: A Legislative Agenda for Congress" by the Center for Data Innovation.

WHY: As the Obama administration winds down, Congress has an opportunity to enshrine elements of its open-data policy into law.

In addition to codifying open data, the authors of the report have 11 recommendations for Congress. Some are controversial, including a plan to require that all regulatory data submitted to the Securities and Exchange Commission be in machine-readable XBRL format and a proposal to create a universal patient identifier for electronic health records.

VERBATIM: "Congress should pass legislation that explicitly defines publishing open data as the official responsibility of federal agencies. To fully secure the benefits of open data for the public and businesses, such legislation should codify the data stewardship and publishing requirement put forth by the Obama administration's Open Government Directive and related executive actions; establish high standards for the accuracy and timeliness of government data; store this data in non-proprietary formats to make it as accessible as possible; and apply these rules to all government contractors and quasi-governmental agencies."

FULL REPORT:
is.gd/FCW_opendata

Privacy, security and one login to rule them all?

Trust, privacy and security were at the center of a panel discussion at the U.S. Digital Service's DigitalGov Citizen Services Summit in May.

"We can build all the beautiful digital services that we want, but if people don't trust them, they're not going to use them," said Dan Morgan, the Transportation Department's chief data officer.

Commercial credentials and a new attitude toward privacy could be the keys to future success.

For instance, the use of "sensitive information" could enable government to provide new levels of service, said Sean Brooks, privacy engineer at the National Institute of Standards and Technology. But people's concerns about privacy necessitate finding a careful balance.

Keeping track of numerous logins is taxing, too, and Jennifer Kerber, director of the General Services Administration's Connect.gov, lamented the need to create unique usernames and passwords for each government service online.

"What if I had the opportunity to bring a credential I trust to the government?" she asked.

And that's exactly what she and her GSA colleagues are creating with Connect.gov, which allows users to connect with the government by using credentials they already have and trust, such as those they've established with Google or PayPal.

Agencies don't track which credential is provided or the digital activity that is so often used for marketing purposes, Kerber said. They simply know that the person's identity has been verified by a trusted third party, which simplifies the process for users and saves the government money.

Brooks said privacy, security, and the ways agencies and people talk about them need to be overhauled.

"If I could eliminate the word 'creepy' from all future conversations about privacy, I would," he said.

When it comes to credentials and digital services, "privacy, security, interoperability and user friendliness" should be the guiding principles, Brooks said, adding that they should be built into digital services from the ground up.

He and Kerber noted that the "5,000-word privacy statement that makes the lawyers happy" is not a good model for the future of digital services. Organizations must shoulder responsibility for privacy and security rather than shunting it onto users.

— Zach Noble

ACT-IAC
@ACTIAC

What do #millennials look for in a career? Better yet, what makes them stay? @FCWnow has the answers #MOC2015 http://ow.ly/Ncev7

Reply Retweet Favorite

11:05 AM - 21 May 2015

Join the conversation

FCW uses Twitter to break news, field questions and ask our own.
Learn more at Twitter.com/FCWnow.

FACE TO 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

Cloud
JUNE 10

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

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

65% of information security professionals say they are concerned about "security technology sprawl"

FCW Insider: People on the move

President Barack Obama intends to make **Denise Turner Roth**'s job as acting head of the General Services Administration into a more permanent one.

Roth stepped into the acting administrator position after **Dan Tangherlini** left the agency in February to become chief operating officer at Artemis Real Estate Partners.

When she took over the acting administrator position, Roth told FCW that she saw her mission as perpetuating the successes her predecessor's strategies yielded.

Before she joined GSA as deputy administrator in 2014, Roth was city manager in Greensboro, N.C. She has also worked on Capitol Hill and for the D.C. government.

Marine Corps CIO Brig. Gen. **Kevin Nally** will retire in July.

At AFCEA NOVA's Naval IT Day in May, Nally told the audience that this would be his last time speaking at the annual event — "unless," he quipped, "I become president of the United States, in which case I'll be happy to come back and talk to you."

He told reporters that after "34-plus years, it's time to transition" but declined to comment on what he'll do next, saying only, "I know what I don't want to do."

Martha Dorris, director of strategic programs at the General Services Administration, won ACT-IAC's 2015 John J. Franke Award.

Mary Davie, Dorris' boss at the Federal Acquisition Service and a former Franke Award winner, described Dorris as "an acknowledged thought leader and committed public servant who encourages collaboration and supports her colleagues, taking risks to improve the customer experience."

The Franke award is named for **John J. Franke**, who was a Marine, businessman and local politician before shifting to a highly effective career in federal government service. He died in 1991.

Greg Ambrose is moving to the Department of Veterans Affairs to take over as deputy CIO for product development, a job that has been open since **Lorraine Landfried**'s departure in July 2014.

Ambrose was director of consular systems and technology at the State Department, where he worked on a modernization project that involved taking the Consular Consolidated Database, a massive system of 12 databases used to process passport and visa applications, from Windows 2003 to Linux. The goal is to give the stovepiped legacy systems a single look and feel.

Clockwise from top left: Denise Turner Roth, Brig. Gen. Kevin Nally, Martha Dorris and Greg Ambrose.

Last July, Ambrose led State's response to a systemwide data warehouse crash that left the government unable to handle requests for three days.

Kenneth Reynolds, Ambrose's deputy in the Bureau of Consular Affairs, will fill in as director on an acting basis, according to a State Department email message shared with FCW.

Dave McClure had been elected executive vice chair of the Industry Advisory Council.

IAC has a built-in succession plan in which an industry leader serves one term as vice chair before ascending to the top job post. Current Executive Vice Chair **Ted Davies** will take over for **Dan Chenok** this summer, and McClure will be in line to succeed Davies in 2016.

McClure, who retired from the General Services Administration in 2014 and is now chief strategist at the Veris Group, said he was excited to return to a larger role at ACT-IAC, particularly for a two-year stint that will span a transition in administrations.

"It's my kind of environment," he said.

The International Information Systems Security Certification Consortium honored a wide range of federal executives with its U.S. Government Information Security Leadership Awards, including:

- The Department of Homeland Security's **John Simms** for speeding the deployment of the Continuous Diagnostics and Mitigation program to 21 agencies while reducing costs.
- The Education Department's **Benjamin Bergersen** for making MAX.gov shared services the first agency-run software-as-a-service offering to receive authorization under the Federal Risk and Authorization Management Program.
- The U.S. Army's **Michael Redman** for identifying a training gap among Defense Department cybersecurity professionals and crafting in-house courses that more than 300 of his colleagues have now taken.
- The State Department's **Samuel Maroon** for his volunteer efforts teaching and managing the Wounded Warrior Cyber Combat Academy, a program that trains injured veterans for careers in cybersecurity.

— FCW staff

GSA.GOV / ZAID HAMID

Solving the Cybersecurity Threat Puzzle

The insider threat is a pervasive security problem for all organizations, and has been from the beginning of the Internet age. While various technology solutions have been used to deal with threats from outside the enterprise perimeter, little seems to have worked to counter those from the inside.

As mobile devices proliferate, and as the limits of the perimeter grow with the use of cloud services, the notion of how, where, why and by whom an organization's systems and data are accessed will also have to expand. Insiders then become not just the organization's employees, but also contractors, collaboration partners, occasional users and even malicious actors that penetrated peripheral defenses.

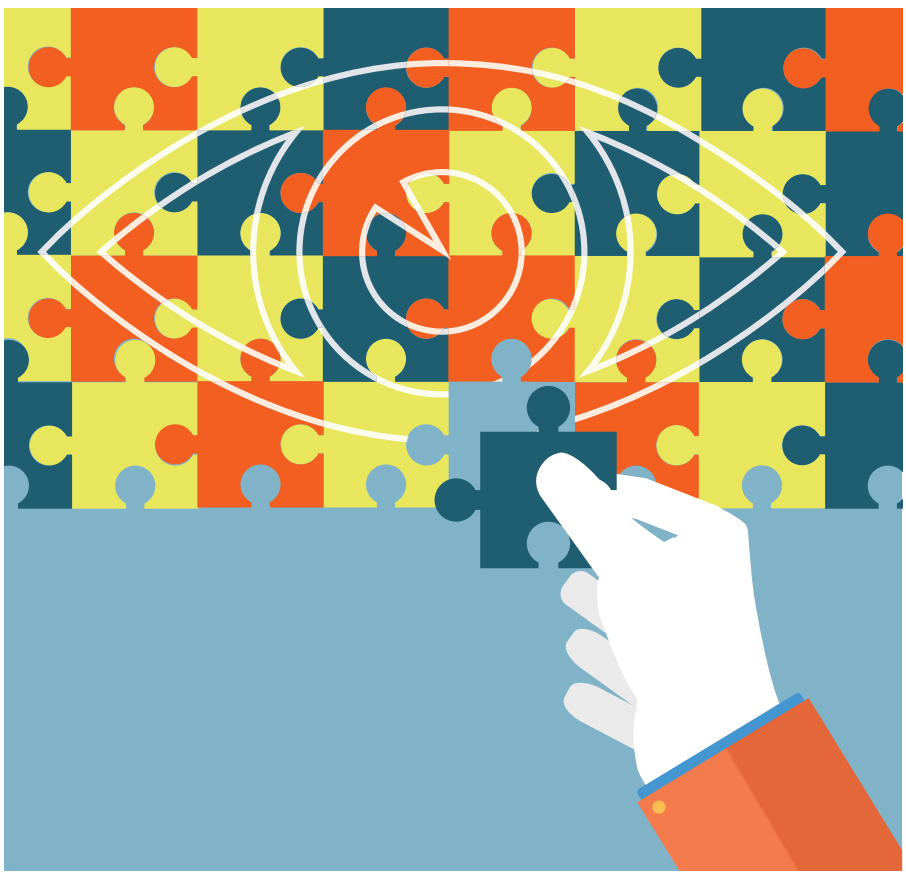
In its well-regarded Annual Data Breach Investigations Report for 2015, Verizon Inc. found that just fewer than 21 percent of all reported attacks were due to insider misuse. Over half of those attacks were due to an insider's deliberate abuse of access privileges. Not too far behind were inadvertent breaches such as when, by mistake or inattention, someone sends a sensitive document over an unsecured link.

Vormetrics' 2015 Insider Threat Report found that 93 percent of the US IT decision makers polled consider their organizations at least somewhat, if not more, vulnerable to insider threats. Six out of 10 believed privileged insiders posed the greatest threat.

Other studies point to a paradox in the way organizations react to this. A December 2014 survey by Market Connections, for example, found most of the government IT executives questioned considered insider threats at least as damaging as those from the outside, and in many cases much more so. Yet investments to combat those outside threats far exceeded those for insiders.

So many people these days view security as an interference to them doing their jobs and also have the skills to get around security protocols, a Defense Contract Management Agency executive said, and "people do what they want to do."

However, government agencies are now under orders to improve their insider threat defenses. Rattled by the 2010 WikiLeaks dump of sensitive government information, followed several years later by the Edward Snowden revelations, President Obama in 2012 issued a memo to heads of all executive departments and agencies requiring them to adopt "minimum standards" necessary to establish effective insider threat programs.



Shutterstock.com

Those minimum standards included, among others:

• The capability to gather, integrate, and centrally analyze and respond to key threat-related information.

• The ability to monitor employee use of classified networks.

That requires data on who in the organization is accessing what sources, when they are accessing them and how, and what they are doing with the information they are accessing. With all of that in hand, IT and security administrators can know if people are straying beyond their security privileges and, if necessary, build a case against them for potential action.

In September 2014, the Defense Department issued a directive to establish its own insider threat program, promising "an integrated capability to monitor and audit information for insider threat detection and mitigation."

It detailed just how extensive that information collection could be, since it said preventing insider threats requires the "integration and synchronization" of programs throughout the DOD, and the ability to monitor information across a wide swathe of sources, including counterintelligence, security, cybersecurity, and personnel management.

The good news is that organizations already have all the data they need for this. Network logs, email activity, new data sources such as social media, and even the physical comings and goings as people enter and leave buildings provide all the information required to establish insider threat monitoring and mitigation. As general IT security is strengthened, new applications and more complex sensors will constantly add to the number of data sources meaningful to cybersecurity.

The problem comes in how to turn this constant flood of unlike data into useful information that organizations can use to take action on insider threats, and do so in a timely way. That means not only being able to collect the information, but also maintain the who, what, when and where links so that the evidence trail is unbroken.

Typically, that comes down to being able to store, enrich and correlate information in a unified repository and provide a single access point for search and discovery capabilities. Only then, investigators or analysts can link information together while keeping all of the pedigree, provenance and attributions that are already attached to the information.

That's particularly important given the increasingly dynamic and complex threat scenarios organizations have to deal with. As they detect vulnerabilities and change security controls and policies to plug the gaps they find, insiders will find new and more innovative ways to get around the fixes and hide their activities, which require even more data sources and more complicated detection techniques. That generates even more, and more complex, information that has to be integrated.

Bringing all of this together in a way that gives an analyst a quick search and discovery capability, and an easy way to capture and maintain the relationships between all the various data and information, is what stumps most organizations today in building a defense again insider threats.

GETTING ACTIONABLE INFORMATION FROM A LOT OF DATA

The core of the problem lies not just in the amount of data that an organization collects, but in the kind of data that exists and the many different formats it can take. Combining and integrating that data is a big task in itself, but getting actionable information from it adds a whole other dimension.

> "THE CORE OF THE PROBLEM LIES NOT JUST IN THE AMOUNT OF DATA THAT AN ORGANIZATION COLLECTS, BUT IN THE KIND OF DATA THAT EXISTS AND THE MANY DIFFERENT FORMATS IT CAN TAKE."

The instances that might indicate an insider threat, sifted from the daily actions of hundreds or thousands of individuals in an organization that are being tracked, are few. The data that is actionable and available is therefore always very small, and represents an extremely weak signal on top of a very noisy environment. Add the fact that data sources can change very quickly, and things get even more challenging.

Depending on the size and breadth of an organization, even the same kind of data may mean different things to different people, and can be used differently in an investigation. A financial regulator institution would have a different need for data on who did what and where and when they did it than, say, another kind of organization

that puts greater importance on where something happened.

So, from the same dataset you can have multiple interests that have to be catered to, and each one has to be represented in the analytical model that's applied to the data since each of those interests will want to track different attributes.

The insider threat program launched by the Defense Department in 2014, for example, calls for monitoring and auditing information from sources that include counterintelligence, security, cybersecurity, civilian and military personnel management, workplace violence, antiterrorism risk management, law enforcement, user monitoring, human resources, IT access logs and any other source deemed necessary.

It's essentially a big data problem. That discipline is based on the fact that relational database management systems (RDBMS) that have supported the explosion of IT solutions over the past several decades cannot keep up with the volume of data that's now being produced.

Not only do they struggle with the structured data that is traditionally used in relational data bases, but incorporating the huge volumes of unstructured data that's now available requires enormous effort on the part of IT departments to extract, transform and load before they can be used. Then tack on the work needed to manage and integrate data sources, predefine queries, and build the analytical applications used for big data.

Still, a big data approach only goes part way to solving the problem for the insider threat. It helps to separate the large volume of irrelevant data from the more interesting stuff, but it still requires data analysts to examine that and apply context. Finding insider threats doesn't depend on seeing people just doing things; it's much more about people doing things at times and in places and ways that differ, perhaps in very subtle ways, from how they've done them before.

Even with big data that still takes a lot of time and effort. Analysts have to build and run complex queries and manually correlate multiple result sets. The ability to continually track a person's activities that way is very limited.

> "THE IDEA IS, AS FAR AS POSSIBLE, TO DEFINE AN OBJECT JUST ONCE AND, THEN OVER TIME, COLLECT AND ATTACH DIFFERENT SOURCES OF INTELLIGENCE ASSOCIATED WITH THAT OBJECT."

It's the same kind of situational awareness problem that the Defense Department has struggled with for years. It uses big data techniques to collect inputs from multiple different sensors and systems in order to analyze activities and develop intelligence it can use for its operations. But analysts still spend most of their time assembling known data.

The DOD is now developing an alternative to this data-centric method that uses object-based production (OBP) to give it a better and more timely insight into the relationships between various data, something it expects should also give it a better way of revealing gaps in its intelligence that are not yet evident.

OBP takes advantage of an approach that the military has used for decades in command and control. Instead of using the traditional relational data-centric model, OBP takes data and automatically associates it with a specific object, such as a building, a vehicle, or a person that are constant across all domains. New data can be attached to the relevant object, and over time relationships between objects can be identified, and constantly updated to reflect new information gathered from the real world. The idea is to define an object just once and, then over time, collect and attach different facts associated with that object. Agencies and communities of interest can share this information and be sure that they are all talking about the same object. Object includes multiple attributes, relationships, context (history, location and semantic), value-level security, provenance and pedigree (trustworthiness), time validity and periodicity. Beyond traditional attributes complex concepts can be attached to objects using free text, knowledge (semantic facts), documents, imagery, videos and links.

HOW OBJECT-BASED INTELLIGENCE WORKS

Over time, government agencies have built extensive knowledge environments using a collection of different database technologies, geospatial software and applications that can be used to extract information about insider threats, but none of them are enough by themselves. Also, in order for security analysts to work in their particular domains, very large databases would have to be

duplicated across multiple divisions of the organization.

And very few agencies have the ability to ingest and handle the full range of both structured and unstructured data needed to track network activity, the activity of staff, what is going on outside the organization, and then do an investigation and implement all of the reforms needed to trace, and protect themselves from, individuals and organizations.

MarkLogic's OBI solution is an example of a new generation of approaches to this problem that promise to provide at least some of the answers, while eliminating much of the complexities that come with legacy solutions. A single NoSQL database, designed to provide the kind of scale and security required by enterprises, combines the search and applications services that enables it to act as a single platform for data integration and information applications.

> "THE OBJECT-BASED APPROACH IS SO ATTRACTIVE TO MANY ORGANIZATIONS BECAUSE IT ALLOWS THEM TO CAPTURE AND USE INFORMATION IN WAYS THAT ARE MUCH CLOSER TO REAL-LIFE SITUATIONS THAN THE TYPICAL DATA-CENTRIC SOLUTION."

It represents the kind of flexibility that will be needed to handle the full range of insider threat information. It is document-centric, rather than data-centric as with traditional RDBMS, and stores documents both in JSON and XML, but can also store images, video, Microsoft Word, Excel PowerPoint, PDFs and other formats.

That's a far better demonstration of the data that's handled in and across organizations than with traditional databases. It also makes sure that much more of the institutional knowledge of experts can be captured.

The object-based approach is so attractive to many organizations because it allows them to capture and use information in ways that are much closer to real-life situations than the typical data-centric solution. The human brain naturally tries to connect location with people and organizations when people are faced with a new environment, and is designed to link concepts together semantically.

They can be linked with whatever association comes to mind. Individual A can be described as working for organization B, for example, or simply that A might be connected to B. Similarly, geolocation and temporal concept are also embedded in the object, another natural way to capture information. Allowing to answer complex questions such as "If A no longer works for B, why A is still accessing systems owned by B?"

MarkLogic's OBI framework enables each part of an organization and community of interest to use a number of different ontologies to define the object types and attributes that allow them to make connection with, and collect information on, the activity of the objects they are most interested in.

They can create multiple objects from the same data, for different communities of interest.

An important part of MarkLogic's solution is providing each community of interest with the ability to define all of the objects and their type dynamically. If each analyst is tracking an individual of interest, for example, and didn't have a database field with which to capture the addresses, they can just decide to start capturing addresses and can modify their view of the object without affecting any other community of interest.

Given that this information can be widely shared, security is a vital part of these kinds of solutions. MarkLogic's can enable different groups, even within the same organizations, to see just a subset of the object based on their security profile.

While organizations are worried about security and insider threats, these kinds of object-based solutions can also be used for other things than making sure people can't reveal mission critical information, such as compliance. That's also a major concern for agencies, and in some ways runs parallel with security issues, and many organizations are already using the object-based solutions to cover such things as IT portfolio risks.

154,000 files were purged from HHS.gov as part of a recent redesign

Experts: Hiring, firing and pay all need fixing

Federal workforce issues were front and center during a Senate hearing in May at which experts discussed the issues that leave cybersecurity and other critical positions unfilled.

The experts told the Homeland Security and Governmental Affairs Committee's Regulatory Affairs and Federal Management Subcommittee that the federal workforce has some serious problems. Employees often take on managerial roles to boost their pay, which can lead to a shortage of employees in technical roles and make it difficult for those managers to make good hiring decisions.

Dan Blair recommends that one-year probationary periods for new employees begin only after training has been completed.

"If you have to go into the management and supervisory roles to increase your pay, whether you feel you're suited for that or whether you really want to do that or not, I think it does a disservice to our technicians and to our managers," said Patricia Niehaus, national president of the Federal Managers Association.

She was not alone in criticizing the General Schedule classification and pay system. Subcommittee Chairman James Lankford (R-Okla.) said, "We've got to ask ourselves, 'Is this the right way to do this?'"

The experts offered some suggestions. For instance, "management should be a profession within the federal government rather than an additional duty," Niehaus said.

Dan Blair, president of the National Academy of Public Administration, recommended that one-year probationary periods for new employees begin only after training has been completed. "When managers…have to make a decision about whether or not to retain an employee, many of [the new employees] are still in training," he added. "Let them show that they can do the job rather than have a supervisor guess."

However, American Federation of Government Employees President J. David Cox warned against a one-size-fits-all probation policy, and he pushed hard for raising salaries for federal employees.

Citing Office of Personnel Management data, he said federal employees' salaries are an average of 35 percent lower than private-sector employees doing similar work.

Other studies that include the value of benefits have shown that federal employees earn more than their private-sector counterparts. A 2012 analysis by the Congressional Budget Office, for instance, showed that feds make 16 percent more in total compensation.

Although Blair and Niehaus recommended tying federal pay more closely to performance to attract talented professionals and incentivize current employees, Cox said federal workers need higher pay across the board and that sequestration should be ended.

He also disputed the notion that the system for getting rid of underperforming employees is overly complex. "The provisions are there to move in a very timely process," he said and blamed conflict-averse managers.

Others recommended a more flexible compensation system that could keep pace with the private sector in critical areas, including IT and cybersecurity.

"The current system promotes a workforce based on longevity rather than performance," Niehaus said. "The highest-performing employees should be rewarded with the highest rates of pay."

— Zach Noble

Can Wikipedia forecast the flu?

Researchers at Los Alamos National Laboratory say they have learned how to glean information that can be used to forecast outbreaks of flu and other infectious diseases by analyzing views of Wikipedia articles.

Understanding the dynamics of influenza and other infectious diseases and forecasting their impact are fundamental to developing prevention and mitigation strategies. To do that, Los Alamos researchers combined modern data assimilation methods with Wikipedia access logs and Centers for Disease Control and Prevention influenza-like illness (ILI) reports to create a weekly forecast for seasonal flu outbreaks.

The research taps into the tendency of people who have come down with the flu to search for information online. Researchers said Wikipedia access logs are highly correlated with historical ILI records and enable accurate prediction of ILI data several weeks before it becomes available.

The researchers' results showed that prior to the peak of the flu season, their forecasting method projected the actual outcome with a high probability.

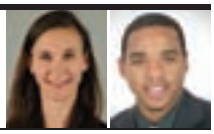
"The ability to more accurately forecast the flu season and other infectious diseases will transform the way health departments prepare for and respond to epidemics, ultimately saving lives," Los Alamos scientist Sara Del Valle said.

"We used techniques often seen in weather forecasting to iteratively tune a model of influenza dynamics based on Wikipedia observations so that our forecast agrees with the most current ILI data," said Kyle Hickman, a researcher at Los Alamos.

— Mark Rockwell

Commentary | KRIS VAN RIPER AND DYLAN MOSES

KRIS VAN RIPER is a practice leader and **DYLAN MOSES** is a research analyst at CEB.



Boosting employees' security awareness

By designing security training tailored to employees' behavior, agencies can quickly reduce risk — and save time and money

President Barack Obama declared cybersecurity a top priority for 2015, which seems timely given the series of high-profile breaches in recent months. The infiltrations of the Energy Department, Army Corps of Engineers, U.S. Postal Service and IRS signal that cybersecurity has truly become an issue of both economic and national security.

With most of the media attention focused on external hackers and cyber criminals, it can be easy to overlook internal risks, yet accidental employee breaches of information security policies are a frequent and critical threat to data security. CEB research shows that employee error contributes to 48 percent of all security incidents, while malware contributes to 20 percent and hacking represents just 11 percent.

And according to a recent poll by SolarWinds, 53 percent of federal IT professionals say careless and ill-prepared employees are the greatest threat to their agencies' security. Take, for example, the July 2013 IRS incident that started with simple human error and ended with nearly 100,000 Social Security numbers compromised in a public database.

CEB research shows that although the average organization invests significantly in employee security training and communications campaigns, most fall short of achieving compliance. In fact, we found a complete lack of correlation between spending and compliance.

By not considering the mindset of their employees when creating campaigns, chief information security officers (CISOs) consistently capture the wrong metrics and therefore misdiagnose compliance issues. Our research shows that leading organizations that focus on employee behaviors tend to conduct more effective training campaigns, which can decrease human error by at least two-thirds.

CISOs should consider the following elements when designing and implementing a security program:

Accidental employee breaches of information security policies are a frequent and critical threat to data security.

• **Understand employees' behavior.** The most effective campaigns identify the "why?" behind employees' lack of compliance, which can include a lack of awareness of policies or a lack of emotional commitment to information security. Capturing employee behavior requires a case-by-case assessment of how end users operate, what drives their actions and how they perceive the CISO's awareness efforts.

• **Craft different messages for different users.** Employees have different patterns of risky behavior, with most of the variability based on role and seniority. Leading CISOs tailor their campaigns for different groups with different risk profiles. They pay special attention to the content being delivered and how it's delivered. Recognizing a campaign's "look and feel" can increase the likelihood that employees will remember and act on communications.

• **Create an incentive program.** Detailed training and communications do not necessarily prompt a change in employees' risky inclinations. Instead, the most effective CISOs incorporate incentives for adopting safer behaviors as well as consequences for failing to do so. Our research shows that incentives, which can be as simple as recognition from a manager, can be just as productive as more costly training or communication efforts.

• **Benchmark employees' current awareness level.** Leading information security organizations measure compliance to trace the successes and failures of particular aspects of their awareness programs. Measuring employees' behaviors helps CISOs understand employees' perceptions and actions in order to address risky behaviors as soon as they arise.

Although the federal government faces many challenges in IT security, employee awareness is one area where agencies can quickly and effectively reduce risk. Keeping end users in mind when developing compliance campaigns can save agencies time and money while helping them better serve the public. ■

DAVID WENNERGREN
is senior vice president of technology at the Professional Services Council.

Cybersecurity: Valuing outcomes, not oversight

Although the government has made progress on cybersecurity, we need to make better use of the tools we have

Every day, new technologies and applications offer opportunities to change how we work, live and play. This frenetic pace is rivaled only by the ever-increasing number and sophistication of the cybersecurity threats we face.

We want to be always connected, from any device, from anywhere. Yet with each new capability that we embrace, new threats and vulnerabilities are introduced.

We must re-evaluate our cybersecurity efforts to ensure that we can quickly exploit new technologies to deliver more effective mission results. Today, the call for speed and agility is nowhere more crucial than in our cybersecurity policies and practices.

Progress has been made. Information assurance professionals used to have to plead that security not be an afterthought. We should applaud federal successes in identity management, public-key infrastructure, Trusted Internet Connections, common security controls, Joint Regional Security Stacks, data-at-rest encryption and continuous monitoring.

But despite heightened awareness and attention, many organizations are not operating at a fast enough pace to make use of important new technologies and proven best practices. And as is often the case, the impediment that most stands in our way is not the adoption of new technology but the acceptance of new thinking.

Through the use of the Common Access Card, the Defense Department significantly improved information and physical security, not to mention enabling electronic solutions to replace labor-intensive, paper-based processes. Yet many civilian agencies still use personal identity verification cards as little more than flash passes.

A number of cybersecurity threat vectors, not to mention barriers to information sharing, could be successfully addressed through the combination of strong identity management, attribute-based access control and security at the data level.

Today, the call for speed and agility is nowhere more crucial than in our cybersecurity policies and practices.

Another conundrum we face is the difference between oversight and outcome. Continuous monitoring provides far more value than a point-in-time focus on certification and accreditation. And although we have long touted the value of reciprocity and the goal of "certify once, use many," the adoption of cloud computing in the federal government provides a great example of a promising technology solution that is lagging in implementation.

It was great to see the recent press release from the Defense Information Systems Agency that highlighted 23 commercial cloud service offerings that had been granted provisional authorizations. Yet those proven offerings still require a DOD organization to conduct the assessment that would lead to an authority to operate — all for solutions that will not handle sensitive information and that have previously been granted a FedRAMP agency ATO or provisional authorization.

Those examples share two classic change management issues: the desire for personal control and a lack of trust. The processes we institute to address those issues must not take the place of what matters most: measurable outcomes that ensure mission results.

A world where we rally around a common goal of secure information sharing will be one where our security efforts help ensure the rapid adoption of new technologies and the ability to get the right information to the right person. Some laws, such as the Federal Information Security Management Act, must be changed, and new laws addressing liability and information sharing must be enacted.

But perhaps even more important than changing laws is changing attitudes to stay ahead of the threats we face and deliver the results we need. ■

TOM BAYBROOK is managing partner at Marbrook Partners.

It's not me, it's you

Handling difficult people at all levels starts with taking a more positive approach to the challenge

Consider the micromanager — the one who checks on progress frequently, demands too much of people's time, treats every problem as a crisis and generally makes the team miserable. How do you handle working with that type of difficult personality?

One of the complexities of working for a living is dealing with people who irritate you. They can be bosses, peers, employees or customers. Assuming that, like most people, you have not won the lottery recently and have limited immediate options for simply walking away, you must find a way to deal with difficult personalities at work.

A number of coping mechanisms come to mind, including avoidance, placation, cajolery, confrontation, behavior modification or plain old endurance with the hope that the person will change over time. Those approaches, however, are negative to neutral, and they generally result in making the situation worse or, at best, support the status quo. Why not take a more positive approach?

Assume, for the moment, that most people want to be successful and do a good job. Let's also assume that most people do not wake up in the morning planning to irritate you. Of course, a few people will fall outside those norms, but usually they do not stay in one job or place very long, so we'll discount them.

But even those people who fall within the norms have differing work values, management styles and personalities. The result might be an unhappy work environment. Whether you are the manager, the managed or a colleague, how do you handle those situations?

Start with the premise that everyone has a contribution to make. Your job — whether you manage up, down, across or outside the organization — is to determine what a person's most important contributions are and try to take advantage of those strengths.

> People generally like to do what they are good at, so identify their best traits and push them in that direction.

By focusing on contribution, you establish a productive work environment and build a pathway to success while limiting areas of irritation.

People generally like to do what they are good at, and they will excel at those activities, so identify their best traits and push them in that direction.

"Even my boss?" you might ask.

Yes. Consider those irritating, demanding management types mentioned above. What are their strengths? If a manager is good with customers, send her on the road. If another is highly analytical, sign him up for technical reviews. If she's a nitpicking editor, give her a lot of material to edit.

Whatever the strength is, get the colleague in question pointed in that direction.

Will there be a 100 percent improvement? Of course not, but life will be measurably better for everyone.

Likewise, determine the principal contributions of each of your employees, peers and customers, and focus on what they do best. Know their weaknesses as well, and avoid setting them up for failure. Do not depend on them to do well what you know they will not.

Managers can still give employees stretch assignments but should not leave them on their own. Understand that those assignments will take extra guidance and follow-up. One of managers' key responsibilities is to help people succeed.

What if that approach doesn't work in a particular case? What if someone truly is outside the norm?

Do it anyway. You will fare better trying the positive approach rather than continuing with a coping mechanism. And if the positive approach doesn't work, you'll then be justified in concluding, "It's not me — it's you!" ■

JOHN MARSHALL is founder and CEO of the Shared Services Leadership Coalition, a nonprofit organization supported by the federal IT and consulting industries and good-government community.

Shared services: Why legislation is needed

The White House could use a push to pick up the pace on shared services and lock in the benefits for future administrations

Comptroller General Gene Dodaro said it best: "Successful management reforms in the federal government need to have legislative underpinnings so they have permanence and consistency over time, no matter who's in the White House or who's leading departments and agencies."

The history of shared services proves his point. In 1983, the Agriculture Department's National Finance Center opened its doors to government customers outside USDA for payroll services, but it wasn't until 2009 that the Office of Personnel Management declared victory when the entire government was served by four cross-government e-payroll providers.

Five presidential administrations spanned those 26 years. Shared services and e-payroll were dropped, rebranded or lost in the shuffle at each transition. Without legislation providing a bridge from one administration to another, shared services languished as a non-priority.

Management legislation drives progress by giving agencies permission to do things and by pushing the bureaucracy to get things done. Landmark bills such as the Chief Financial Officers Act and the Cling-er-Cohen Act empowered CFOs and CIOs, respectively, by giving them new structures and authorities, but most of the power was in the push to implement best practices defined in the legislation.

Legislation can accelerate shared services by creating a vision of a modern future state and directing the executive branch to pick up the pace in defining key roles and responsibilities, setting service standards and metrics, creating a real shared-services marketplace, encouraging private investment, promoting competition to drive scale and innovation, and empowering customer agencies to choose their providers.

> Putting the requirements into law would ensure continuity and sustainability under future presidents.

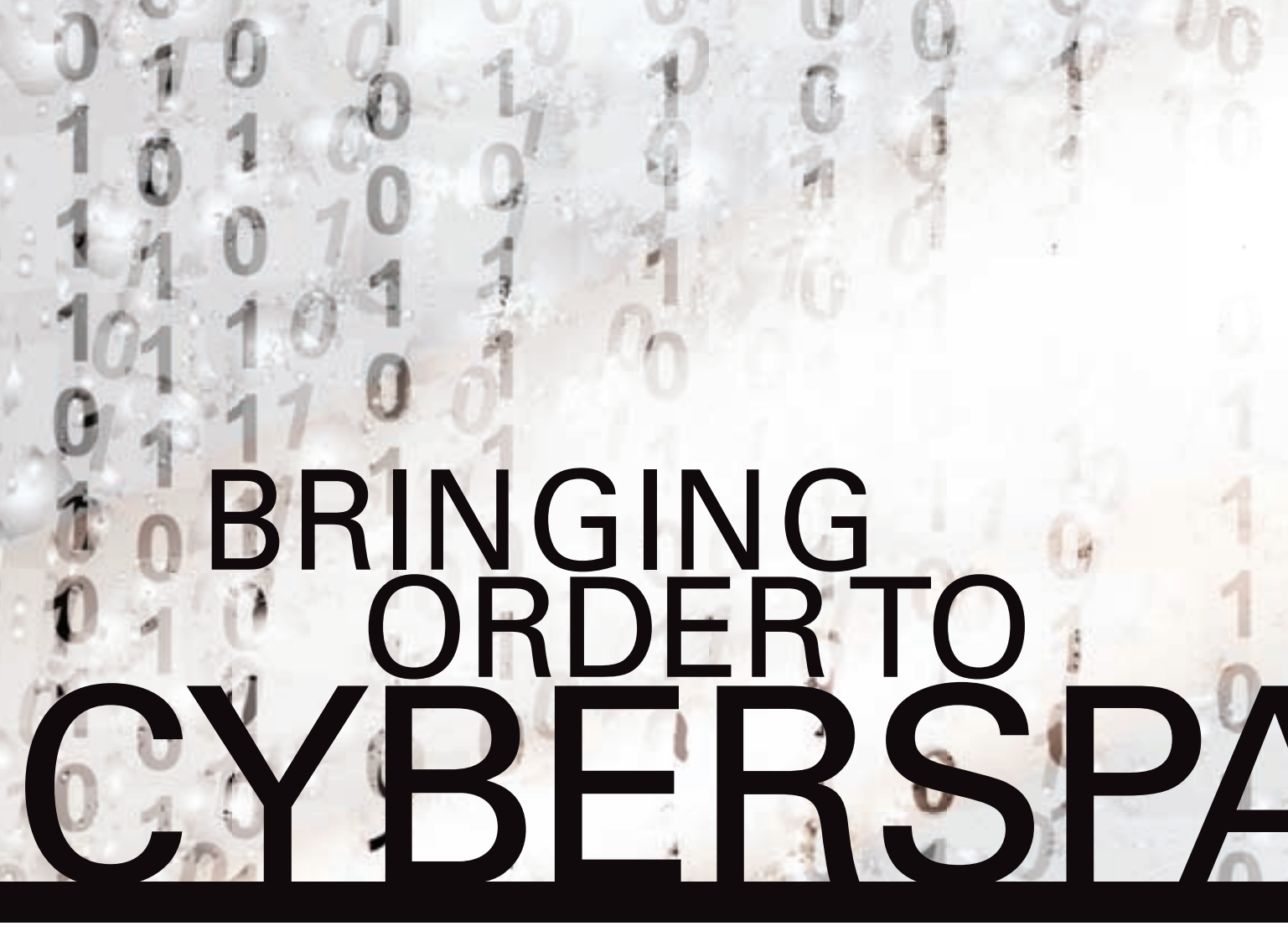
The good news is that the Obama administration is already doing many of those things. Putting the requirements into law would ensure continuity and sustainability under future presidents.

The administration needs permissions, too. Federal Shared Service Provider business models date back to the 1930s and 1940s and were last updated in legislation in 1994. FSSPs are intended to operate on a cost-recovery basis, and they cannot charge customers more than their own cost. Although most have authorities (on paper) to accrue reserves for contingencies and future modernization needs, congressional appropriators tend to oppose the use of reserves, which they view as hoarding money for unauthorized purposes.

Without the ability to finance modernization organically — and without the clout to compete with the higher-priority mission needs of their host agencies for scarce appropriated funds — FSSPs get stuck in antiquated, sub-standard platforms with unhappy, captive customers. Legislation should authorize business-like investment practices by all FSSPs and encourage their responsible use. Concerns about abuse of reserves could be addressed by transparent business practices, reporting, audits and oversight.

The stars are aligned as never before. The Obama administration appears supportive. Strong advocates at the Office of Management and Budget and key agencies are pushing the envelope and want to ensure a clean hand-off to the next administration. The Republican majority in Congress needs to show that it can govern. There's palpable energy in the industry and good-government community around a vision of a dynamic, competitive, public/private marketplace in which competition drives commercial investment, scale and innovation. And there's hunger in the country for bipartisan action on big national challenges.

Last questions: If not now, when? If not us, who? ■



BRINGING ORDER TO CYBERSPA

The quest for command and control in the online arena

BY SEAN LYNGAAS

Lt. Gen. Edward Cardon goes about his work as head of Army Cyber Command with the subdued intensity of someone who knows he will be at it awhile. The soft-spoken Californian is trying to build a cyber workforce, and he is clear about where that effort is falling short.

Some private-sector IT specialists want to "come work for us for a year or two, but they don't want to… be there for 20, and we don't have a mechanism to really do that," Cardon said in a recent interview at the command's offices in Fort Belvoir, Va.

Cardon is part of a generation of military officers whose job is to draw clearer lines around the Defense Department's role in cyberspace. Those commanders typically have a blend of battlefield and systems management experience, but rarely are they IT experts. They help shape doctrine and give orders, while the "cyber warriors" in control rooms around the country and the world conduct network defense and potential hacking of adversaries.

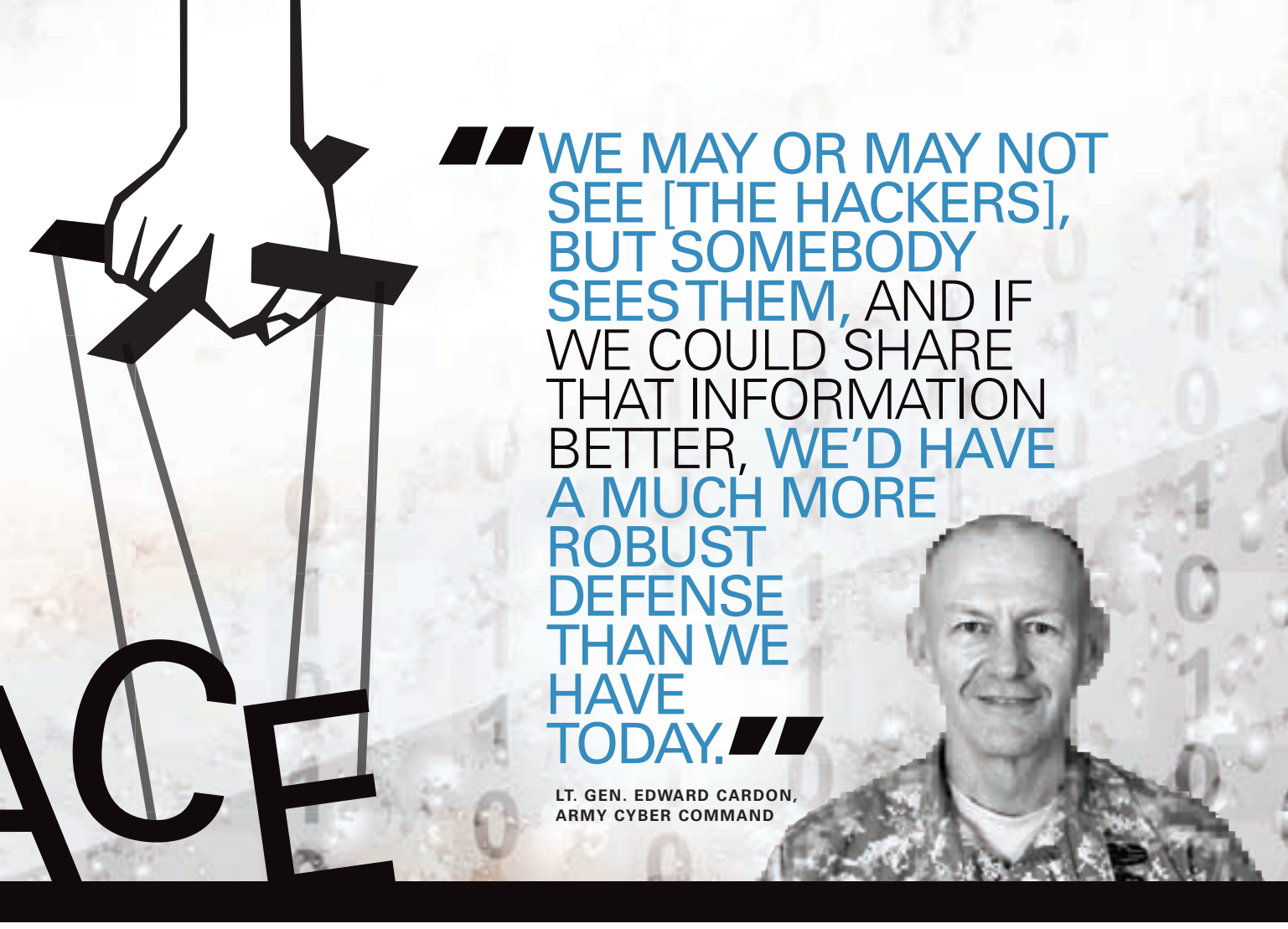
Since the American military declared cyberspace an operational domain in 2011, it has not been a question of if but how the Pentagon will organize its capabilities.

There has been no shortage of ideas inside and outside the Pentagon for how to better use people in the nation's cyber defense. Cardon in particular has been outspoken on the subject.

At a February cybersecurity conference in Washington, he said that, given the diffuse nature of digital networks, "command" might not be the right word for organizing cyberspace. Instead, "maybe it's the way that we organize against very specific missions," he said. Those missions then become opportunities for leadership, and recruiters find the "skills and attributes that we need to be able to do that."

In other words, Cardon is interested in creating teams that, contrary to centuries-old notions of chain of command, are driven by specialized skillsets rather than hierarchy.

Although "command" is still the operative word for his perch, Cardon's thinking on the issue points to a less hierarchical approach to cyberspace. He was a brigadier general in Iraq during the 2007 surge that pushed the number of U.S. troops there to about 170,000, and he wants to apply that experience to cyberspace.



> "WE MAY OR MAY NOT SEE [THE HACKERS], BUT SOMEBODY SEES THEM, AND IF WE COULD SHARE THAT INFORMATION BETTER, WE'D HAVE A MUCH MORE ROBUST DEFENSE THAN WE HAVE TODAY."
>
> LT. GEN. EDWARD CARDON, ARMY CYBER COMMAND

"When you have a hierarchy that works against a network, it doesn't work as fast as the network. And so in Iraq, what happened is Gen. [Stanley] McChrystal recognized that there was a lot of information coming in," he said, referring to one of the now-retired architects of the surge and the military's broader efforts to counter the decentralized insurgencies in Iraq and Afghanistan. "But the information was organized geographically and not against the network. And so by creating a place where everyone could come together, he in effect created a network to work against the network. You can instantly see this application to cyber because the threat isn't geographically constrained."

In the same vein, Cardon has floated the idea of applying the concept of "fusion cells" — small teams of Special Forces and intelligence officers dispatched to Iraq in 2008 — to cyberspace. Whereas the fusion cells' targets were Iraqi insurgents, Cardon's cyber cells would target intruders lurking on DOD networks. The ability to pinpoint those hackers would rest on better information sharing.

"We may or may not see [the hackers], but somebody sees them, and if we could share that information better, we'd have a much more robust defense than we have today where we all sort of operate in our lanes," he said.

A growing force against growing threats

On the one hand, the military brass portrays the buildup of Cyber Command as a steady march toward 6,200 employees. But seen in another light, the Pentagon's cyber posture has been a reactive response to a threat that has been steadily growing.

In the past several years, multiple intrusions into Pentagon networks have sounded alarm bells for military leaders. William Lynn III, a former deputy Defense secretary, called a 2008 hack of classified military computer networks "the most significant breach of U.S. military computers ever" and "an important wake-up call." Another flash point came in 2013, when Iranian hackers embedded themselves in the unclassified portion of the Navy Marine Corps Intranet.

The most recent shot across the Pentagon's cyber bow was a Russian intrusion that Defense Secretary Ashton Carter disclosed on a recent trip to Silicon Valley. The hackers had breached an unclassified DOD network via "an old vulnerability in one of our legacy networks that hadn't been patched," he said.

Carter added that DOD network defenders were able to drive the Russians off the unclassified network. But whether such a cleanup operation can continue to limit the damage done to some of the largest, richest networks in terms of intellectual property is

> **COMPUTER WARFARE IS BEING THRUST UPON MOST OF THE SENIOR [MILITARY] LEADERSHIP,** AND I DON'T THINK MOST OF THEM HAVE A FOUNDATIONAL KNOWLEDGE OF HOW PACKETS GET ROUTED, **HOW APPLICATIONS GET CRAFTED.**
>
> CARL HERBERGER, RADWARE

another question altogether.

"We're getting faster and faster with our operations," Cardon said. "The challenge we still have is the disparate nature of the networks."

Barriers to private-sector collaboration

Despite Cyber Command's focus on offensive and defensive operations, cybersecurity analyst Richard Stiennon likes to think of the command as a "centralized IT security department" for the Pentagon, albeit one that is stifled by acquisition regulations.

Cyber Command "can only buy things that the big contractors have figured out how to sell," said Stiennon, who is founder and chief analyst at IT-Harvest. "So they can't go to Silicon Valley and talk to the startup that's got the solution for Windows XP. They can't get the latest breach-detection solution because no startup in their right mind would take a year and a half out to go through the [federal] qualification process."

Cardon acknowledged that barriers to entry are a sticking point in his outreach to the private sector. A lot of technology firms don't want to deal with the government because they find the process cumbersome, he said.

"We have to figure that out because we're going to need them because the money that they're investing in science and technology and research and development dwarfs the Department of Defense," he added.

The federal acquisition process is one impediment to the greater interaction between Cyber Command and private-sector IT experts sought by Cardon and his boss, U.S. Cyber Command and National Security Agency leader Adm. Michael Rogers. Another hurdle is the cultural differences between IT experts who have spent their careers in the private sector and Pentagon officials who view cyberspace as a warfighting domain.

"Cyber, to us, is a form of a maneuver," Cardon said. "So to me…the danger is the IT world views things through [what] I call the role of the help desk. Just make my computers, phones, everything work, [and] I'm happy, as opposed to thinking, 'Hey, this space is contested and you have to protect it.'"

Regardless of how Pentagon officials view cyberspace, many of them are looking at it through nontechnical eyes, said Carl Herberger, a former electronic warfare officer in the Air Force.

"Computer warfare is being thrust upon most of the senior [military] leadership, and I don't think most of them have a foundational knowledge of how packets get routed, how applications get crafted" and other technical activities, said Herberger, who is now vice president of security solutions at data security firm Radware.

Yet military leaders generally won't be the ones defending DOD networks. That is the work of the cyber forces that Cardon and his counterparts in the other military services are developing. The Army cyber force will consist of 41 protection teams that will defend Army networks from intrusions, and Cardon said the service is making progress in recruiting.

"We had a lot of failure rates in the beginning," he said, adding that some of the early recruits for the cyber force lacked the technical aptitude for the job. But now candidates take an exam that gauges their technical skills and their likelihood of passing the training process.

Those cyber soldiers will enter a contested space that Cardon and other Pentagon leaders believe they have no choice but to enter.

"Sometimes you hear the term, 'We're militarized in cyberspace.' No, that's not it at all," he said. "In fact, the struggle is already ongoing between criminal groups, nation-states, etc. The question is, in the construct of military operations, how do we use cyber?" ■

ENGINEERED FOR YOU @ THE SOURCE

Join us August 3 – 7, 2015 for TechMentor 2015: Datacenter Edition, focused entirely on making your datacenter more modern, capable, and manageable through 5 days of immediately usable IT education.

SAVE $300!

WHEN YOU REGISTER BY JULY 1

USE PROMO CODE **TMJUN1**

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

THE AGENDA FEATURES:

- 75-minute topic overview breakout sessions
- 3 hour content-rich deep dives
- "Hands on" labs with your own laptop

CONTENT AREAS INCLUDE:

- Windows PowerShell
- Infrastructure Foundations
- Runbook Automation
- Configuration and Service Management
- Datacenter Provisioning and Deployment

EVENT SPONSOR: Microsoft

PLATINUM SPONSOR: GRIDSTORE

GOLD SPONSORS: GOVERLAN, pluralsight

SUPPORTED BY: Redmond Magazine, Redmond Channel Partner, Virtualization Review

PRODUCED BY: 1105 MEDIA

TECHMENTOREVENTS.COM/REDMOND

Through computer forensics training and internships, veterans are helping Immigration and Customs Enforcement tackle a backlog of child exploitation cases

Joe (left), shown here with fellow students Robert and Dianne, said HERO Corps offers an "opportunity to pick [a mission] and do something we want to do."

FINDING A NEW MISSION

BY SEAN LYNGAAS

Service-disabled veterans are finding a new mission in the fight against online child predators.

For the third year running, former warfighters have been trained to help the Department of Homeland Security's Immigration and Customs Enforcement process an immense backlog in child exploitation cases.

Virtual warehouses full of case data sit unexamined on servers around the country, and that backlog has weighed heavily on Brian Widener, who leads a computer forensics unit at ICE.

"How many victims are sitting there on a computer for X number of months because we didn't get a chance to get to it?" he said.

ICE's computer forensics teams processed 3.9 petabytes of data on child exploitation cases in 2013 and 5.2 petabytes of data in 2014, according to Widener.

The clear need to increase staffing led ICE to create a yearlong program that trains veterans in computer forensics so they can join the Human Exploitation Rescue Operative (HERO) Child Rescue Corps.

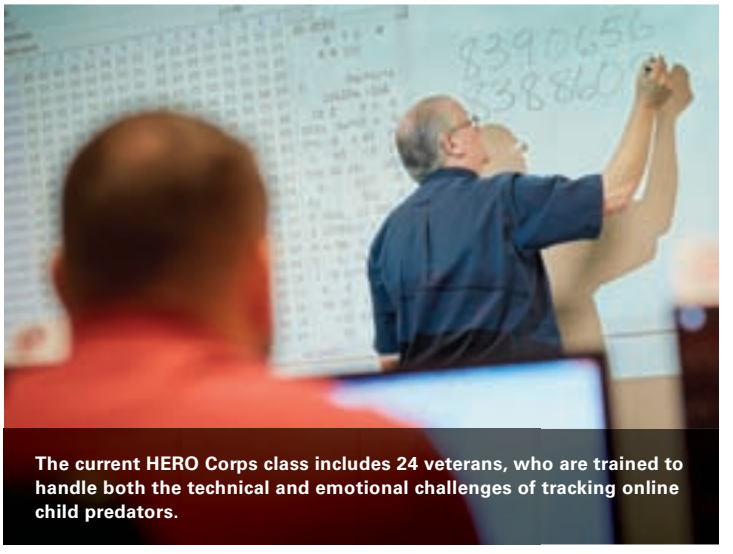
The program has expanded beyond the veterans of Special Operations Command who initially participated to include veterans of the National Guard and Reserve. ICE said it has hired several program graduates as computer forensic analysts in its Homeland Security Investigations division.

The application process is competitive. From a pool of 94 applicants, 24 veterans were chosen for the latest class. The curriculum is both technical and emotional, but applicants do not necessarily need technical skills to apply. Computers are just one "component of the battle on child exploitation," said Joseph Arata, ICE's chief of strategic recruitment.

Multilayered training

The first three weeks of the course focus on the gravity of the mission, and the veterans are trained to cope with the trauma of processing graphic and disturbing images of child exploitation.

Many of the veterans "are driven more than anything else in life by wanting a new mission," said Grier Weeks, executive director of the National Association to Protect Children, the program's nonprofit partner in conducting the immersion training. "It's been amazing to see how they grab hold of this mission."



The current HERO Corps class includes 24 veterans, who are trained to handle both the technical and emotional challenges of tracking online child predators.

DAVID WIEGOLD

After gaining insight into the underworld of child predation, the veterans spend eight weeks in computer forensics training at ICE's Cyber Crimes Center in Fairfax, Va. They start with the basics, such as creating hash values to catalog digital images. Within two to three weeks, the veterans have typically earned a CompTIA A+ IT security certification, according to Widener.

Software vendors then teach the veterans how to use platforms such as EnCase to log evidence. And the endgame is always in mind: Last year, trainees took part in a moot court in which lawyers grilled them on the evidence they had unearthed.

The third part of the program is a 10-month internship at ICE field offices across the country, where the veterans work side by side with investigators, often processing evidence after a warrant has been served.

"They're an integral piece right from the get-go," Widener said.

Inspired by their children

Two of the veterans in the program said they were inspired to participate because they have young children. Mark and Joe asked that their last names be withheld for privacy reasons.

The more Mark heard about the program from a friend, the more it "resparked that interest and that motivation to continue to serve my country — not only for the country but for the kids themselves, the victims," he said.

"It's a good mission," Joe said. "Sometimes we don't get to pick and choose our missions in the military.… But here, now that we're out…we have this opportunity to pick and do something we want to do, so this is important to us."

Joe, a multiple amputee, said he had originally wanted to be an investigator in child exploitation cases but realized that "for every one investigator, there [are] 35 dudes punching on computers, pulling up information that they use to build the case file. For me, I knew that switch had to be made to the technology side." ■

Knowledge transfer through discovery

Rules and data are relatively easy to share, but capturing an organization's deep, experience-based knowledge requires special effort

BY DOROTHY LEONARD, WALTER SWAP AND GAVIN BARTON

A fully realized knowledge transfer initiative requires substantial resources — financial, time and personnel. Yet the need for expertise to be passed on, and the costs of not doing so, must be recognized. Most organizations do not have knowledge transfer built into their operations. Instead, they need to make special efforts to transfer know-how. (In our survey of CIOs, CTOs and HR executives, only 23 percent indicated that their organization had a specific program dedicated to knowledge transfer.)

In the face of a lack of resources, your temptation will likely be to resort to lectures by the experts to the learners as the most expeditious mode of transfer. You know that you can't possibly re-create expert decision-making and diagnostic capabilities in learners' minds that way. Yet those deep smarts are what your organization truly needs. And allowing the learner to actively discover the knowledge can be a very effective strategy.

An example of discovery in action

The U.S. Army's Leader Challenge embodies active discovery in the classroom. An experienced military leader (usually through video, but sometimes in person) poses a dilemma that he or she has personally experienced in the field. Here's an example:

> Most organizations do not have knowledge transfer built into their operations. Instead, they need to make special efforts to transfer know-how.

In Iraq, the U.S. platoon leader has been on an extended patrol and is returning to base when an improvised explosive device (IED) kills one of his soldiers. After personally carrying the dead soldier to the medevac helicopter, he receives an order from the company commander. The leader presents the challenge he faced to a class as follows:

"Coming back from an all-night foot patrol, Sgt. H. was hit by an IED. He didn't make it. After getting him medevac'd out, I began thinking about what I was going to tell the platoon once we got back to our base. Then, the commander called and gave me a direct order to clear the nearest village, where the guys who put in the IED could be located — a mission that would easily take eight hours. My guys were out of food and water, were already physically smoked, and they were pissed off about Sgt. H. He was easily the men's favorite team leader, and there's no way those people [Iraqis] didn't know about that IED. Then my trusted platoon sergeant tells me, 'Sir, there is no way we can do that mission. Look at the guys!' At that point, my company commander called again to find out why I wasn't moving to the village. What do I do?"

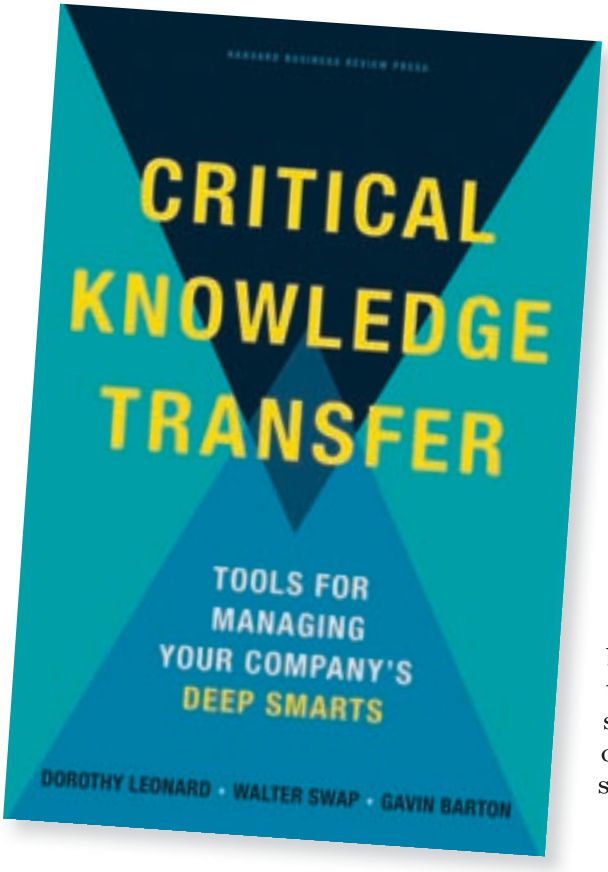
The classroom of learners now has the opportunity to discuss what to do, including thinking through potential second-order effects, both in the moment and long term. After exploring the possibilities and potential consequences of each action, the participants watch the second part of the video, which reveals what the platoon leader did. He occupied a building in the village where he took a tactical pause

to refit with water and to explain to his men what [had] happened and what their new mission was. The platoon then conducted the mission and returned to base.

The objective of having the learners actively grapple with a complex issue such as this one before being told how it was resolved is to instill judgment — wise decision-making is a hallmark of deep smarts. Learners are warned that the solution reached in a particular case was not the only possible solution — perhaps not even the best. There is no way that the soldiers can be prepared for all contingencies by remembering specific solutions. But these learners will have to make such decisions quickly, using the best information available at the time; the Leader Challenge is a kind of simulation of the real world in which the soldiers will lead.

Feedback from participants included such statements as: "This works. How do I get more of these challenges?" Not only did the challenges build confidence in decision-making, but the exercise also helped the learners figure out what they didn't know and where they had been overconfident.

Discovery exercises similar to the Army's are deployed effectively in business settings as well. Using vignettes for training has produced a statistically significant improvement in situation awareness, sense making and planning skills. For example, Holly Baxter, the chief scientist at Strategic Knowledge Solutions, recounts a technique that begins with a subject-matter expert preparing a scenario of a situation that required a decision. The background and other relevant information were provided, but not the action taken by the subject-matter expert. The scenario was presented to the knowledge recipients, who shared with one another their thoughts, including the pros and cons of various possible decisions. Only then was the actual decision taken by the expert presented. Baxter describes this method as "a simple technique that puts students in the moment and gives surrogate experience, which enhances knowledge transfer."



Simulations in the hands of individuals who have no real-world experience can lead to miscalculations. Product designers report saving lots of money avoiding the necessity of building physical prototypes by using simulations. At the same time, though, says Ashlee Vance, some critics see drawbacks in simulations:

"Design experts say they worry that young engineers now place too much emphasis on simulation and not enough on knowing how to build physical objects. Ultimately, it's an engineer who establishes the

The objective of having the learners actively grapple with a complex issue...is to instill judgment — wise decision-making is a hallmark of deep smarts.

constraints of the software, and setting the simulation parameters requires awareness of the physical world's complexities. '[Practice with simulations] won't make a bad engineer good,' says Jim Cashman III, CEO of Ansys, the largest producer of simulation software. 'It will make a good engineer great.'"

And that is what we are after — experience building that creates deep smarts. Computerized simulations employed to train airplane pilots or doctors in medical school build tacit knowledge through repeated, highly realistic experiences. Be thankful that the pilot on your next flight and the surgeon who replaces your knee, hip or heart had experience with simulations. Such simulations allow the user to accumulate vicarious experiences, from which learners will derive principles of decision-making and behavior and will develop the sensory skills that help build their expertise.

Software-based simulations are expensive to build and are not a likely option for transferring the deep smarts of a particular individual or group in your organization. However, discovery exercises like the Army's Leader Challenge are well within your reach, given the ease of video creation.

We know of a worldwide construction company whose managers puzzled over how to transfer the expertise of their troubleshooters without constantly flying these experts around the world. One solution the managers came up with was to videotape common construction problems, such as water damage from inadequate preparation of walls. The YouTube-like video did not have high production value, but the stains and crumbling stucco from the problem were clearly visible. After some context was provided (climate, age), workers in far-flung regions of the company were asked to view the video, diagnose what had happened and suggest a remedy. Only then was the cause explained and the preventative steps demonstrated, again by video.

That is what we are after — experience building that creates deep smarts. Computerized simulations employed to train airplane pilots or doctors in medical school build tacit knowledge through repeated, highly realistic experiences.

Similarly, in your organization you can create short text vignettes of dilemmas specific to your operations. The critical-incident technique we described in chapter 5 is also a form of simulation, although it does not have the element of discovery unless you take the story in pieces, asking at various points what those unfamiliar with the details might have done, what information they might have sought or whom they would have contacted. If you do so, the critical incident begins to approximate the cases that are used as text simulations in so many business school classrooms around the world.

Simulations, guided experience and discovery exercises all have the same objectives. First, they all build, through repeated decision-making, a repertoire of experiences and associated patterns on which learners can draw when considering possible responses. Second, these techniques all create a relatively safe environment in which to fail forward — that is, to learn from making wrong decisions without penalty to the learners themselves or others. Failure is highly memorable, so these experiences are a low-cost way to imprint system thinking — that is, to learn to anticipate possible implications of an action on others' subsequent decisions and actions. Third, these techniques all create a sense of self-efficacy in the learners [and] enhanced confidence in their ability to address future situations and problems.

The effectiveness of all these methods is best determined by the ability of the learners to demonstrate expertise in the real world. The usual separation in time and situation between the learning process and its eventual outcome makes evaluation difficult — but not impossible. ■

Visual Studio LIVE!

EXPERT SOLUTIONS FOR .NET DEVELOPERS

vslive.com/sf

San Francisco

JUNE 15-18

THE FAIRMONT, SAN FRANCISCO, CA

SAN FRANCISCO Code Trip

NAVIGATE THE .NET HIGHWAY

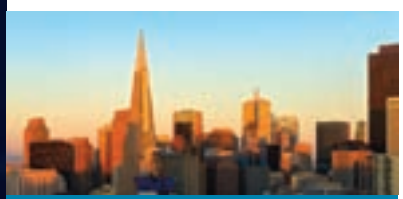
CODE BY THE BAY

Visual Studio Live! returns to **San Francisco June 15 – 18** for the first time since 2009! Bring on the cable cars, Chinatown, Pier 39, Alcatraz, and the Golden Gate Bridge. We can't wait to Code by the Bay!

Join us as we explore the latest features of Visual Studio, JavaScript/ HTML5, ASP.NET, Database Analytics, and more over 4 days of sessions and workshops. Code with industry experts, get practical answers to your current challenges, and immerse yourself in what's to come on the .NET horizon.

DEVELOPMENT TRACKS INCLUDE:

- Visual Studio / .NET
- Web Development
- Cloud Computing
- Mobile Client
- Database and Analytics
- Windows Client



SESSIONS ARE FILLING UP QUICKLY

REGISTER TODAY!

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

Use promo code SFJUN1

SUPPORTED BY

Microsoft | Visual Studio | msdn magazine | Visual Studio MAGAZINE

PRODUCED BY

1105 MEDIA

vslive.com/sf

'You can have a mindset of moving quickly'

Box CEO Aaron Levie discusses innovation, the "black box" of government and getting Silicon Valley to engage with agencies

For the closing session of this year's Management of Change conference, ACT-IAC invited Aaron Levie, the 29-year-old co-founder and CEO of Box, to discuss technology trends and leadership strategies. The cloud-based document collaboration company went public in January and is now valued at nearly $2 billion.

FCW Editor-in-Chief Troy K. Schneider sat down with Levie shortly before his May 19 presentation.

Not to put too fine a point on it, why are you at MOC? Cambridge, Md., is a long way to come for a few hours at a federal IT conference.
Yeah. [laughs] I thought it was a lot closer to the airport.

I'm here because we're ramping up our investment within the federal space pretty aggressively. Starting a couple years ago, we saw that our product was being pulled into federal agencies. We recognized that there was a huge opportunity to make a pretty big dent in how agencies collaborate, share and actually work together.

Was there a catalyst that prompted you to say, "Hey, the public sector is actually a place we should focus on and worth the investment to meet the security and acquisition requirements"?
In Silicon Valley, the government IT and agency ecosystem is very mysterious. It's this black box that we don't fully understand. You hear stories about billion-dollar IT projects gone wrong. It's this confusing landscape that you tend not to pay attention to.

But it became obvious that actually these organizations look a lot like the same organizations we serve in the private sector. They have the exact same talent issues. They have the same resource constraints. They're trying to get more efficient, more productive and more innovative.

Somewhere along the way, we recognized that if agencies looked exactly like Procter and Gamble, General Electric, Eli Lilly and the hospitals we serve, then we could probably have a pretty big impact.

Has government proven to be a different beast or is it just another regulated sector?
There are unique flavors of the challenges and of the things that we'll run into but nothing that is operationally different from the work that we had to do to get into financial services or to get into health care.

In fact, in some industries, I wish there were a sort of FedRAMP equivalent because it creates a very nice standard across the ecosystem of how to adopt these kinds of technologies. In the federal space, it's nice to have that level of consistency.

What does success look like for Box in the federal space?
We'd like government to run better. We think technology can actually be that bridge. We can be that bridge between agencies. We can be that bridge between teams. We can be that bridge between agencies and the outside world. We think that with the right technology — not just Box, but lots of these up-and-coming platforms — the government can just be more efficient, be more productive.

That translates into better services, better regulation, better costs. Those are all things that are incredibly important. That's the ultimate goal.

Are there lessons that you think agencies can learn from how Box operates — not just the tools it provides, but the way your team works together?
Yes! Now, we have a different set of factors in our business. We don't have the procurement policies that government has. We don't have the hiring policies. We don't have a lot

We think that with the right technology — not just Box, but lots of these up-and-coming platforms — the government can just be more efficient, be more productive.

of the legacy that any large organization or institution has.

But I think the thing that we can and we do share is you can have a mindset of moving quickly, of being disruptive, of trying to find edges and the boundaries of what is possible.

Some agencies already do that, for sure, and some we want to help catch up to that.

There are methodologies that get you there. There are certainly agile methodologies. But there's also just the mindset, in general, of impatience: Why do things happen in the timescales that we're seeing? Why can't they be a third or half or a fourth as long?

What about picking partners? There is a lot of teaming on federal contracts, and Box seems to be both collaborating and competing with many of the bigger names in tech.

Most of the partners that we're coming into the federal space with are purely complementary. They're providing a government infrastructure function for us. That's a little bit different than what we do in the software space, where we both partner and compete with Microsoft. We partner and compete with Google.

It takes an understanding that the entity is different from the product. We can partner with Microsoft even if we compete with a product of Microsoft's. We've had that mindset since Day One. And now Microsoft finally has that mindset, too. I think that's a big change that's happening with a lot of the big tech companies right now.

You were invited to MOC because people wanted to pick the brain of a Silicon Valley executive, but are there things you're trying to learn from those in the government space?

All of the domain of government, I'm learning constantly. Most of my time out here is actually just listening. What are the pain points? How is work changing? What do you wish technology could do that it doesn't do? That gives me a better sense of where there are the points of friction or misalignment between the Valley and D.C. and what can we do to more broadly actually create that alignment.

And separate from "can we get government to run better?" is "can we get government to be an attractive place for Silicon Valley to engage with?" That's going to be a unique challenge because in Silicon Valley, you don't want to be held up by regulation or bureaucracy. You want to be able to move as quickly as possible, so that leads a lot of tech companies in the Valley to not necessarily engage with D.C.

It would be great if we could figure out a better, more common way to work together. ■

DRAGUTIN CVIJANOVIC

Striking a much-needed balance on data access

A bipartisan pair of former agency executives explores the issues involved in the LEADS act and giving law enforcement access to data stored in other countries

BY KAREN S. EVANS AND JULIE M. ANDERSON

These days it's rare when members of both parties find consensus on any issue, let alone on actual legislation before both chambers of Congress.

As two appointees who have served in different presidential administrations, we don't see eye to eye on every issue. But we do share common ground in our support of the Law Enforcement Access to Data Stored Abroad (LEADS) Act.

The bill is a bipartisan opportunity to improve international law enforcement practices while protecting the privacy of individuals at the same time.

First a bit of background: The rules governing law enforcement's access to electronic communications are nearly 30 years old and were established long before the advent of email and cloud computing.

In light of today's vast technological advancements, those laws are outdated and ineffective.

In the discussion that follows, we outline how the LEADS Act clarifies that U.S. warrants do not apply to non-U.S. citizens' email messages when they are stored abroad, and we explore the issues of data access, fairness for all parties and international cooperation.

Who should be granted access to this data?

Evans: Without updated laws and procedures, any government could request access to anyone's email correspondence through the respective technology provider. In today's world, email messages are often stored in a different country from where they were drafted. Our national security is threatened if we participate in a system that allows other countries, such as Russia and China, to have access to our citizens' email messages without authorization.

Anderson: Long-standing treaties and established processes govern who has access to personal correspondence across borders. The LEADS Act respects that tradition and improves specific procedural aspects to streamline the process. U.S. law enforcement agencies must follow well-established processes to access data stored internationally. Similarly, other countries should be expected to respect the same rules.

Keeping our digital economy equitable and regulated

Evans: Statutory certainty enables the efficiency of the tech economy. Only when governments and businesses abide by the same rules can participants expect clear results. It's unfair for a government to force a technology provider to do what it can't legally undertake (e.g., provide access to U.S. citizens' email messages). Blurring those lines could mean that companies and individuals shy away from investment and innovation.

Anderson: It's unfair to put American consumers at risk if the U.S. sets a precedent of avoiding global privacy standards. Other countries are more likely to access personal correspondence of U.S. citizens through unauthorized means if we do it as well. We should continue to adhere to long-established international agreements in order to protect the rights of our citizens.

International cooperation and the importance of game theory

Evans: In a time of increased transnational threats, the U.S. must work with other like-minded democracies to address those risks. Pursuing unauthorized access to email correspondence across borders could weaken those relationships with our international partners at a

time when we need them the most. If those international relationships deteriorate, we run the risk of putting our country and our citizens in danger.

Anderson: The game theory of international cooperation means that if we violate the rights of other countries by accessing the correspondence of their citizens, other countries may do the same to us. The U.S. must continue to set and adhere to high standards. Updating those regulations will allow us to preserve our alliances with other countries, which will, in turn, benefit law enforcement and individual privacy.

Although we view aspects of the LEADS Act through different lenses, there is no doubt that the bill makes vital improvements to the law governing access to personal correspondence. It strikes a balance between security and privacy that is critical today. We encourage Congress to pass the LEADS Act and enable the U.S. to set the example for other countries around the world. ■

"We should continue to adhere to long-established international agreements in order to protect the rights of our citizens."

JULIE M. ANDERSON, AG STRATEGY GROUP

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.

Julie M. Anderson is a principal at AG Strategy Group. She previously served as acting assistant secretary and deputy assistant secretary of policy and planning at the Department of Veterans Affairs under President Barack Obama.

Is NetCents-2 finally cleared for takeoff?

After more than a year of protests and re-competes, the Air Force's big IT acquisition vehicle is close to being fully open for business

BY MARK ROCKWELL

In the past several weeks, the Air Force has been busily naming vendors for the last spots on its Network Centric Solutions-2 multiple-award IT contracting vehicle.

At the end of March, the service added 10 more vendors to NetCents-2's Application Services contract, bringing the total number of awardees to 20 out of 21 original bidders. In early April, 17 of 29 bidders made the cut for the small-business portion of the Network Operations and Infrastructure contract. And on May 15, 20 of 21 bidders were named to the full-and-open Network Operations and Infrastructure contract.

It's a welcome bit of forward momentum — not just for the Air Force, but for the vendors and a wide range of IT buyers across government.

NetCents-2 is a huge acquisition vehicle — a $24 billion, seven-year package of seven indefinite-delivery, indefinite-quantity (IDIQ) contracts. It replaces the Air Force's existing NetCents contract, which stopped taking orders at the end of fiscal 2013. The last day for performance or delivery of task orders issued under the original NetCents contracts is Sept. 9, 2015.

Like its predecessor, NetCents-2 provides the Air Force with network-centric hardware, software, solutions and services that are not offered by other mandatory-use Defense Department or Air Force vehicles. It is a far broader and more complicated set of contracts, however. Although the original NetCents eventually expanded to an ordering ceiling of $10.5 billion, it was a relatively simple umbrella contract that carried just eight vendors.

NetCents-2, on the other hand, covers five distinct areas:

- **Application Services.**
- **Enterprise Integration and Service Management**, which provides advisory and assistance services for IT and network-centric enterprise management.
- **IT Professional Support and Engineering Services**, which provides program management support and other IT services.

Rounding out the contract rosters

The full-and-open contract for Network Operations and Infrastructure solutions is the most recent one to make awards. As much as $7.9 billion in business will be placed over the next few years with the following companies:

- AT&T Government Solutions
- BAE Systems Information Solutions
- Booz Allen Hamilton
- Computer Sciences Corp.
- Federal Network Systems
- General Dynamics IT
- Harris IT Services
- HP Enterprise Services
- IBM U.S. Federal
- LGS Innovations
- Lockheed Martin
- L-3 National Security Solutions
- NCI Information Systems
- Northrop Grumman Systems
- NextiraOne Federal
- Raytheon
- SAIC
- SRA International
- Telos
- URS Federal Services

NetCents for everyone — most of it, anyway

Not every part of the Air Force's Network Centric Solutions-2 contract vehicle is available governmentwide, and the conditions under which agencies outside the Air Force can use it varies by contract.

	Network Operations and Infrastructure	Application Services	NetCentric Products	Enterprise Integration & Service Management	IT Professional Support and Engineering
Air Force	✓✓	✓✓	✓✓	✓✓	✓✓
Army	✓✓	✓	✓		✓
Navy/ Marines	✓✓	✓	✓		✓
Other DOD components	✓✓	✓	✓		✓
Federal agencies	✓✓	✓	✓		✓

✓✓ Customer can use corresponding contracts without restriction.

✓ Customer can use corresponding contracts, but only if certain criteria are met.

Source: Air Force

• **NetCentric Products**, which provides a full range of technology products.

• **Network Operations and Infrastructure**, which provides services and solutions for network operations.

There are dedicated small-business contracts for the Application Services and the Network Operations and Infrastructure components. As this issue of FCW went to press, the Enterprise Integration and Service Management contract was the one piece that remained unawarded.

But although the first solicitations for NetCents-2 date back to 2008, getting to the point where all seven contracts are fully operational has been a long and troubled process. Both the March additions to the Application Services contract and the April awards for the small-business Network Operations and Infrastructure contract, for example, were re-competes that came after successful bid protests derailed the initial awards.

The anxiety and vendor pushback surrounding the contracts are not hard to understand, said Alan Chvotkin, executive vice president and counsel at the Professional Services Council. Any federal agency may purchase through most of the NetCents-2 contracts (see above for details). The Air Force, however, is required to use NetCents contracts for any products and services that they cover.

That mandatory-use rule means being named as a vendor on one or more of the NetCents-2 IDIQs is a primary entryway into the Air Force's IT business, he said.

The IDIQs were set up with heavy input from the Air Force CIO's office and with significant thought given to how the contracts would fit with the Air Force's networks and architecture.

"Its unique focus for voice, data and IT solutions as a primary source for the Air Force is not common" in other contracts, Chvotkin added.

The Air Force has heavily committed to the General Services Administration's $60 billion One Acquisition Solution for Integrated Services contracts. In fact, OASIS Executive Program Officer Jim Ghiloni said recently that a third of that vehicle's task orders have come from the Air Force. But the scope of the two efforts is different, Chvotkin said, adding that OASIS is oriented toward professional services and lacks the IT focus that NetCents-2 offers.

Larry Allen, president of Allen Federal Business Partners, agreed with that assessment and said he views NetCents-2 as competing with GSA's Alliant and Schedule 70, the Army's IT Enterprise Solutions-2, and the Navy's SeaPort-e, among others.

As NetCents-2 moves ahead, the Air Force is using its experience with the predecessor NetCents contract to gauge how the new vehicle will be used, Chvotkin said. "Because of NetCents, they have a good understanding of how the [spending] will work."

All that protest activity could have an impact, however. "Because it took a while, the scope of work might require some review," he said. With some awards dating back to 2013, "it will take some watching to keep it current." ■

FCW

THE BUSINESS OF FEDERAL TECHNOLOGY

Everywhere you want us to be.

Mobile

Tablet

Desktop

Print

FCW Index

People

Agencies/Organizations

Advertisers

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

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

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

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

The digital — yet skeptical — citizen

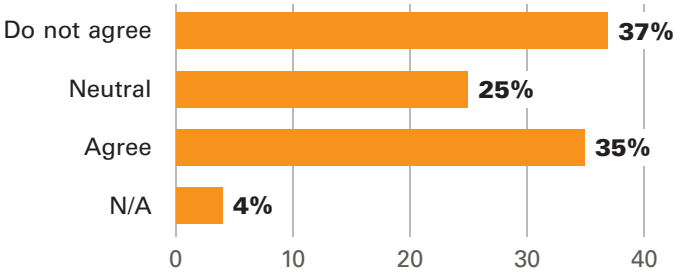
The Obama administration has requested more than $140 million for digital services efforts in fiscal 2016, yet only 41 percent of U.S. adults think the federal government should focus on offering more digital services.

According to Forrester Research, here's how Americans are really engaging with federal agencies:

- **41%** Visiting agency websites
- **37%** In person
- **33%** Postal mail
- **32%** Phone
- **16%** Email
- **8%** Social media
- **5%** Online chat
- **3%** Mobile app

Just **30 percent want location-based services** from government on their mobile devices, while **40 percent would be interested in a single-sign-on credential**. Privacy concerns were a main objection of those not interested.

"I am confident the federal government keeps secure any personal information it has on its citizens":



Still, **more than half of respondents said they want a single portal** that lets them check all federal accounts in one place.

Forrester's recommendation?

"Rebalance the digital customer experience portfolio" by prioritizing new investments based on measurable demand and shutting down underused digital channels to focus on those worth perfecting.

Source: Forrester Research report "Washington Must Work Harder to Spur the Public's Interest in Digital Government"

NOMINATIONS DUE JULY 2

SUBMIT YOUR NOMINATIONS TODAY!

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

FCW.com/2015RisingStars

FCW RISING STAR AWARDS

Budget cuts anyone would approve.

SPRINT DISCOUNT PROGRAM

15% discount for federal employees.

Applies to select regularly priced Sprint monthly service.

Switch to Sprint, turn in your current phone, and register and upload your last bill. We'll pay off your contract and whatever you owe on your phone via an American Express® Reward Card.

To verify eligibility or learn more:

Visit sprint.com/fed

Call 866-639-8354

Sprint

May Req. Activ. Fee: $36/line. Credit approval req. **Contract Buy Out Offer:** Offer ends 7/9/15. Consumer, SDP and CL lines purchasing a new device with: Sprint Easy Pay, Sprint Lease, iPhone for Life Plan, at full MSRP, or Certified Pre-Owned and porting the new line on a service plan. Amount based on ETF (early termination fee) charged or remaining balance on install-bill device (excludes prepaid devices). All lines must be ported from an active wireless line at another carrier and remain active and in good standing to receive the American Express Reward Card. Requires you turn in your current competitor phone associated with the installment billing balance or ETF submitted to Sprint. Important: If you do not turn in the correct device in good working order (i.e. phone powers on, screen is intact, no broken, cracked or missing pieces. iPhones must have activation lock disabled), you will be charged up to the amount of the Reward Card provided to you. You must register and submit your final bill showing your ETF or installment balance within 60 days of switching to Sprint. Allow approximately 15 days after registration approval for your Reward Card to arrive. Register at sprint.com/joinsprint after your registration has been approved. Excludes 100+ Corporate-liable, upgrades, replacements and ports made between Sprint entities or providers associated with Sprint (i.e., Virgin Mobile USA, Boost Mobile, and Assurance). **Reward Card:** Terms and conditions apply to Reward Cards. See Cardholder Agreement or visit www.americanexpress.com/sprint for details. Subject to applicable law, a $3.00 monthly service fee applies beginning in the seventh month after Card issuance. Card is issued by American Express Prepaid Card Management Corporation. American Express is not the sponsor of this promotion. **Gov't Employee Discount:** Avail. for eligible employees of gov't agencies participating in the discount program (ongoing verification). Discount may be subject to change and is available upon request for monthly svc charges. Discount only applies to Talk 450 and primary line on Talk Share 700; and data svc for Sprint Family Share Pack, Sprint $60 Unlimited Plan, Unlimited, My Way, Unlimited Plus Plan and Sprint Family Share Plus plans. Not avail. with no credit check offers or Mobile Hotspot add-on. **Other Terms:** Offers and coverage not available everywhere or for all devices/networks. Restrictions apply. See store or sprint.com for details.