



THE BUSINESS OF FEDERAL TECHNOLOGY

ON-SITE OR IN THE CLOUD WITHOUT COMPROMISE

VMware vCloud® Government Service provided by Carpathia™

—
An enterprise-class hybrid cloud service providing federal agencies with common platform to extend their data centers to the cloud – rapidly, easily, confidently.

Introducing the Hybrid Cloud Service
that Needs No Introduction.

VMware vCloud® Government Service

provided by Carpathia™

- Enterprise-class security, reliability and performance
- FedRAMP Provisional Authority to Operate (P-ATO)
- Designed specifically for government agencies

carahsoft. | vmware®

 CARPATHIA

FCW

THE BUSINESS OF FEDERAL TECHNOLOGY



Have the IGs gone too far?

PAGE 30

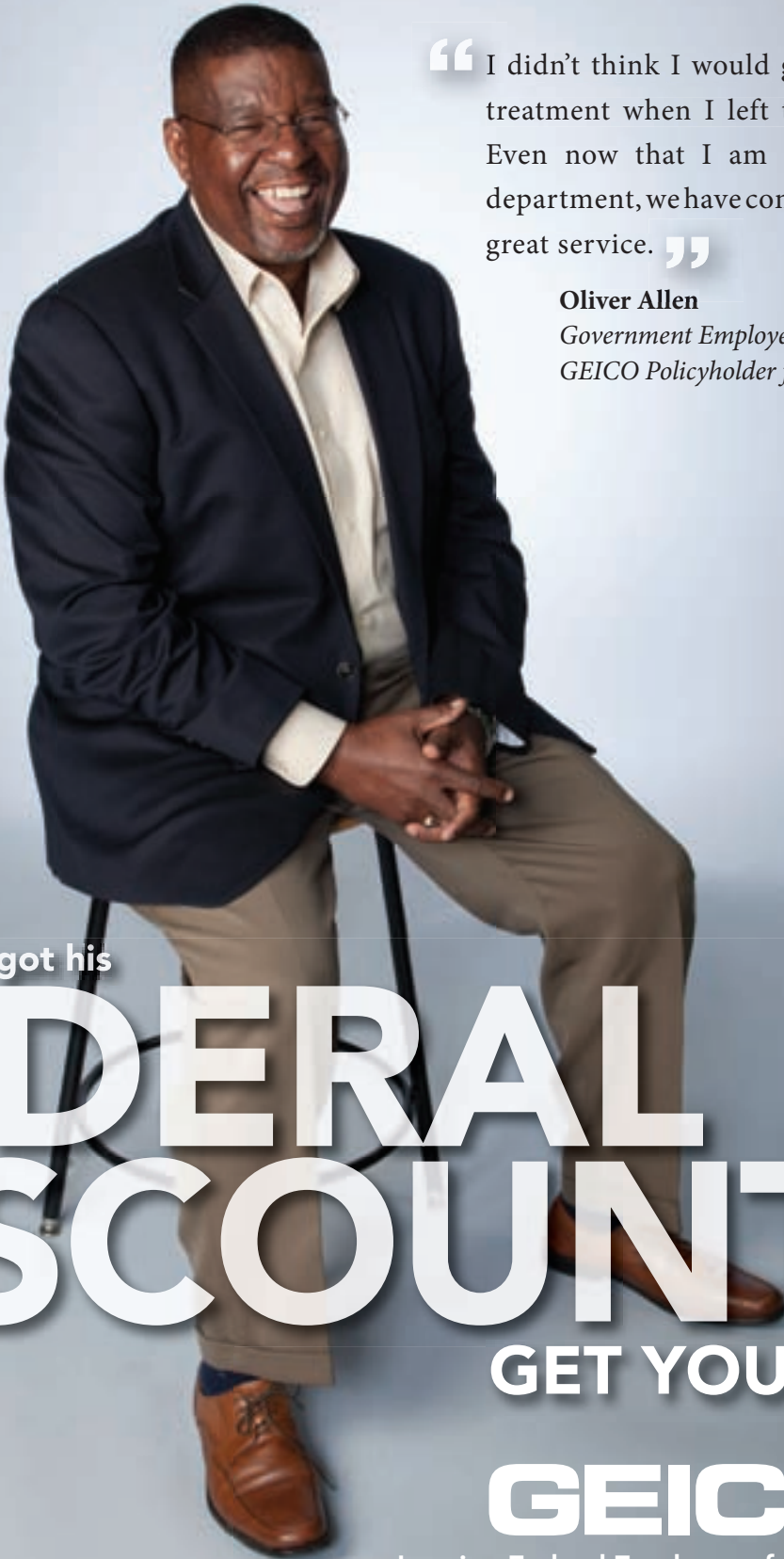
Greetings from Silicon Valley

PAGE 28



CLOUD CONTROL

How cloud and managed services are reshaping the industry landscape PAGE 14



“ I didn’t think I would get the same treatment when I left the Military. Even now that I am in a federal department, we have continued to get great service. ”

Oliver Allen

Government Employee for 19 years

GEICO Policyholder for 30 years

OLIVER ALLEN got his

FEDERAL DISCOUNT.

GET YOURS.

GEICO®

Insuring Federal Employees for over 75 years

1-800-947-AUTO

Some discounts, coverages, payment plans and features are not available in all states or all GEICO companies. Discount amount varies in some states. One group discount applicable per policy. Coverage is individual. In New York a premium reduction may be available.

GEICO is a registered service mark of Government Employees Insurance Company, Washington, D.C. 20076; a Berkshire Hathaway Inc. subsidiary. © 2015 GEICO

NIST official: Internet of Things is indefensible

The interconnectivity of the Internet of Things leaves public and private computer systems essentially indefensible, and no amount of security guidance can help.

That's the sobering assessment of a top analyst at the National Institute of Standards and Technology, the agency responsible for providing such guidance. Federal officials can implement as many security controls as they want, said Ron Ross, a fellow in NIST's Computer Security Division, but hackers will still "have a slice of that pie that will always be accessible because there are things that are off our radar due to their complexity."

"You can comply perfectly with all of that stuff, and you can still have a very vulnerable infrastructure because of the complexity," Ross said at an event hosted by AFCEA's Bethesda chapter in April. "There are things that those standards and guidance... don't touch."

NIST is one of the primary dispensers of federal security guidance, which is not in short supply. As Ross put it, agencies are "drowning in guidance." His answer to the challenge is, ironically, more guidance.

Ross and his colleagues are working on a publication he hopes will be a rubric for applying security controls throughout the life cycle of IT systems. He told FCW that his goal for the document is to "do a better job of engaging the right people in the organization, the decision-makers who are taking those risk-based decisions, and get



"You can comply perfectly with all of that stuff, and you can still have a very vulnerable infrastructure because of the complexity."

— RON ROSS, NIST

them involved early in the process."

A draft of that publication, NIST 800-160, has been published, and Ross said he hopes to release a second draft in the next few months and the final version by the end of the year or early in 2016.

The nonbinding document is aimed at anyone involved with or affected by IT engineering in the public and private sectors. That means systems and software engineers, acquisition managers and C-suite security officials, to name a few.

Ross said tackling the insecurity wrought by the Internet of Things

would require the kind of collaboration among government, the private sector and academia that helped the United States in its space race with the Soviet Union in the 1960s.

In a separate interview, Robert Bigman, a former chief information security officer at the CIA, said "there's a bigger problem" than the need for vol-

untary security standards. "We don't have any governance policy or regulations at the...federal level over this entire issue of the Internet of Things. No one's tackled this issue, and frankly, no one wants to tackle the issue."

Bigman, now a private IT security consultant, said the Office of Management and Budget should ask NIST to come up with recommendations for regulating the Internet of Things.

Hacks have occasionally raised eyebrows, but "no one's paying attention to the bigger issue," he said, referring to the lack of federal regulation.

— Sean Lyngaas

FCW CALENDAR

5/17-19 **Innovation**
ACT-IAC's annual Management of Change conference will dig into continuous delivery, workforce development and the Internet of Things. Cambridge, Md. is.gd/FCW_MOC2015

5/28 **Commerce IT**
Washington Technology's first industry IT day focuses on Commerce's key component agencies and their projected \$2.3 billion in fiscal 2016 IT spending. Falls Church, Va. is.gd/FCW_CommerceIT

RISING STAR
AWARDS

NOMINATIONS NOW OPEN

Nominations for the 2015 Rising Star awards are now being accepted. Learn more at fcw.com/2015risingstars.

Contents



14 CLOUD New players, new playbooks

Cloud and service-driven IT demands are bringing new vendors into the equation — and prompting radical evolution among the perennial industry partners

BY TROY K. SCHNEIDER

20 DEFENSE IT Air Force lags on JRSS at Joint Base San Antonio

Lt. Col. Timothy Kneeland wants the Air Force to move more aggressively on a key DOD IT modernization project

BY SEAN LYNKAAS

24 EXEC TECH The quest for a single government login

Identity management is central to efforts to make a wide range of IT activities secure, but streamlining the process is essential

BY JOHN MOORE

TRENDING

3 SECURITY

A NIST official says the Internet of Things is indefensible

FCW CALENDAR

Where you need to be next

6 MANAGEMENT

Agencies scale back PortfolioStat savings, and time is running out for Rising Star nominations.

8 UAVs

Who's responsible for autonomous killer robots? And an FCW Insider news roundup.

10 CONGRESS

Kendall welcomes a House acquisition reform bill, with caveats

DEPARTMENTS

11 COMMENTARY

Maintaining the right balance

BY DAVID WENNERGREN

IT's role in supporting workplace collaboration

BY KRIS VAN RIPER AND JOHN TAYLOR

'Wisdom of crowds' vs. group discussion

BY STEVE KELMAN

22 DRILL DOWN

Agencies seek millions in digital services funding

BY ADAM MAZMANIAN

28 CIO PERSPECTIVE

When the agency CIO heads to Silicon Valley

BY RICHARD A. SPIRES

30 ACQUISITION MATTERS

Overcoming fear of the inspector general

BY KYMM McCABE

33 FCW INDEX

34 BACK STORY

Cybersecurity's same old song



Editor-in-Chief Troy K. Schneider

Executive Editor John Bicknell

Managing Editor Terri J. Huck

Senior Staff Writer Adam Mazmanian

Staff Writers Sean Lyngaas, Zach Noble,
Mark Rockwell

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

Editorial Fellow Jonathan Lutton

Vice President, Art and Brand Design

Scott Shultz

Creative Director Jeff Langkau

Assistant Art Director Dragutin Cvijanovic

Senior Web Designer Martin Peace

Director, Print Production David Seymour

Print Production Coordinator Lee Alexander

Chief Revenue Officer Dan LaBianca



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

Co-President and Chief Content Officer
Anne A. Armstrong

Chief Revenue Officer
Dan LaBianca

Chief Marketing Officer
Carmel McDonagh

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

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

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

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

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

Marketing

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

FederalSoup and Washington Technology
General Manager Kristi Dougherty

OTHER PSMG BRANDS

Defense Systems
Editor-in-Chief Kevin McCaney

GCN
Editor-in-Chief Troy K. Schneider
Executive Editor Susan Miller
Print Managing Editor Terri J. Huck
Senior Editor Paul McCloskey

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

Federal Soup
Managing Editors Phil Piemonte,
Sherkiya Wedgeworth

THE Journal
Editor-in-Chief Christopher Piehler

Campus Technology
Executive Editor Rhea Kelly



Chief Executive Officer
Rajeev Kapur

Chief Operating Officer
Henry Allain

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

Executive Vice President
Michael J. Valenti

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

Chairman of the Board
Jeffrey S. Klein

SALES CONTACT INFORMATION

MEDIA CONSULTANTS

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

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

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

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

EVENT SPONSORSHIP CONSULTANTS

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

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

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

MEDIA KITS

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

REPRINTS

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

PARS International

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

LIST RENTALS

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

SUBSCRIPTIONS

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

REACHING THE STAFF

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

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

CORPORATE OFFICE

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

DHS covers vetting for all major mobile apps

The Department of Homeland Security's Science and Technology Directorate has expanded its mobile app-vetting and archiving capability to cover all major app markets.

S&T officials said in a statement that their technology can now archive apps from iTunes, Windows Phone Store, Google Play, Amazon and 83 global third-party mobile app markets, including Baidu and Cydia.

Officials said the expansion is part of the Cyber Security Division's app-archiving program, which DHS launched in 2013 with George Mason University and commercial provider Kryptowire to help the government quickly vet and inventory mobile apps.

In December 2014, Kryptowire and the university launched the program's first phase, which archived Android smartphone apps and integrated existing app-vetting capabilities to help analysts understand changes over an app's lifespan.

Kryptowire has commercialized the technology's second phase, which has archived more than 2.4 million free apps and the top 200 paid apps at four major app stores. The technology has the capability to archive additional mobile apps on demand.

DHS planned to showcase the technology at the RSA Conference in San Francisco in April, along with other DHS-funded technologies that are ready to transition into the marketplace.

DHS Secretary Jeh Johnson gave a keynote address at the event about evolving cybersecurity threats and his agency's strategies for addressing them.

— Mark Rockwell

NS2020 sparks a deluge of questions

The General Services Administration has received more than 1,600 comments and questions from industry and federal agencies concerning its draft request for proposals on the contract that will be the cornerstone of its next-generation Network Services 2020 telecommunications strategy.

GSA released the draft RFP on Feb. 28 for the Enterprise Infrastructure Solutions (EIS) contract, which requires potential contractors to cover four mandatory services: virtual private networks, managed networks, regional telecom and Ethernet. The comment period for the document closed March 31.

In an April 15 email message to FCW, a GSA spokesperson said the agency had received 1,215 questions/comments from 15 companies and 405 questions/comments from government agencies.

Managers of the contract said in a conference call in early March that they expected a variety of vendors to be interested in bidding on the \$50 billion, 15-year vehicle, and they anticipated a competitive battle.

Fred Haines, EIS program manager in GSA's Office of Network Services Programs, said during the call that the draft RFP was developed with significant industry and agency input, and it sought to widen the playing field in a number of ways, including reducing geographic network coverage requirements for providers.

Potential bidders won't need to have the vast network infrastructure of a traditional telecom company to participate, he added.

The agency said it expects to issue the final RFP in July and to award the EIS contract by the end of fiscal 2016.

— Mark Rockwell

1,215

questions/comments were received by GSA from 15 companies

405

questions/comments were received by GSA from government agencies

INK TANK



68%

less money has been saved via
PortfolioStat than originally expected

Agencies scale back PortfolioStat savings

In 2014, federal agencies decreased their projected PortfolioStat savings by more than half of what they reported in 2013, with the Defense Department missing the mark by billions, according to a new Government Accountability Office study released April 16.

GAO said at least 68 percent of agencies backed off their original savings estimates.

Agencies initially expected to save at least \$5.8 billion from fiscal 2013 to 2015, GAO said, but those estimates were reduced to about \$2 billion. DOD and the Department of Homeland Security accounted for most of the difference.

DOD reported that it planned \$3.2

billion in savings in 2013 but only \$560.5 million in revised savings in 2014 — a gap of \$2.6 billion.

Despite the downward revisions, GAO said savings from federally mandated data center consolidations could improve the picture a little. Even though the Office of Management and Budget made its Federal Data Center Consolidation Initiative part of PortfolioStat in 2013, GAO said agencies have not consistently included planned savings from the initiative in their PortfolioStat reporting. As a result, the total amount agencies expect to save through fiscal 2015 is understated, according to GAO.

— John Bicknell

NIH awards \$20B GWAC

The National Institutes of Health announced the 65 vendors that will be on its \$20 billion CIO-Commodities and Solutions contract.

The governmentwide acquisition contract is the successor to NIH's Electronic Commodities Store III. It is intended to "support the full range of IT needs across the federal government with a particular emphasis on agencies involved in health care and clinical and biological research," according to NIH.

There are 58 value-added resellers on the contract, along with original equipment manufacturers AT&T, CSC, Dell Federal Systems, HP, IBM, IMS Government Solutions and Vion.

— Troy K. Schneider

EDITOR'S NOTE

Rising Star nominations: Time is running out!

The **deadline** for 2015 Rising Star nominations is fast approaching, and we need your input to be sure we find the best possible candidates for our judges to consider.

The Rising Star awards spotlight women and men who — even in the early stages of a federal IT career — are having an outsized impact and who show clear signs of being leaders in the community in the years to come.

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 50-year-old veteran

who has embarked on a second career is every bit as eligible.)

What makes for a winner? In many ways, it's the same criteria used for the Federal 100 awards — someone 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, too, but that's what the GCN awards are for. (Those nominations are open as well, by the way; learn more at GCN.com!)
- Winners go above and beyond, whatever their level or rank. A fancy job title is not required, and doing one's job well is not enough.

- Impact matters. The judges need to know not only what a nominee did but also what all that work accomplished.

- The award is for work done in the past year. Future leadership potential is important, but nominees must have had clear accomplishments in the past 12 months.
- You can make multiple nominations. Do so early and often.

So gather your information and supporting nominators, and get those nominations in 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](https://twitter.com/troyschneider)



FCW Insider: People on the move

Dan Gordon, former administrator of the Office of Federal Procurement Policy and now an associate dean at George Washington University Law School, said he has been gradually pulling back from his many advisory roles in the past few months with an eye to retiring by July 1.

He said his enthusiasm for the government's procurement system is undimmed, despite the increasing complexity and technological changes that have many calling for reform.



Dan Gordon

A complete overhaul could be shortsighted because the system isn't broken so much as in need of updating, he said, adding, "We get high-quality equipment to warfighters, and we do a good job of getting IT systems that work. Our system has more transparency. It is good and effective."

However, the system does need to continue evolving. Agile development, more competition and innovation are all important ingredients, he said, while congressional micromanagement of the process is not. Instead, the government should be looking for ways to inject more uniformity into the procurement process and get agency IT and contract employees to work together more closely.

The system's biggest flaw is a lack of investment in employees, Gordon said. "There is an unwillingness to spend adequate money on 1102 [contract specialists] and training. There's not enough staff."

During his tenure as OFPP administrator, from 2009 to 2011, he worked on a variety of acquisition issues, including improving and standardizing the workforce, overseeing the implementation of strategic sourcing,

and pushing for more industry and agency communication through his "myth-busters" campaign. He has frequently testified on acquisition issues before Congress.

Former General Services Administration CIO **Casey Coleman** left AT&T Government Solutions to become Unisys Federal's civilian agency business leader in April.



Casey Coleman

Previously, she worked at Lockheed Martin and Kana Software.

A three-time Federal 100 winner, Coleman told Washington Technology her time at GSA would serve her well at Unisys. "I have a lot of empathy for our government customers," she said. "You have to understand the pressures they are under."

The Senate confirmed **Russell Deyo** as undersecretary for management at the Department of Homeland Security on April 16.

"Given the challenges associated with fusing 22 separate agencies into one cohesive department, the undersecretary for management at the Department of Homeland Security is an enormously important position," Sen. Tom Carper (D-Del.) said in a statement.

Energy Department Deputy CIO **Don Adcock** left the agency in April. Adcock had been interim CIO until March 5, when **Michael Johnson** was named DOE's CIO. Johnson had been serving as assistant director for intelligence programs and national security systems at the White House's Office of Science and Technology Policy.

— FCW staff

CRITICAL READ



MIND THE GAP
The Lack of Accountability for Killer Robots

WHAT: A report from Human Rights Watch and Harvard Law School's International Human Rights Clinic on the legal, moral and practical concerns regarding fully autonomous weapons.

WHY: Such weapons are all but incapable of distinguishing between lawful and unlawful targets as required by international humanitarian law. However, it is unlikely that military commanders or the weapons' programmers and manufacturers could be held liable if an autonomous system illegally killed noncombatants. But there are also concerns about an arms race that could put such weapons in the hands of those with little regard for the law.

VERBATIM: "Existing mechanisms for legal accountability are ill suited and inadequate to address the unlawful harms fully autonomous weapons might cause. These weapons have the potential to commit criminal acts — unlawful acts that would constitute a crime if done with intent — for which no one could be held responsible."

FULL REPORT:
is.gd/FCW_HRW



EARLY REGISTRATION DISCOUNT

Register by June 26
and save up to \$345

USE PRIORITY CODE BOS7

Boston 2015

The Analytics Experience

July 26–31, 2015

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

Core Tracks

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

Hot Topics

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

KEYNOTES



Data to Profit: Revenue Growth through Analytics and Monetization

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



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

Wayne Eckerson
Principal Consultant, Eckerson Group, LLC

New!

HANDS-ON TRAINING

LEARN HOW TO USE ALL THE LATEST ANALYTICS TOOLS AND TECHNOLOGIES

PEER-TO-PEER LEARNING

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



Advancing all things data.

IN THE IT PIPELINE

WHAT: The Defense Advanced Research Projects Agency is accepting proposals for its Building Resource Adaptive Software Systems (BRASS) program, which seeks to advance the design and implementation of long-lived software systems.

WHY: Researchers want those systems to dynamically adapt to changes in the resources they depend on and the environments in which they operate, instead of having to be manually updated by IT personnel.

Those advances will require developing linguistic abstractions, formal methods and resource-aware program analyses that can discover and specify program transformations. Systems designed to monitor changes in the surrounding digital ecosystem will also be needed, DARPA said.

"Technology inevitably evolves, but very often corresponding changes in libraries, data formats, protocols, input characteristics and models of components in a software ecosystem undermine the behavior of applications," DARPA Program Manager Suresh Jagannathan said in a statement. "The inability to seamlessly adapt to new operating conditions undermines productivity, hampers the development of cyber-secure infrastructure and raises the long-term risk that access to important digital content will be lost as the software that generates and interprets content becomes outdated."

FULL LISTING:
is.gd/FCW_DARPA_BRASS

Kendall welcomes House acquisition reform bill, with caveats

According to Frank Kendall, undersecretary of Defense for acquisition, technology and logistics, a recently unveiled bill to reform the troubled acquisition system largely gets it right, with at least two possible exceptions.

Kendall said he was wary of the over-involvement of military service chiefs in the acquisition process. Although they have an important role to play, they should not be in the business of program scheduling, he added.

"I have seen some very disastrous cases" in which service chiefs have set arbitrary dates for program deliverables, leading to undue risk-taking, Kendall said at a Brookings Institution event in April. "I just want to be careful about how far we go in that direction."

The legislation, written by House Armed Services Committee Chairman Mac Thornberry (R-Texas), would not delegate program scheduling to the service chiefs, but it would amend the U.S. Code to require their involvement in acquisition policy.

Thornberry's bill would also create a dual-track career path for military officers that involves combat and acquisition experience. That approach is intended to "more closely align the military operational, requirements and

acquisition workforces of each armed force," the bill states.

But Kendall said he and Adm. James Winnefeld, vice chairman of the Joint Chiefs of Staff, were concerned that such a provision would not allow for enough specialization in the Defense Department acquisition workforce.

"If somebody were half a doctor and half a lawyer, you wouldn't expect him to be terrific at either one," Kendall said.

To improve the Pentagon's acquisition policies and practices, he recently unveiled the third iteration of the Better Buying Power initiative. The new guidance is intended in part to ensure that cybersecurity is "constantly in mind" in the acquisition process.

When asked by FCW what he would say to critics who might charge that cybersecurity should have been a key tenet of earlier versions of the BBP, Kendall said, "they're probably right."

"It's not that we're not doing anything about cyber. We are," he added. "But I think the need to make my acquisition workforce much more conscious of it in the pervasive way that I think we need to be conscious of it probably ...existed earlier."

— Sean Lyngaas



Mary Davie
@marydavie

Our brave new smartphone world - @kelmansteve gets it right
<http://fcw.com/blogs/lectern/2015/04/kelman-brave-new-smartphone-world.aspx> ... via @FCWnow

↩ Reply ↻ Retweet ★ Favorite

5:43 AM - 17 Apr 2015

Join the conversation

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

Learn more at Twitter.com/FCWnow.



Maintaining the right balance

Think you can succeed by zeroing in on a single problem?
Sorry, but life is not that simple.

In his book “Polarity Management: Identifying and Managing Unsolvable Problems,” Barry Johnson makes the case that although we are trained from a young age to identify and solve problems, many of the challenges we face don’t reflect a single problem to solve. Far more often, the true challenge is a polarity of two things occurring simultaneously. By limiting our view to a single problem to solve, we miss the impact of the related issue that we’re not addressing and end up making things worse, not better.

Examples of polarities are all around us, and they include cost/quality, efficiency/effectiveness and change/stability. Technology leaders face a number of polarities masquerading as problems, and failure to grasp the importance of managing both ongoing issues will inevitably delay or destroy the best-laid transformation plans.

Information security professionals could minimize risk by walling off their organizations from the outside world. When taken to the extreme, however, that is a sure path to a self-inflicted denial-of-service attack. Bad things don’t get in, but necessary information doesn’t move either.

Similarly, if your job is to advance information sharing, your best efforts might fail to recognize that you’re under attack and your intellectual capital is being served up to adversaries and competitors. In a world where users demand access from any device, anywhere,

a successful cyber strategy must embrace both information sharing and information security. By shifting our focus (and language) to “secure information sharing,” we will raise the bar on security while encouraging, rather than thwarting, the flow of knowledge.

Another important polarity is determining the balance between work done at the enterprise and local levels. Way back in the last

By shifting our focus to “secure information sharing,” we will raise the bar on security while encouraging the flow of knowledge.

millennium when PalmPilots and Deep Blue roamed the earth, we lived in a world of local-area networks and systems. The advantages of doing things locally included a manageable scale, speed, agility and proximity to your customer. The downside was that we wasted time and money developing duplicative solutions that were not interoperable and that created electronic barriers to sharing information.

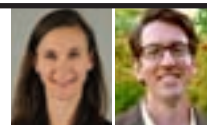
With the advent of the Internet Age, we discovered that we could eliminate the expense of duplicate, disparate solutions. However, the

pendulum has perhaps swung too far toward doing things at the enterprise level, resulting in more than a few major system implementations that, due to their immense size, failed to delight anyone by trying to appease everyone.

Agile methodology has demonstrated the power of breaking work into modular increments, and locally developed apps that meet local needs are examples of bigger not always being better. However, if managing the scope of an effort becomes the problem to solve, your preference will always be for smaller solutions, blinding you to the other aspect of the polarity.

Sometimes “evolutionary” change through small engagements is the right path to build momentum and gain support. At other times, “revolutionary” change is needed. If the Defense Department had not demanded a single Common Access Card solution for all 3.5 million of its people, DOD officials would be years behind their current state in addressing identity management, information security, e-business and physical access issues.

We live in a world that demands choice in the applications and devices we use while deriving great value from consolidated offerings such as enterprise services and cloud computing. The art is to understand that both enterprise and local solutions have their place and to ensure that early in your work, you decide the optimal balance to effectively manage the polarity you face. ■



IT's role in supporting workplace collaboration

As feds increasingly turn to cloud-based tools, IT leaders have an opportunity to reduce risks without hindering innovation

Today's workforce is more collaborative than ever. CEB research shows that the average employee works with 10 or more individuals to accomplish daily tasks, and nearly half of an employee's performance comes from integrated contributions. Two-thirds of employees report doing more collaborative work now than they did three years ago, and this change will only increase.

Despite the demand for collaboration, however, federal employees are often dissatisfied with the managerial support and tools they receive to enable it. In the 2014 Federal Employee Viewpoint Survey, only 54 percent of federal employees said their managers support collaboration across work units to accomplish organizational objectives. Additionally, our research shows that only 42 percent of employees rate their IT-provided collaboration tools as effective.

In the government, business units have addressed the gap between their collaboration needs and IT's current support by turning to cloud-hosted solutions. A recent report by Skyhigh Networks claims that the average government organization uses 721 cloud services — more than 10 times the number that central IT expects. Collaboration tools top the list, with the average organization making use of 120 cloud-based resources.

Business units and individual employees are turning to those solutions because the unpredict-

ability of collaboration needs defies IT standards and set processes. IT leaders and even business unit leaders can't typically foresee which processes will be the most effective for a future opportunity. Effective collaboration tools meet real-time needs, and employees are voting with their feet by choosing apps and cloud-based tools that meet their needs in a more targeted and timely fashion than traditional IT offerings.

Despite the demand for collaboration, federal employees are often dissatisfied with the managerial support and tools they receive.

IT departments have valid concerns about such business-led technology sourcing, including potential security risks, excessive portfolio complexity and potentially duplicative spending. However, IT often underestimates the benefits of business-led technology experimentation, while business partners often underestimate the risks and true lifetime costs of cloud-based services.

IT leaders can best balance concerns about risks with potential rewards by adapting their engage-

ment model to meet the context of collaboration. Frontline employees and their managers are typically best positioned to know their collaboration needs, but IT has a cross-enterprise perspective, knowledge of the capabilities and limitations of systems and data, and expertise in managing technology projects.

IT leaders can maximize those advantages by:

- **Equipping business leaders to be informed technology consumers.** Instead of trying to force business leaders to source their solutions through IT, the department can act as a "buyer's agent" for business units. The IT team can educate them to ask vendors the right questions and gain an early and complete understanding of the trade-offs associated with a particular solution.
- **Scaling good solutions to the enterprise.** Although business units are more capable of experimenting with collaboration tools, IT can promote scalable solutions across the enterprise. Instead of developing applications internally, IT should provide a set of integration services and a flexible access point for all potential users in the form of an enterprise app store.
- **Enabling stakeholders to manage information risks.** Business units are the true owners of the risk from self-procured cloud services. The IT team should act as a security adviser and teach employees to identify risks by providing clear, easy-to-use risk assessment templates and reference guides. ■



'Wisdom of crowds' vs. group discussion

Do we get better responses by averaging individual judgments or discussing those judgments in a group? The answer has implications for decision-making in government.

The idea of the "wisdom of crowds" was popularized in a 2004 book with that title by James Surowiecki. The author goes beyond just saying that "two heads are better than one" or that groups often make better judgments than individuals, including individual experts.

Instead, Surowiecki asserts that averaging the individual judgments of many people about the answer to a question will produce better results than having people discuss their initial views and then reach a common judgment.

Some of the discussion has pitted the averaged judgments of large groups against those of individual experts. But belief in the wisdom of crowds also challenges another common view, which is that group discussion will typically produce better decisions than averaging the judgments of lots of individuals without discussion, as a prediction market does.

Recently, social psychologist Julia Minson, a young colleague of mine at Harvard's Kennedy School of Government, presented her research on the latter topic. Specifically, she asked: For questions where there is a lot of uncertainty about the correct answer, do we get better responses by averaging individual judgments or by discussing those judgments in a group?

The answer has important practical value for decision-making in government and other large organizations.

Minson's research, which

involved lab experiments, resulted in two key findings. First, averaging individual responses performs dramatically worse than discussion when some members of the group have estimates that turn out to be dramatically wrong. However, that approach is not as bad if there are not such egregious errors among group members.

The improved accuracy of discussion over averaging is due mostly to participants giving greater weight to better information.

The improved accuracy of discussion over averaging is due mostly to participants giving greater weight to better information and not simply the distortion in averaging caused by the terribly wrong estimates.

Second, the accuracy improvements from discussion are larger when participants do not reveal their estimates before the discussion. Sharing estimates in advance tends to limit the range of options considered, which has a negative effect on accuracy. Minson notes that this conclusion runs counter to most people's intuition.

Can we apply this research to development of estimates used in

government and other large organizations? Minson's research involved situations in which participants were often very uncertain of the facts but where correct facts indeed existed. (For example, respondents were asked to estimate the annual salaries of nine Fortune 500 CEOs.) But does it apply to uncertain estimates about the future?

Clearly, Minson's calculations required a comparison with some standard of a correct answer, which does not yet exist for estimates about the future. Nonetheless, the principle that there is what will turn out to be a correct estimate about an uncertain future, even if we don't know it now, is the same for the two scenarios, and my view is that we can make the crossover.

There was another lesson in Minson's presentation. One of the great virtues of being at a university is having structured opportunities to be exposed to the ideas of young colleagues. The Kennedy School and most other research-oriented universities regularly hold seminars at which faculty members present their research, and a large proportion of the presentations are by young colleagues.

It is tremendously stimulating and encourages the rest of us to develop new ideas and new ways of thinking, which benefits our organization as a whole. Government would do well to create similar opportunities for newer employees to present their thoughts to those who have been around longer. ■

NEW PLAYERS, NEW PLAY

Microsoft

The king of installed software now sells SaaS, developer platforms and pure infrastructure cloud

Salesforce

The SaaS pioneer now has a full-blown apps ecosystem in government

CenturyLink

A quintessential telecom firm is looking more and more like an IT services provider

Lockheed Martin

Four key acquisitions in 2014 helped keep a lock on the top IT contractor slot

Amazon Web Services

First an eye-popping CIA contract, then aggressive partnering throughout the market

Huddle

Leveraging In-Q-Tel funding and U.K. government market share to challenge the SharePoint status quo

Unisys

Sixty-four years after UNIVAC I, the emphasis is on service and "stealth" cybersecurity

IBM

Focusing on consulting and cloud services — and showcasing Bluemix in hackathons with NASA

Splunk

Analytics for everyone — including SAIC's own security operations center

Monster

A consumer-jobs giant has quietly carved out HR business with 130 agency components

Cloud and service-driven IT demands are bringing new vendors into the equation — and prompting radical evolution among the perennial industry partners

YBOOKS

BY TROY K. SCHNEIDER

Strange things are afoot in federal IT.

Companies that a decade ago were nowhere to be found on contracts — and in some cases did not even exist — are working with agencies on mission-critical systems.

Splunk is supplying the analytics to monitor the F-35 stealth fighter's systems and performance data. Monster Government Solutions now works with virtually every Cabinet agency on recruiting and retaining staff. Salesforce.com has established a thriving applications ecosystem, and Amazon Web Services is called out by name in requests for proposals.

The traditional IT powerhouses, meanwhile, are hardly standing still. Unisys — the company that sold the first computer to the government — is now working with several agencies on predictive analytics and has emerged as

a leader in software-defined security. AT&T, CenturyLink and Verizon have all evolved far beyond their telecom roots. Microsoft

— long the godfather of

locally installed software and enterprise licenses in government

— is now arguably many agencies' most aggressive cloud enabler.

So what exactly is going on?

A catalyst in the cloud

Perhaps the clearest sign that the federal IT landscape had changed came in early 2013, when FCW broke the news that Amazon had won a \$600 million CIA contract to build a private cloud for the intelligence community.

In every interview conducted for this story, sources pointed to the CIA deal as a watershed moment. As Deltek Vice Presi-

dent Kevin Plexico put it, "10 years ago, if you were to say who are the companies going after that contract, you never would have in a billion years thought of Amazon."

According to Professional Services Council President Stan Soloway, "The Amazon CIA deal was huge not just because it was Amazon's first big win, but [also] because it said to the national security space, 'Oh, the national security customer may be willing to do something different,' at a time when a lot of folks in the national security space did not believe that their customers wanted to go that route."

Dave Wennergren, a former Department of the Navy CIO and longtime Defense Department executive who is now PSC's senior vice president for technology, agreed and asked: "Does it really mean that it's a change in the guard, or does that just mean that the way we're asking for things in a changing marketplace is creating new opportunities?"

Changes, yes, but no changing of the guard

When it comes to cloud contracts, one thing that is clearly not happening is some wholesale changing of the guard. In a Deltek analysis of known agency cloud contracts to date, Booz Allen Hamilton, Carahsoft, CGI Federal, CoreSphere, DLT Solutions, HP Enterprise Services, IBM, Smartronix and Verizon all have won more awards than Amazon has.

"I definitely think there's some disruption taking place, and it's forcing...some significant changes in the main stage players," Plexico said. "In the scheme of dollars, it hasn't caused a big shift. But in the scheme of business strategy, pricing, partnering and the teaming relationships that have been formed in the past versus the ones that are forming now, I think there are big changes when you look that way."

Alex Rossino, who conducted the cloud-contract research as Deltek's principal research analyst for federal industry analysis, agreed. "I look at it less from new players that are entering as opposed to old players that are changing in order

AT&T

The Alliant contract and Schedule 70 spot are evidence of a shifting federal focus

Cloud

to adapt to the new situation firsthand,” he said.

And adapt they have. Rossino cited Microsoft in particular for the way the software giant has been “transitioning current customers over to their Azure cloud and the Office 365 offering.... That keeps those customers sticking with them.”

Other players in the field have grumbled about that, he said, because the migrations have come in the guise of renewing software licenses. “That’s definitely a different way of doing stuff,” he added. “It’s just how the market is nowadays.”

The evolutions extend beyond pure cloud plays as well. “Cisco is a great example,” Soloway said. “I think they haven’t done it with a lot of publicity, but they were a router and switch company. Now they’re selling capabilities. That is a huge cultural and business-model shift for a company that size.

Or look at Verizon, Rossino said. “Verizon used to be known as a Baby Bell. They provided telecom services. Now they do cloud everything.... They’ve radically changed their business model in order to accommodate the new technologies.”

Other firms have taken different approaches. Large pure-play government contractors such as Lockheed Martin (which perennially places No. 1 on Washington Technology’s list of top federal IT firms), Northrop Grumman (the consistent No. 2), CACI, Man-Tech and SRA International have been aggressive in acquiring smaller firms to strengthen their cyber, business intelligence, cloud and health IT offerings.

For others — such as Engility, Harris, PAE and Vencore — acquisitions have been more about improving their economies of scale.

The government’s growing receptiveness to the idea of using commercial technology, meanwhile, has played to the strengths of companies such as Accenture, Computer Sciences Corp., HP, IBM and Unisys, whose government units can take advantage of the companies’ much larger private-sector businesses. Accenture, HP and IBM, of course, also have robust consulting and services businesses, positioning them to apply commercial practices to government needs and helping HP and IBM stress IT services over traditional hardware and software products.

There are other approaches as well,

and many companies are embracing more than one. For additional examples, see the illustration on Page 14.

“The current incumbents have lots of innovation going on,” Wennergren said. “Boeing is inventing force fields.... IBM continues, I think, to offer innovative work on a scale unrivaled, pretty much, in the technology business.” The list, he said, “goes on and on.”

So what, then, are these newcomer firms doing? The entry points for agency business vary, of course, but the common thread is that companies are offering agencies technologies that have caught fire in other sectors, usually in corporate IT. Before Splunk landed its F-35 work, for example, the firm had crunched data for Cars.com and NPR, among many others. But Huddle has capitalized on its government success in Great Britain, while Maximus has done the same with its state and local experience as health IT has grown more important at the federal level.

The newcomers are also capitalizing on two critical aspects of cloud computing: scale and standardization. The first has long been a hallmark of federal IT; the second is slowly being embraced.

Historically, enterprise IT systems

CENTURYLINK AND THE TELECOM TRANSFORMATION

One of the more intriguing cloud trends to watch is the evolution of the major telecommunications players as they continue to embrace cloud technology and a managed services approach to the government market.

As a sign of that trend, earlier this year CenturyLink promoted Tim Meehan to senior vice president and general manager of its government business. It’s important to note Meehan’s background in the IT market. He was vice president of sales for the company’s east region and the financial services industry, and he ran inside sales for CenturyLink Technology Solutions. Before joining CenturyLink, he led various business groups in Oracle’s consulting division and was in charge

of North American sales for the company’s cloud-hosting unit.

AT&T made a similar move in 2013 when Kay Kapoor was picked to lead AT&T Government Solutions. She had held IT leadership positions at Lockheed Martin and Accenture.

Meehan’s background will be critical for his vision of making CenturyLink a leading IT services provider. “It’s bringing that single pane of glass so agencies can look across their networks and understand what is going on,” he said.

It is a decidedly enterprise view of IT that CenturyLink and other telecom players are uniquely qualified to bring to the market. That vision is predicated on the telecom compa-

nies focusing not on selling trunk lines and telephony but on bringing a mission focus to how they sell their communications infrastructure to government agencies.

How CenturyLink, AT&T and Verizon deliver on the mission will vary from agency to agency, so the companies are offering a range of public, private and hybrid cloud solutions, in addition to meeting customers’ on-demand computing, storage, platform and application needs.

The shift in strategy also reflects the evolving contract vehicles. The General Services Administration is developing the Enterprise Infrastructure Solutions contract as part of its Network Services 2020 strategy. It is the suc-

WHEN MOST IT SYSTEMS WERE ON-PREMISE, FEDERAL SYSTEMS OFTEN REQUIRED A SCALE — THINK IRS OR U.S. ARMY — THAT COULD SCARE OFF FIRMS NOT BUILT AROUND GOVERNMENT BUSINESS.

were made-to-order affairs — especially in government. There's only one IRS or U.S. Army, so why not tailor the infrastructure to fit?

As Google and Facebook have famously demonstrated, however, there are clear upsides to cookie-cutter servers and other components. Others have followed suit, Rossino said, and “the architectures have now developed to a point where the hardware is standardized enough to leverage something like infrastructure as a service.”

Dave Bartoletti, a principal analyst at Forrester Research, put it slightly differently: “The cloud works when you make yourself fit to the cloud.”

“If you think your relationship with the cloud is ‘I’m going to call...and tell them what I want — what servers I

want, what network I want’ — that defeats the whole model,” he said. “It’s sort of the ‘build it and they will come’ model, versus the ‘what do you want me to build for you?’ model” that has long been prevalent in government.

And if government is slowly acclimating to commodity infrastructure, the rest of the world is catching up when it comes to scale.

When most IT systems were on-premise, federal systems often required a scale — again, think IRS or U.S. Army — that could scare off firms not built around government business. For an Amazon or a Google today, however, an agency’s storage or computing needs are not nearly so daunting.

Bartoletti pointed to Docker, the popular containerization solution,

as a case in point. Containers are “a cool new technology,” he said. “And in the past, a few people would play with it, and take a risk and see if it works. Well, Google now launches 2 billion containers a week. So if you’re the government, and you’re worried about should you deploy your applications in containers — are they safe? Are they stable? Well, of course they are.... You’re not the first one using them anymore. You’re not bleeding edge in the cloud.”

According to Soloway, this means that “not only is the IT industry going to market differently as a service model, but the way the technologies are being deployed is fundamentally changing the services economy — or has the potential, at least.”

Preconceived notions and missed opportunities

Soloway, however, also said he was concerned that agencies might be selling familiar companies short as they look to the cloud.

“There is a bit of a sense, I think, among some of the leadership in government that the existing traditional contractor base is no longer innovative or agile,” he said. “I think that’s a very dangerous assumption because in any market the suppliers respond to what their customers really want and direct them to do.... The biggest frustration they have is the ability to bring that innovation to the customer.”

Wennergren went further by asserting that deconstructing the cast of contractors risks missing the larger point.

“We have this penchant for [saying], ‘We’re not getting what we want; therefore, we must need to go to new people to get it,’” he said. “It doesn’t matter whether you’re going to these new guys or the current guys. If you don’t ask for it right, you’re not going to get the kind of innovation that you seek in the future.” ■

Washington Technology Editor-in-Chief Nick Wakeman contributed to this report.

cessor to the Networkx contracts currently in use and held by AT&T, Verizon, CenturyLink, Level 3 Communications and Sprint.

GSA officials have been vocal about wanting more than the traditional telecom companies to pursue the contract, but so far only Harris has come forward to say it will bid as a prime contractor.

The contract has several optional requirements that seem to play to the strengths of systems integrators, but the mandatory requirements are squarely in traditional telecom companies’ wheelhouse and are most likely too expensive for systems integrators to develop on their own. Therefore, NS2020 could be a major opening for the telecom

companies to bring broader IT services to the market and step up as challengers to the more traditional IT providers.

The market has been headed in this direction for several years. AT&T and Verizon holds spots on large multiple-award IT contracts, such as GSA’s Alliant. AT&T, Verizon and CenturyLink also hold spots on GSA’s Schedule 70 IT services vehicle.

But GSA’s NS2020 strategy and the EIS contract will push the telecom companies deeper into the IT space. For government buyers, the results should be more choices among providers and contract vehicles and more competition.

— Nick Wakeman



ENDURING FORCE

Strike

.....

Mobility

.....

Surveillance & Engagement

.....

Unmanned & Missile Systems

.....

Global Support

www.boeing.com/militaryaircraft

 **BOEING**



Air Force lags on JRSS at Joint

Lt. Col. Timothy Kneeland wants the Air Force to move more aggressively on a key DOD IT modernization project

BY SEAN LYNKAAS

Joint Base San Antonio, a sprawling complex shared by the Army and Air Force, has been a testing ground for a signature piece of the Defense Department's IT modernization plans. But the Air Force component of the base is lagging behind the Army in implementing the Joint Regional Security Stacks project and missing out on its security benefits, according to Air Force Lt. Col. Timothy Kneeland, commander of the base's 502nd Communications Squadron.

The Air Force at JBSA "has not moved as aggressively to utilize the JRSS and all the capabilities within it" as the Army has, he told FCW.

"That's something I seek to do," he added, because the stacks will enable interoperability at the base.

The 502nd Communications Squadron is charged with facilitating communication across the constellation of facilities that make up JBSA. The squadron serves 84,000 customers annually, according to Kneeland.

JRSS is a collection of servers, switches and software tools meant to give DOD network operators a clearer view of network traffic. By sending that traffic to the cloud for analysis, the stacks can help operators quickly respond to network threats by, for example, opening certain ports or blocking a given IP address.

DOD CIO Terry Halvorsen has touted the stacks as the cornerstone of a larger departmentwide initiative known as the Joint Information Environment, which seeks to standard-

ize and consolidate IT networks for better security. A test of JRSS last year revealed a solid architecture and showed that "we had the capacity size right, [but] we needed to do some fine-tuning of the software sets and tools," Halvorsen told reporters in December.

JRSS is being deployed at more than 20 military sites around the world. Installation is complete in Europe, and the stacks reached initial operating capability at JBSA in September. According to Kneeland, however, the Air Force is flowing traffic only through the outer boundary of the stack.

His goal is to run network traffic through each layer of the stack and fully use the analytics and security



nt Base San Antonio

features that are possible through JRSS. The focus so far has been on “making sure that the links are all in place but not actually utilizing the capabilities that are there,” he said. “When that happens, I’ll be able to then reroute traffic [to] the other installations.”

The Air Force at JBSA was set to begin use the JRSS security features in February, but their activation has been delayed, perhaps until July, Kneeland said. A spokesperson for the Air Force’s 26th Network Operations Squadron, which is helping implement JRSS at the base, could not be reached for comment.

When asked what he could do to speed implementation of JRSS, Kneeland said, “Nothing.... We’re ready to roll on this end,” and added that he planned to talk to DOD officials about the direction of JRSS implementation.

Kneeland said he understands that, given its finite resources, the Penta-

gon had to prioritize implementation of JRSS in some places at the expense of others. “But being responsible for this area here in JBSA, I’d like to see us...completely utilize JRSS because I think there’s great benefit in it,” he added.

Kneeland’s goal of interoperability remains elusive, however. Some 1,000 Air Force personnel at JBSA’s Fort Sam Houston, for example, have to use an Army network because the Air Force’s network is unavailable to them. Having full access to the Air Force network would enable the personnel at Fort Sam Houston to work with their colleagues at other JBSA facilities on records management and storage-area networks, he added.

“You don’t want to have to have a separate desktop environment for each place that you go,” Kneeland said. “You want to be able to have a single one that you can be mobile and move around throughout.” ■

JRSS in a nutshell

Since becoming Defense Department CIO more than a year ago, Terry Halvorsen has made the Joint Regional Security Stacks a signature piece of his IT stewardship.

When up and running, JRSS will reduce the “access points to our network,” Halvorsen said. “It gives us a more limited number of control points, which immediately limits your physical footprint, which is a good thing.”

JRSS will not mean fewer cyber-threats to DOD networks but, ideally, better responses to those threats.

In an interview with FCW, Richard Breakiron, who was program director for JRSS at the Defense Information Systems Agency from January through May 2014, said tests at Joint Base San Antonio showed big improvements in usable bandwidth and better response times to threats.

In addition, teams trained by the National Security Agency have tested the JRSS infrastructure for resiliency by attacking it, and the stacks proved effective in defense, said Breakiron, who is now senior director of cyber solutions at Vion.

The ability to turn DOD networks into digestible forensics will be one of the biggest payoffs of JRSS, he added.

“Forensics not only gives you the chance to look at the long-term attacks and potential vectors from an enemy, but it also allows you to start understanding your insider threat better as well,” Breakiron said.

The military has been doing a staggered deployment of JRSS at military sites around the world, starting with bases in Europe.

Halvorsen has said the stacks will begin going live in early fiscal 2016, and by the end of that year, they will be delivering much of their expected capabilities on DOD networks worldwide.

— Sean Lyngaas

Agencies seek millions in digital services funding

Most CFO Act agencies have bought into the concept of digital services teams and are including them in their 2015 budget requests

BY ADAM MAZMANIAN

It's no secret that the federal government is on the lookout for a few good geeks. The fast-growing U.S. Digital Service, housed at the Office of Management and Budget, is trying to induce private-sector techies to do a stint in government. And now agencies are incorporating funding for such teams into their budget requests.

Federal Deputy CIO and USDS Administrator Mikey Dickerson pegged overall spending on the new tech teams at about \$105 million.

"The demand from the agencies is...more than we could ever satisfy," Dickerson said in a recruiting pitch at the South by Southwest conference in March. "We have met with 22 of them and identified around 60 projects that need attention."

Most of the agencies that fall under the CFO Act have made budget requests to fund digital services teams. However, the Defense Department is not establishing such a team, and the congressional justification documents for the departments of Energy and Housing and Urban Development make no mention of the program. Otherwise, buy-in is solid up and down the line.

There are at least \$75 million worth of digital services funding requests, even though some agencies that are currently fielding teams or plan to do

so in fiscal 2016 did not include dollar figures in their documents.

Budget justification documents appear to have borrowed some boilerplate text, presumably supplied by OMB, that explains the need for digital services teams and the gains in productivity and efficiency they can engender. One particular passage — "The suc-

The demand from the agencies is... more than we could ever satisfy.

MIKEY DICKERSON, USDS



cess rate of government digital services can be improved when the department has digital service experts on staff with modern digital product design, software engineering and product management skills" — can be found in more than a few of the documents.

Some agencies have spelled out specific plans for their digital services teams and made budget requests that are outsized, at least when compared to their overall IT spending.

The Commerce Department, for example, is seeking \$6.4 million for

its digital service, with an eye to standardizing its data and making it interoperable. The agency said it envisions a common data system as "a key asset that will enable the department to increase access to a more consumable version of the data it collects and produces."

The Department of Health and Human Services is requesting \$10 million for its digital services team. The agency wants 30 full-time employees and is focusing on establishing a core team with strong management skills to guide the development of digital services across HHS.

"The initial group will need core expertise in program management, program evaluation, procurement, data science, information architecture and structured content," the budget document states.

HHS leaders are taking advantage of the new program to promise tighter coordination between its CIO, chief technology officer and Office of the Assistant Secretary for Public Affairs, which has broad authority over the department's public-facing websites.

The Treasury Department is planning a 41-person, \$10 million digital services team that will focus on the usability of online government services across platforms and devices, better

IT procurement, and the use of data to drive innovation.

The Department of Homeland Security is seeking \$10 million for a 50-person digital services team that will bring commercial best practices such as agile development and open-source technology to bear on IT projects. The plan is for a decentralized team whose members are located at various DHS components.

The Small Business Administration is requesting \$1 million for a digital services team to improve and develop the agency's SBA One portal, which is envisioned as a one-stop shop for accessing loan, contracting, capital and other services.

The Department of Veterans Affairs did not release a dollar figure for its digital services team in its fiscal 2016

budget request, but the VA has by far the most mature program and has already shown results on several projects. The department has budgeted for a 75-person team, the largest outside the program office at OMB, and the price tag is surely far ahead of other agencies' programs.

Other requests include:

- Transportation Department — \$9 million
- Agriculture Department — \$7.6 million
- Justice Department — \$7.4 million
- Social Security Administration — \$4.6 million
- Interior Department — \$3 million
- State Department and U.S. Agency for International Development — \$1.3 million

- National Science Foundation — \$1 million

NASA, the Nuclear Regulatory Commission and the Office of Personnel Management include digital services in their budget requests, but do not specify a dollar amount or headcount.

The Obama administration has requested \$35.2 million for the Information Technology Oversight and Reform fund at OMB, which supports USDS and other governmentwide IT and e-government efforts. It's not clear how much OMB will devote to USDS, but the effort is budgeted for 87 full-time employees in fiscal 2016.

When OMB's request is added to agencies' funding, the overall digital services effort climbs to more than \$100 million. ■

REGISTER NOW

FCW WEBCAST SERIES

INSIDE CONTINUOUS MONITORING, INSIDER THREAT AND BEYOND

SESSION 3

PROACTIVE SECURITY THROUGH BEHAVIORAL ANALYSIS AND CONTROL

JUNE 17, 2015 AT 2PM ET

REGISTER NOW AT:

FCW.COM/HLT3XSERIES_SESSION3

DLT SOLUTIONS **ForeScout** **Symantec**

The quest for a single government login

Identity management is central to efforts to make a wide range of IT activities secure, but streamlining the process is essential

BY JOHN MOORE

A federal agency's website is on the front lines of delivering services to the public.

Indeed, a majority of Americans now go online to seek government services. A few years ago, the Pew Research Center estimated that 82 percent of U.S. Internet users search for information or complete a transaction on a government website, and a new Pew survey found that 40 percent do so via smartphones.

Unfortunately, individuals who want to access government applications and services generally must create a username and password for each agency site they visit. And agencies maintain their own identity management systems to authenticate users.

Security suffers as well; weak and stolen passwords rank among the top ways an online system can be compromised.

In response, the federal government has been moving toward an identity management approach that will let people use the same credential to conduct business with multiple agencies, thereby creating a common mechanism

for transmitting identity information and introducing stronger authentication.

But much work remains to be done. A key consideration is building a system that affords robust security but is easy to use. Onerous security measures invite users to pursue workarounds, which neutralizes the protections.

"The usability of secure identity solutions is something that the market has been struggling to improve for years," said Jeremy Grant, senior executive adviser for identity management at the National Institute of Standards and Technology. "We've had no problem developing 'secure' identity technologies, but if people don't use them, then they really don't offer much security."

Why it matters

Since the passage of the E-Government Act of 2002, myriad federal services have emerged online. A 2014 Government Accountability Office report noted that agencies operate more than 11,000 websites. As more people make the Web

How Connect.gov works

Under Connect.gov, government-approved partners issue digital credentials to individuals who want secure access to online government services without creating separate logins for every agency.

Source: Connect.gov

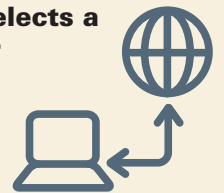
1. Customer seeks access to an online government application

When identification is needed to access an application, Connect.gov will appear as an option.



2. Customer selects a sign-in partner

The customer chooses from a list of approved sign-in partners and is directed to the partner's website to log into an existing account or register for one.



their default choice for government interactions, the need to provide safe access has become even more important.

The sharp rise in the use of mobile devices to access federal websites adds another dimension to the security challenge. The White House's 2012 Digital Government Strategy states that "policies governing identity and credential management may need to be revised to allow the introduction of new solutions that work better in a mobile world."

In general, identity management undergirds efforts to secure a range of IT activities, from mobility strategies to big-data initiatives.

"Identity and access management is the foundation for all security," said Paul Christman, vice president of the public sector at Dell Software.

The fundamentals

In 2009, the White House published a Cyberspace Policy Review that included the need to create a "cybersecurity-based identity management vision and strategy" on a list of 10 action items. That paper led to the launch in 2011 of the National Strategy for Trusted Identities in Cyberspace, which works with private- and public-sector entities to support the development of interoperable identity credentials. That move set the stage for a cloud-based, federated identity management solution.

A NIST-managed National Program Office coordinates NSTIC activities. The office collaborated with the General Services Administration to draft the requirements for the Federal Cloud Credential Exchange and awarded a contract to SecureKey Technologies in 2013 to create the exchange. FCCX was designed to let people use third-party credentials to access federal services online. In addition to improving the user experience, the governmentwide exchange would

help agencies sidestep the cost of credentialing the same person numerous times.

FCCX is now known as Connect.gov and falls under the auspices of GSA. The program allows people to use digital credentials provided by government-approved sign-in partners to confirm their identities when requesting access to online government services.

When they log in, users consent to share what Connect.gov describes as a "limited set of personally identifiable information." Connect.gov then serves as the pipeline for transmitting identity information from the sign-in partner to the agency's online application.

Jennifer Kerber, director of Connect.gov in GSA's Office of Citizen Services and Innovative Technologies, said Connect.gov has contracts with ID.me and Verizon to serve as sign-in partners, and other contracts will follow.

"We want to add more in the future to provide choice for the users," she said.

Kerber noted that six agencies are currently integrating with Connect.gov, and NIST, the State Department and the Department of Veterans Affairs will likely be the first to use the system.

In another development, Connect.gov's core technology, which is provided by SecureKey, was granted provisional authority to operate under the Federal Risk and Authorization Management Program. SecureKey CEO Charles Walton said that although FedRAMP certification is required for cloud-based services, it could have broader applications.

"As other online organizations start to use cloud-based services and cloud-based identity and authentication, FedRAMP lends a stamp of approval on our services," he said.

Connect.gov is not the only federal credentialing effort,

3. Customer's identity information is transferred to the agency

Once the customer has consented to share a limited set of personally identifiable information with the partner, Connect.gov facilitates the transmission of the identity information to the agency application.



4. Customer is given access to the online agency service

The customer now has access to the agency's application. Once a customer has registered with a sign-in partner, he or she can sign into all online government services that use Connect.gov.



however. Indeed, the NSTIC program office continues to spawn a variety of pilot projects for identity management.

ID.me, for example, has been working on a project to build on its Troop ID credential, which lets military personnel obtain discounts at online retailers. The pilot project aims to expand Troop ID's scope to include government services. In the initial phase of the expansion, veterans will be able to use the credential to access online services at the VA, said Matthew Thompson, founder and chief operating officer at ID.me.

The company plans to replicate that approach elsewhere. "We can scale that out to other government agencies," Thompson said.

Another expansion in the works will enable Troop ID credential holders to use that solution to access services at other government agencies via Connect.gov.

Resilient Network Systems, meanwhile, was among the first companies to receive pilot funding via NSTIC. The program office selected the company and its partners to create two pilot solutions for boosting information access in the education and health care fields, using Resilient Network Systems' Trust Network platform. (Note: Richard Spires, Resilient Network Systems' CEO and a former CIO at the Department of Homeland Security and the IRS, writes frequently for FCW.)

Grant, who helped launch the NSTIC program office, said more than a dozen pilot projects have been funded thus far, and he is excited about what they have accomplished.

"We actively chose pilots that pushed the envelope, with a focus on making something happen in the marketplace that otherwise would not," he said. "And while not every pilot has been a smashing success, collectively, the pilots have had a major impact in helping to catalyze the marketplace."

The hurdles

New identity management solutions face a number of challenges, but technical issues rate below other considerations.

"In the few occasions where pilots have struggled, it's rarely been because of technical challenges," Grant said. "The bigger issues have been around the policies and business rules involved with rolling out a new identity solution that is trusted by multiple parties across different sectors."

At GSA, Kerber said getting the public comfortable with using credentials via Connect.gov is one of the ongoing challenges. She said the important task is instilling trust in users, who are often concerned that a credential provider will keep track of the government websites they visit. However, the Connect.gov website states that the program "prevents sign-in partners from knowing which agencies or applications customers are accessing."

Grant also pointed to privacy protection as a key issue. He said officials have been addressing the challenge of creating identity solutions that handle individuals' personal data fairly and transparently without enabling new types of tracking.

"There are some great ways to build privacy into identity solutions right from the start, but it takes some extra effort," Grant said. "And in many cases, we've seen that unless organizations are proactive about protecting privacy from the start, these privacy-enhancing elements don't always make it into systems."

A poor user experience can discourage people from using an identity management system. Spires said issues can arise when a system doesn't fit what users are accustomed to or fails to conform to the users' notion of a good solution.

If "they have to go through a number of hoops to get data that they normally have access to," he said, it can prove difficult to retrain users to work with such a solution. ■

What's next?

- **Standards development.** Many government organizations have adopted single-sign-on solutions that are based on Security Assertion Markup Language. Although SAML's deployment history gives it staying power, standards such as OpenID Connect are growing in importance. Stu Vaeth, senior vice president of business development at Secure-Key Technologies, said OpenID Connect offers a simpler approach and a modern application programming interface. He added that where

legacy infrastructure isn't an issue, new identity management solutions will move to OpenID Connect.

- **Identity as a service.** Identities provided as a service — and not bound to a specific application — will become more prevalent in the next three years, said Paul Christman, vice president of the public sector at Dell Software. He said the approach will provide advantages in security, usability and application development.

- **Usability gains.** Industry and government are working on improving the usability of identity manage-

ment technologies. The National Institute of Standards and Technology, for example, issued guidelines last year for derived credentials, which can be deployed directly on smartphones and tablets. That method lets users avoid having to attach a personal identity verification card reader to a mobile device, which can be awkward. Jeremy Grant, senior executive adviser for identity management at NIST, said new solutions are being built into computers and mobile devices that will free users from carrying a separate verification tool.

— John Moore



FIREEYE GOVERNMENT FORUM

ADVANCING THE CYBER ENTERPRISE

PREVENT • DETECT • ANALYZE • RESPOND



Dave Dewalt
Chairman & CEO
FireEye



Kevin Mandia
SVP & COO
FireEye

Register today for the **ONLY** event where experts who protect the most valuable assets in the world will share their insights into the technology, intelligence and expertise which allow them to minimize the impact of security breaches.

JW Marriott, Washington DC
May 21, 2015

Register Today!

FCW.com/FIREEYE

SECURITY
REIMAGINED

When the agency CIO heads to Silicon Valley

Never mind the dress codes. The real divide between East and West is over how to build and for whom.

BY RICHARD A. SPIRES

A little over a year ago, I took the helm of Resilient Network Systems, an early-stage software company that has its headquarters in San Francisco. Since then, I have been living a bicoastal life, spending about a third of my time out West and the remainder in the Washington, D.C., area or traveling as needed to visit potential clients.

I have been in a startup before, and not surprisingly, it does feel like déjà vu. Resilient has many of the same issues that most early-stage companies face as they attempt to bring new products to market: building credibility and references, working to raise one's next round of funding, hearing lots of rejection from potential customers and investors, and getting jazzed when a new deal closes.

It's quite difficult, but I, like so many

other entrepreneurs, have a passion for what we are doing and the utmost belief that our technology can help change the world for the better. And like so many other entrepreneurs, I sometimes wonder why our value proposition is not immediately obvious to others.

Given my years of work in federal IT (both in and out of government), I understand this business and its culture. So I am finding it fascinating to face a new set of experiences and culture as I work in Silicon Valley and deal with venture capitalists, angel investors, other IT companies (small and large) and potential customers.

My observations reflect my personal experiences, and I appreciate that there are examples that one can cite that would not align with my observations. Still, I think it is instructive to reflect on some significant differences I have observed between West and East. There are important perspectives worth noting as all of us in government IT work to better capitalize on new, innovative technologies and solutions, and many of those innovations do indeed come from Silicon Valley.

• **Laid-back vs. buttoned-down.** The most obvious difference between West and East is reflected in visible cues of dress codes, office space, etc.

But if you work on both coasts, you quickly realize this is all just cosmetic. The laid-back label is not correct, and while there certainly are some truly buttoned-down firms in the East, that typically has less to do with a company's culture than with the persona they wish to project to their customers. That said, I do dress more casually on the West Coast.

• **Consumer vs. enterprise focus.** Perhaps most striking to me has been the more "consumer-oriented" approach to building business in the West than what I see in the East. Certainly there are Silicon Valley firms that do not sell directly to consumers, but even so, the approach is more about driving adoption at a grassroots level that in many cases has no immediate economic return.

Clearly, that strategy has been spurred on by the rise of companies that have changed the world of social media, and it is hard to argue given some of the successes we have witnessed in the past decade.

My sense is that the East struggles with this model. On the flip side, however, I also see a need for technologies and solutions that can drive needed change for large enterprises — and they are just not coming from large, established IT companies. And I have

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



found that West Coast investors are more reluctant to invest in such opportunities. Given their ultimate bottom-line orientation, they must feel that the chance for outsized returns is less in the enterprise market. The one current exception is companies that make cybersecurity products.

• **Speed vs. completeness.** The orientation in Silicon Valley is to quickly build a minimally viable capability, deploy it to get feedback and then incrementally improve from there. This is taking agile development beyond software to the business of building a company.

As I have learned from having participated in a number of startups, testing and refining your capabilities with potential and actual clients is the foun-

dation for success. Almost no one gets the killer app right at the start. It is the refinement through use and feedback from customers that is the key to creating a successful product or service.

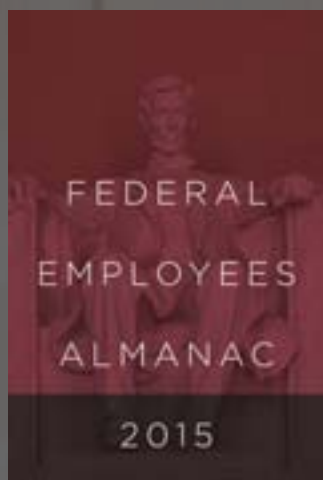
Unfortunately, as those of us who have worked in federal IT know all too well, this is not how the government typically buys. That is the critical rub and why many early-stage companies (no matter where they reside) are averse to selling to the government.

On a final note, I was recently pitching to one of the major venture capital firms on Sand Hill Road. Overall, it was going well — until we started to discuss our market focus. One of our target markets is the federal government because I believe our capabilities are well suited to support it. The investors'

reaction was very negative, which is indicative of how government is viewed by many West Coast investors.

Even though we have certain organizations — for example, the Defense Advanced Research Projects Agency and the Department of Homeland Security's Science and Technology Directorate — that are working to bring innovative technologies to government, the government as a whole continues to lag behind in technology adoption because it is not attracting young, innovative companies.

This is by no means an easy problem to solve, but any meaningful procurement reform should seek to address how to enable the most innovative firms to access the government market. ■



2015 FEDERAL EMPLOYEES ALMANAC

The *Almanac* is your one-stop resource on federal policy information — used annually by thousands of federal employees to reference the latest 2015 rules, regulations, and procedures.

NOW IN STOCK - ORDER TODAY!

Single copies start as low as \$23.95 Federal Soup subscribers save an additional 10%!

FederalSoup.com/FedStore • 800-989-3363

Overcoming fear of the inspector general

Overly aggressive oversight on the part of IGs is costing a fortune and stifling communication between agencies and vendors

BY KYMM McCABE

In 2013, inspectors general from 78 government offices processed a stunning 619,460 complaints that came in through their hotlines.

That's 1,697 per *day*.

In the same year, IGs claimed 19,000 indictments or criminal investigations, "successful" prosecutions, and suspensions or debarments, according to the annual report by the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

Interestingly, in 1995, there were considerably fewer take-downs. CIGIE's report for that year indicates there were 8,273 "successful" prosecutions, debarments, exclusions and suspensions of people or companies doing business with the federal government.

So have government and industry become more derelict — or have the IG offices become more fervent in their pursuits?

IGs are charged with the critical function of rooting out waste, fraud and abuse at their respective agencies. Their role was created in 1978 as an important safeguard in an unwieldy system in which taxpayer dollars might be subject to misuse.

In recent years, however, it seems

IGs have traded their magnifying glasses for microscopes and are prosecuting cases that in years past would have been handled administratively (for those at the highest level) or in the woodshed (for those at the lowest level).

Increased oversight, including the feverish rate of probes by the IGs, is creating a fearful paralysis in the entire federal system.

In its 2013 report to the president, CIGIE claimed that IGs' prosecutions "strengthened programs" and "resulted in significant improvements to the economy."

But my own quiet conversations with industry leaders, government executives and our hard-working public servants suggest a different and troubling reality: Increased oversight, including the feverish rate of probes by

the IGs, is creating a fearful paralysis in the entire federal system.

Drawing attention to the problem

The IT community is especially hard-hit by the chill. In a world in which systems and partnerships must necessarily be nimble and collaborative, fear of the IG has virtually frozen communications — and progress.

Government officials — especially those in the acquisition function, who are afraid of even the appearance of favoritism or impropriety — often choose to avoid direct contact with industry, even though such discourse is heralded as an important business practice under the Federal Acquisition Regulation and is actively supported by the Office of Federal Procurement Policy and Defense Department leaders.

Those communication barriers between government and industry are hardly new or unacknowledged. Since 2011, OFPP has actively championed a "myth-busting" campaign that is designed to dispel assumptions and fears about government interactions with industry. OFPP's administrator at the time, Dan Gordon, sorted rumor from rule regarding meetings, con-



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

REGISTER BY MAY 13 AND SAVE \$200!



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

Use promo code **SFMAY1**

versations and exchanges of information between government and industry. Ever since, the drumbeat encouraging improved communications has continued by top leaders across government.

But well-founded fear cannot be overcome by well-meaning efforts. Risk aversion is learned behavior, and therefore, suspicion and paranoia continue to dominate stilted conversations. And now the lack of communication is effectively preventing the development of good solutions, hampering competition and breeding poor decision-making.

And so, despite the demand to overcome risk aversion, foster collaboration, improve efficiency and decrease costs, the fear factor reigns.

Maybe more disturbing, though, is the McCarthy-era hush that has fallen over those in government and industry who are unwilling to publicly speak out about their concerns for fear of attracting unwanted attention and consequences.

Off the record, sources in both communities report widespread feelings of powerlessness. As one government procurement official told me, “No one oversees the IGs, so we have no place to turn.”

A former DOD official privately shared that he believes “we have reached the point that what were previously recognized as common, even routine, administrative and business decisions and debates are now being elevated to suspicion or even accusation of criminal wrongdoing and behavior.”

The official went on to suggest that “professionalism is being ceded to political and prosecutorial convenience, [which] in turn is resulting in a beaten-down workforce that sticks to rigid transactions rather than strategic thinking.”

Thankfully, media discourse is beginning to openly raise questions about the issues with the current IG structure and processes.

For example, in a recent highly publicized case, two IGs were at odds over an employee who once worked at the Department of Veterans Affairs and now works at the Treasury Department. A VA IG report concluded that the procurement official is guilty of misconduct. The Treasury IG said she’s not.

Interestingly, the individual in question had testified against the VA colleague who brought the case to the IG for creating a hostile work environment. Payback?

The Treasury IG, in a letter to the House Veterans’ Affairs Committee, quotes several witnesses who say the complainant openly sought to retaliate against the executive. And the Washington Post reports that Treasury’s IG is now accusing the VA’s IG of misconduct, saying the case “fuels growing concerns about [the VA IG’s] work.” The Post also reports that the VA’s IG is requesting an expedited review of the matter by CIGIE.

Interrupting the cycle

Observers in the federal community are watching the case closely in the hope that it will catch the eye of an authority that will help rebalance the scales in favor of a less punitive approach. But those hopes might be unfounded because, as is often the case, the policy and rhetoric originating from Congress are powerful drivers. And in February, Sen. Chuck Grassley (R-Iowa) introduced the Inspector General Empowerment Act of 2015, described on Congress.gov as a bill that would “strengthen the independence of the inspectors general.” So it seems that strengthened authorities and oversight might again be the default position.

Becoming the subject of an IG investigation is no small matter. Many report that when IG investigators come to your door, they assume guilt and hang around longer than your in-laws. Even if they find no wrongdoing, work is unnecessarily stalled and managers and workers are unfairly sullied. Parties involved in those investigations say they have been condemned before anything resembling due process has occurred. Even if you emerge with no conviction, you’ve probably been pretty well bloodied and bruised.

The enforcement mentality is not only casting a frost over important relationships, it’s costing a fortune. Government contractors spend an estimated 25 cents on the dollar complying with burdensome regulations and responding to a barrage of audits and investigations. And individuals faced with an IG inquiry are spending a personal fortune to gain and maintain representation for investigations that continue without a clear process or endpoint.

In short, we are trapped in a cycle of fear, risk aversion, suppression and, ultimately, mission failure.

It’s time to interrupt the cycle.

It’s time to shed light on the impact of current oversight policies and conduct a review of practices, processes and governance over our important but intimidating IG community.

It’s time for a transparent process by which the severity of a claim, level of investigation and process are determined and communicated. A proper vetting system would prevent lower-level complaints from improperly escalating and would be met with a collective “hurrah!”

Earnestly working to establish a more just and balanced approach would allow the IG community to continue its noble quest of ensuring integrity while beginning to mend the injured federal culture so we can all focus on what is most important: mission delivery, value and service to our country. ■

Kymm McCabe is president and CEO of Value Storm Growth Partners.

FCW Index

People

Adcock, Don..... 8	Jagannathan, Suresh..... 10	Rossino, Alex 15-17
Bartoletti, Dave..... 17	Johnson, Jeh 6	Soloway, Stan... 15-17
Bigman, Robert..... 3	Johnson, Michael 8	Spires, Richard 26, 28-29
Breakiron, Richard 21	Kapoor, Kay 16	Surowiecki, James..... 13
Christman, Paul 25-26	Kelman, Steve 13	Taylor, John 12
Coleman, Casey..... 8	Kendall, Frank..... 10	Thompson, Matthew 26
Deyo, Russell 8	Kerber, Jennifer 25-26	Thornberry, Mac.... 10
Dickerson, Mikey 22-23	Kneeland, Timothy..... 20-21	Vaeth, Stu 26
Gordon, Dan 8, 30	McCabe, Kymm..... 30, 32	van Riper, Kris 12
Grant, Jeremy... 24-26	Meehan, Tim 16	Walton, Charles 25
Grassley, Chuck 32	Minson, Julia 13	Wennergren, David 11, 15-17
Haines, Fred..... 6	Plexico, Kevin 15	Winnefeld, James.. 10
Halvorsen, Terry 20-21	Ross, Ron 3	

Agencies/Organizations

Air Force 20-21	ID.me 25-26
Amazon Web Services 14-15	Joint Chiefs of Staff..... 10
Army 20-21	Kryptowire 6
AT&T 14-17	Lockheed Martin 14-16
CEB 12	Microsoft 14-16
CenturyLink..... 14-16	Monster 14-15
CIA 15	NIH 7
CIGIE 30, 32	NIST 3, 24-26
Cisco 16	NSA 21
Commerce..... 22	OFPP 8, 30
Congress 10, 32	OMB..... 7, 22-23
DARPA 10	Partnership for Public Service.... 34
Dell Software 25-26	Professional Services Council..... 11, 15-16
Delttek..... 15-16	Resilient Network Systems..... 26, 28-29
DHS..... 6, 7, 8, 23	Salesforce..... 14-15
Docker..... 17	SBA 23
DOD 7, 10, 11, 20-21, 30, 32	SecureKey Technologies 25-26
DOE..... 8	Skyhigh Networks..... 12
Forrester Research 17	Splunk..... 14-16
GAO 7, 24	Treasury..... 22-23, 32
George Mason University 6	Unisys..... 8, 14-15
Google..... 17	USDS 22-23
GSA..... 6, 8, 16-17, 25-26	VA 23, 32
Harvard..... 8, 13	Value Storm Growth Partners... 32
HHS..... 22	Verizon..... 15-17, 25, 34
Huddle 14, 16	Vion..... 21
Human Rights Watch..... 8	White House 23, 25
IBM..... 14-16	

Advertisers

Carpathia Hosting, Inc.
www.carpathia.com **1a-1b**

DLT Solutions
www.FCW.com/DLT3Xseries_session3..... **23**

FCW Rising Star Nominations
www.FCW.com/2015RisingStars **35**

Federal Employees Almanac 2015
www.FederalSoup.com/FedStore **29**

FireEye Government Forum
www.FCW.com/FIREEYE **27**

GEICO
www.geico.com **2**

SAP National Security Services
www.SAPNS2.com **36**

TDWI
www.tdwi.com **9**

The Boeing Company
www.boeing.com/militaryaircraft..... **18-19**

Visual Studio Live San Francisco
www.vslive.com/sf **31**

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

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

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

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

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

Cybersecurity's same old song

The good news: Most threats continue to fall into a few well-understood categories. The bad news: Government remains a top target, and it still can't hire enough cybersecurity talent.

79,790

total security incidents in 2014 (all sectors)

50,315

public-sector security incidents in 2014

2,122

incidents with confirmed data loss (all sectors)

303

public-sector incidents with confirmed data loss

2.6%

of all reported incidents involved confirmed data loss.

63%

of the reported incidents show that public-sector systems were the target.



Most incidents fall into nine attack patterns:

29.4%

Miscellaneous errors

3.9%

Denial of service

25.1%

Crimeware

0.8%

Cyber-espionage

20.6%

Insider misuse

0.7%

Point-of-sale intrusions

15.3%

Physical theft/loss

0.1%

Payment card skimmers

4.1%

Web app attacks

The challenge of finding and keeping cybersecurity talent hasn't changed much either.

There are **92,863** civilian cyber employees governmentwide. But agencies lost more than they hired last year:



5,335
fiscal 2014
separations



4,709
fiscal 2014
new hires

And **pay gaps** remain a significant obstacle to recruiting top talent, with private-sector software engineers earning more than their federal counterparts:

\$8,000-14,000
entry level



\$24,000-33,000
senior level

Sources: Verizon's "2015 Data Breach Investigations Report" and Partnership for Public Service's "Cyber In-Security II: Closing the Federal Talent Gap"

N O M I N A T I O N S D U E J U L Y 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



**RISINGSTAR
AWARDS**

GOT CYBER BIG DATA?

UNLOCK IT WITH SAP HANA®

*MULTI-MODAL INGEST AND
DIMENSIONAL ANALYSIS ON
ONE CONVERGED PLATFORM*

The SAP HANA platform, delivered by SAP NS2, offers multiple capabilities to cyber defenders in one easy-to-deploy server, including high performance in-memory processing of both streaming and historical data using predictive, geospatial, unstructured text and graph-engine link analysis.

WWW.SAPNS2.COM
info@sapns2.com
877-972-7672



NATIONAL
SECURITY
SERVICES®

