FCW
THE BUSINESS OF FEDERAL TECHNOLOGY

HOW HARD CAN HEALTH RECORDS BE?

The Defense Health Agency's David Bowen is about to find out

PAGE 20

+ The Pentagon's push on biometrics

PAGE 14

SEWP: The inside story

PAGE 24

MARCH 15, 2015 • VOLUME 29 NUMBER 3

Trending

$1.6B is the cost of a proposed DOD-wide license agreement with VMware that is being protested as unduly restrictive to competition

The new frontier for information sharing

How cyberthreat information-sharing practices between government and industry develop in the next few years will set the tone for that collaboration for decades to come, said White House Cybersecurity Coordinator Michael Daniel.

In the next three to four years, "we will be defining how a lot of these relationships will operate for the next 50," Daniel said at an Atlantic Council event in February. Given that most cyber-related infrastructure is privately owned, "there is almost no other issue in the national security and the economic security space…that is shared in that same manner."

The key role of the private sector in cybersecurity "means that we are having to chart…some new ways of interacting between the government and the private sector that don't fall neatly into traditional regulatory or contractual categories that we've had," he added. "And so as a result, we're struggling, in many ways, to figure out what those relationships are going to be."

A recent executive order seeks to flesh out those relationships by encouraging exchanges beyond established, sector-specific information sharing and analysis centers.

Daniel also echoed a common warning from cybersecurity experts that information sharing is just a means to an end, not a solution unto itself. Different types of information sharing are needed for active cyber defense and situational awareness, he added, without elaborating on those methods.

In addition, a newly announced Cyber Threat Intelligence Integration Center will free up cybersecurity specialists at the National Security Council to evaluate and coordinate intelligence and get them out of the business of interpreting raw signals, Daniel said.

In the next three to four years, "we will be defining how a lot of these relationships will operate for the next 50."
— MICHAEL DANIEL

"There's a degree of integration that's occurring on my staff that really should not be occurring," he said. "It needs to come into us that way. I think that [CTIIC] will be a great force multiplier in this space."

The center is modeled on the National Counterterrorism Center and will operate under the authority of the Office of the Director of National Intelligence. It will have about 50 staffers to start, about half of whom will be permanent employees of CTIIC and half detailees from the intelligence agencies that will be its customers.

"At least in our conception right now, the staffing of the center will be government because it's primarily not designed to interact with the private sector on a daily, ongoing basis," Daniel said.

Sector-specific knowledge will come from cybersecurity specialists at the FBI and Department of Homeland Security who have experience working with the private sector. "That's one of the issues that we do need to consider — how the CTIIC's knowledge base and capabilities remain relevant and fresh and up-to-date," Daniel said.

Primarily, CTIIC is being conceived of as a "government back-office organization designed to enable the centers to do their job better and enable the White House to do a better coordination function with the agencies," he added.

— Sean Lyngaas and Adam Mazmanian

FCW CALENDAR

3/26 **Federal 100**
The 26th Annual Federal 100 Awards Gala will honor this year's winners and announce the 2015 government and industry Eagles. Washington, D.C.
fcw.com/fed100

4/1 **IT modernization**
The ModernGov Summit, presented by FCW, will feature insights into portfolio management, proactive analytics, business strategy and more. Washington, D.C.
fcw.com/moderngov

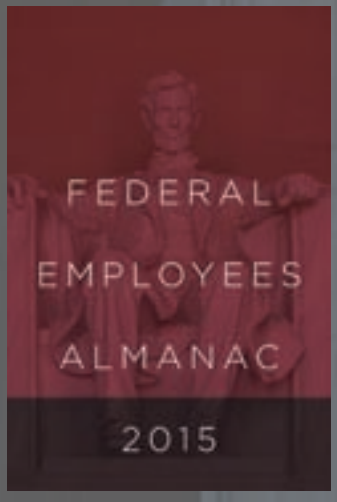
4/2 **Cybersecurity**
U.S. Cyber Command's Adm. Mike Rogers, DHS' Phyllis Schneck and the FBI's Joseph Demarest are among the speakers at this AFCEA Washington event. Washington, D.C.
is.gd/FCW_AFCEAcyber

Contents

TRENDING

DEPARTMENTS

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

FCW
THE BUSINESS OF FEDERAL TECHNOLOGY

SALES CONTACT INFORMATION

MEDIA CONSULTANTS

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

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

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

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

EVENT SPONSORSHIP CONSULTANTS

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

90% of "anonymized" credit card users in an MIT study were identified using four readily available contextual clues

Obama gets an earful about acquisition

Leaders from the General Services Administration's Federal Acquisition Service have talked with President Barack Obama twice in recent weeks about FAS initiatives to bring more efficiency to the federal acquisition process.

FAS Commissioner Tom Sharpe said executives met with the president on Feb. 2 and again on Feb. 9 to talk about the agency's efforts to develop a Common Acquisition Platform (CAP) and detailed product category hallways that federal IT buyers can use to build better solutions and get better prices.

Sharpe mentioned the meetings as part of his remarks at a Professional Services Council event on Feb. 13. Although he declined to share details, industry and agency officials told FCW that the conversations lasted 10 to 20 minutes and covered GSA's work to strengthen federal acquisition practices, improve efficiencies, and reduce red tape through category management and CAP.

Sharpe and Obama also discussed other activities the government could undertake to bolster federal acquisition practices.

"The meetings may not have been long, but they were significant," said one source familiar with the talks.

Kevin Youel Page, assistant commissioner of GSA's Integrated Award Environment, and Laura Stanton, GSA's director of program management for CAP, were also present at the presidential meetings, according to sources.

Alan Chvotkin, PSC's executive vice president and counsel, said FAS' meetings with Obama "send a strong signal to agencies that this stuff matters."

— Mark Rockwell

Pushing ahead on spectrum sharing

Now that the government has auctioned off 65 MHz of highly coveted spectrum formerly controlled by the Defense Department, the Commerce Spectrum Management Advisory Committee (CSMAC) has turned its attention to how agencies will go about making more spectrum available for commercial use.

The committee, a group of experts from the private sector who advise the National Telecommunications and Information Administration on policy, did much of the groundwork for clearing that spectrum and relocating incumbent users.

Now while NTIA and other government entities are exploring the prospects for dynamic, real-time spectrum allocation, CSMAC is answering tough questions about how sharing policies might look in the highly regulated federal and commercial environments. The work is an important part of the Obama administration's plan to unleash 500 MHz of spectrum for commercial use by 2020.

In a February meeting, CSMAC adopted draft recommendations to address how government and industry might begin to sort out security issues by using a database-driven approach to spectrum sharing and how sharing might work in both directions by also giving government access to commercially licensed spectrum for emergency use.

CSMAC's recommendations are non-binding, but its deliberations give policy-makers a sense of expert consensus. The group is still developing guidance on how to measure and predict agencies' spectrum needs and how agencies might be compensated for sharing or relinquishing spectrum for unlicensed use.

However, legislative action might be required. Accordingly, a bipartisan, bicameral group of lawmakers is backing the Wi-Fi Innovation Act, which would set swathes of spectrum in the 5 GHz band for unlicensed use.

Beyond mobile communications, aerial drones, traffic management systems and other users are competing for precious airwaves.

— Adam Mazmanian

INK TANK

28% of the global cloud infrastructure market now uses Amazon Web Services, according to Synergy Research Group

FCW Insider: People on the move

Acquisitions expert **Rich Beutel** helped write and managed passage of the Federal IT Acquisition Reform Act while serving as a senior staffer on the House Oversight and Government Reform Committee, and he has now turned his attention to industry.

Rich Beutel

His new consultancy, Cyrrus Analytics, is aimed at guiding midsize cloud service providers through the maze of compliance directives required to do business with the federal government.

Beutel launched Cyrrus in late January, and so far he's landed Adobe and MeriTalk as clients.

"I [will] be problem-solving issues that are hindering clients' ability to do business with the federal government," Beutel told FCW in an email message.

He said his areas of practice include achieving certification under the Federal Risk and Authorization Management Program, keeping up with the National Institute of Standards and Technology's security guidance, navigating agency procurement models and understanding general government contracting issues.

Jeremy Grant, the National Institute of Standards and Technology's senior executive adviser for identity management, is leaving government.

Federal News Radio reported that Grant, who leads the National Strategy for Trusted Identities in Cyberspace, has not announced future plans but will leave NIST in April.

Dana Keoki Jackson is now vice president and chief technology officer and **Rodney Makoske** is senior vice president of corporate engineering, technology and operations at Lockheed Martin.

Jackson has worked for the defense giant since 1997, most recently as the vice president in charge of integrating the firm's five disciplines. Makoske was most recently a vice president in charge of the company's Mission Systems and Training business area.

— FCW staff

EDITOR'S NOTE

When government is the innovator

It's a common refrain in federal IT: "If only the government could be more like the private sector."

If only agencies would be more agile. If only we could hire more Megan Smiths and Tony Scotts and Mikey Dickersons and DJ Patils. If only there were enough Presidential Innovation Fellows for every IT shop. If only...

The converse, meanwhile — that steady brain drain as talented feds take jobs in industry — is dismissed as "cashing out" or smart people getting fed up with government.

It's worth remembering, however, that great things get started at both ends of the street. And there were two excellent examples of that in recent weeks.

First, there is Hyperion — a malware detection and software assurance package developed by the Energy Department's Oak Ridge National Laboratory that outshines existing commercial solutions. R&K Cyber Solutions licensed Hyperion in January, and it was the second government cyber technology to go commercial via the Department of Homeland Security's Transition to Practice program.

Then there is Sqrrl, a big-data security startup that FCW flagged as a "hot company to watch" in 2013. It was founded by former White House and National Security Agency officials, and a few weeks ago it launched Enterprise 2.0 — a full-fledged version of a product that grew out of NSA's Apache Accumulo data-mining system.

In both cases, technology developed for government missions has proven to have much broader potential — and the private sector has jumped on those innovations.

Commercial adoption of federal technology dates back to the earliest days of IT and continues unabated — even if we sometimes act as though it ended with NASA's Apollo program.

None of this is to knock the Obama administration's aggressive recruiting in Silicon Valley. Federal IT absolutely needs new blood, but let's not pretend that government lacks homegrown innovators. We will showcase a slew of them in FCW's next issue, in fact, and there are countless others.

Innovations — and innovators — are tucked away in all sorts of places. Let's not forget to look in government.

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

$4 million is the Army's estimated savings from adopting NASA-built automated software development procedures

Is government ready for agile?

An organization that promotes agile development, Agile Government Leadership, has released a new handbook that lists resources such as books, white papers, directives and articles, and includes a checklist, key questions and a "manifesto" of rules to live by when using agile techniques.

"We find that many people are interested in agile in government, but they don't know how to begin, so they sort of need an introductory text on agile use in government," said Robert Read, co-founder of the General Services Administration's 18F and a member of AGL's Steering Committee. "I think it's a great starting point for information about doing agile, although I think people really need to practice agile in order to understand it."

We find that many people are interested in agile in government, but they don't know how to begin, so they sort of need an introductory text.

— ROBERT READ

About a year ago, GovFresh founder Luke Fretwell teamed up with software integration company CivicActions on a number of projects, including researching the use of agile development in government. After surveying the field, Fretwell said two things stood out.

First, no community for agile had come together in government. "We wanted to create a hub and the community to support [agile development], so we started working with government officials and building that community," Fretwell said.

Second, feds' awareness and understanding of agile development varied. "There was an agile divide," Fretwell said. "There were people like Robert who are expert in agile and then other people who didn't have a clue what agile is."

Aside from what 18F and the U.S. Digital Service have done recently to raise awareness of new methods and techniques, the TechFAR Handbook also makes a case for why government should adopt agile techniques for IT development and project management. And the Government Accountability Office released a list of 10 best practices for agile development in July 2012.

In the spirit of the movement, AGL's Agile Government Handbook has been published on GitHub, and the team is asking for feedback.

"We're expecting that there are people who are new to agile using it and then more seasoned people using agile who may have more case studies or success stories to add," said Elizabeth Raley, director of professional services at CivicActions. "We're seeing the handbook as an iteration as well that we can continue to add things that will be of great use to the people using it."

Read said the intended customer is "the person who is in control of a $200,000 to $20 million budget, who needs to run an IT project and wants to do a good job using modern software methodology but doesn't necessarily know where to begin and may not even be sure if they have permission to use agile."

But do agencies have the processes and people in place to adopt agile methodology?

"That's like asking whether the government is ready for oxygen," Read said. "It needs it, whether it knows it needs it or not. I think the federal government is ready, [and] program managers are ready to see immediate results and de-risk projects by having gradual progress."

He added that government procurement strategies, however, might not be ready.

"We need to discover ways to procure agile services properly," Read said. "But we're breaking new ground in that respect."

— Colby Hochmuth

CMS sends faulty tax info to 800,000 customers

The government sent incorrect tax information to about 800,000 people who received subsidized health insurance under the 2010 health care law.

The glitch is the result of a miscalculation of the benchmark monthly premium amount that is used to determine subsidies. It is keyed to the second lowest priced Silver plan available to a customer in his or her state. That information, presented on the new 1095-A tax form, is used to calculate the total tax credit available to a filer for the year.

Taxpayers who receive coverage under the law are required to reconcile any advance tax credits with their premium costs and their income for the year. Some people will owe tax on advance credits, based on changes in their income.

Officials at the Centers for Medicare and Medicaid Services are investigating what went wrong with the forms and said revised tax documents will go out in early March. Filers can also get their benchmark rates via a tool on HealthCare.gov.

— Mark Rockwell

215+ government authors contributed to DigitalGov.gov in its first year of publication

IN THE IT PIPELINE

WHAT: A General Services Administration request for information looks to industry and federal users for ideas about how to push ahead with its cloud acquisition contracting, including alternative models and processes.

WHY: The Cloud Computing Services Program Management Office offers cloud IT services to federal, state, local and tribal governments through an infrastructure-as-a-service (IaaS) blanket purchase agreement and an email-as-a-service BPA. GSA is looking for ways to evolve those purchasing vehicles in the face of fast-moving technology and capabilities.

Officials said informational meetings about a new special item number for cloud technology under IT Schedule 70 generated feedback from industry and federal agencies on how GSA could improve existing IaaS BPAs.

The feedback noted that cloud professional services contracts could include more assessment, planning, migration and integration capabilities; more extensive training; a more comprehensive suite of cloud products and services; and more flexibility to keep current with the growth of cloud products and services.

GSA also said the feedback suggested cloud acquisition vehicles should allow for opportunities to take advantage of the increasing number of authorizations under the Federal Risk and Authorization Management Program.

FULL LISTING:
is.gd/FCW_gsa_rfi

In search of a mobile app standard

The CIO Council's Mobile Technology Tiger Team has released a set of criteria for federal agencies to vet mobile applications. The goal is to create more consistency in their vetting standards and enable industry to better meet agency needs.

The criteria follow the National Institute of Standards and Technology's Special Publication 800-163, "Vetting the Security of Mobile Applications."

"The vision is to have industry and government respond alike," said Robert Palmer, acting deputy executive director of the Enterprise Systems Development Office at the Department of Homeland Security and co-chairman of the tiger team. "From my perspective, being a practitioner in [the DHS CIO's office], I would love to have a suite of tools that I could readily get to through whatever vehicle that I know meet [these] criteria."

The criteria were rolled out through the National Information Assurance Partnership, and the materials will be housed in the NIAP Protection Profiles. The group has been developing the technical aspects of the criteria for a year and a half and signed off on them last week.

"We have a situation where we're taking all of the great work done individually and collectively by federal agencies and industry, aligning it in terms of making sure the technical details are in sync and having a good home for sharing," Palmer said.

The Defense Department and DHS have taken the lead in adopting the criteria, with both agreeing to follow the guidelines, he added.

Several industry days are planned to generate awareness of the new criteria, and the group also plans to publish the guidelines through the CIO Council.

The benefits will manifest themselves in the response from industry, Palmer said. Companies can streamline the process for adopting new applications by making tools that meet the criteria. In an environment where the number of applications is growing so rapidly, having industry work with one set of standards will save agencies time and money.

"When we write the guidelines, we like to talk to industry directly to make sure that what we recommend can actually be performed by industry," said Tom Karygiannis, an author of NIST's SP 800-163. "You don't want to create a guideline or requirement that no one can meet. I think when compared to what the state of practice is in industry, we've raised the bar a little bit and gave them a target to improve what they're doing now."

— Colby Hochmuth

Phaedra Chrousos
@PSChrousos

FedRAMP website set for makeover! Can't wait to see it @MrFedRAMP (no pressure :)) http://fcw.com/articles/2015/... via @FCWnow

Reply Retweet Favorite

10:49 AM - 22 Feb 2015

Join the conversation

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

IS YOUR DATA CENTER A DUMPING GROUND?

WE'VE GOT THE ARCHITECTS TO REBUILD, REORGANIZE AND OPTIMIZE.

CDW·G **ITES–2H** Ordering Guide

Contract #W91QUZ–07–D–0009

ITES·2H · INFORMATION TECHNOLOGY ENTERPRISE SOLUTIONS

CDW·G PEOPLE WHO GET IT™

CDW·G and ITES-2H HAVE YOUR I.T. REQUIREMENTS COVERED

About ITES-2H and CDW·G

CDW·G was awarded the ITES-2H (Information Technology Enterprise Solutions-2 Hardware) contract to support the Army's requirements covering a full range of Information Technology (IT) equipment for server, storage and network environments; for related integration services; and for maintenance/warranty of legacy IT equipment as part of an ITES-2H solution.

CDW·G provides the purchase of commercial RISC/EPIC servers, Intel/AMD servers, desktops, notebooks, workstations, thin clients, storage systems, networking equipment (including wireless), network printers, product ancillaries (including equipment cabinets, racks and mounts), peripherals (including monitors), network cabling products, video teleconferencing (VTC) products, stand-alone displays (for example, plasma screens, HDTVs), scanners, Everything over Internet Protocol (EoIP) products, communications devices, power devices, basic warranties and warranty options, and other related accessories and options.

ITES-2H CATALOGS

Catalog I: RISC/EPIC-based Servers
Catalog II: Windows-based Servers
Catalog III: Workstations, Thin Clients, Desktops and Notebooks
Catalog IV: Storage Systems
Catalog V: Networking Equipment
Catalog VI: Network Printers
Catalog VII: Cables, Connectors and Accessories
Catalog VIII: Video Equipment Products
Catalog IX: Uninterruptible Power Supplies (UPS)

CONTRACT INFORMATION

Issuing Agency:
Army Contracting Command — Rock Island
1 Rock Island Arsenal
Rock Island, IL 61299-8000

ACC/NCR Contracting Office:
Contracting Officer:
Ilana C. Bohren
309.782.1844
Ilana.C.Bohren.civ@mail.mil

Army Computer Hardware, Enterprise Software and Solutions (CHESS):
Product Leader
Nicole Wilson
703.806.8436
nicole.e.wilson23.civ@mail.mil

CHESS IT E-mart:
https://chess.army.mil
888.232.4405

CONTRACT DURATION:
Visit the CHESS website at chess.army.mil
The contract is currently set to expire 6/23/15

Authorized Users:
Visit the CHESS website at **chess.army.mil**
Open to Army customers only

CDW·G ITES-2H Payment Information:
Contract #W91QUZ-07-D-0009
Federal Tax ID number: 36-4230110
DUNS number: 026157235
Cage Code: 1KH72

Remit to address:
75 Remittance Drive, Suite 1515
Chicago, IL 60675

Wire and EFT:
The Northern Trust Company
50 S. LaSalle Street
Chicago, IL 60675

Routing transit number:
Routing #071000152 Account #91057

CDW·G ITES-2H Sales Team:
CDWG.com/ites2h
Contact your dedicated CDW·G account manager:
866.371.2362
ites2h@cdwg.com

Website: CDWG.com/ites2h
Send RFQs to: ites2hquotes@cdwg.com

CDW·G ITES-2H Program Management Office:
Kathy Gaston, Program Manager
703.621.8222
kgaston@cdwg.com

Neil Hooper, Contracts Administrator
703.621.8206
neil.hooper@cdwg.com

CDW·G Warranty/Tech Support:
ites2hsupport@cdwg.com

COMPLETE YOUR MISSIONS WITH THE RIGHT I.T.

Cisco® Catalyst® 3850-24T-S Switch
Enterprise-class stackable Ethernet access and aggregation layer switches

CALL FOR PRICING

Cisco® Catalyst® 3850 Series Switches support BYOD/mobility and offer a variety of performance, security and operational enhancements versus previous models.

Palo Alto SFP+ Transceiver Module 10GBase-SR

CALL FOR PRICING

Ethernet 10GBase-SR, plug-in module, SFP+ transceiver module.

F5 Enterprise Manager Appliance 4000
Reduce the cost of managing your application delivery infrastructure

CALL FOR PRICING

Optimize application performance; gain flexibility by using both virtual and physical management appliances.

Nutanix NX-3260 Virtual Computing Platform
Converged infrastructure for remote and branch offices

CALL FOR PRICING

Standardize branch office infrastructure to ease IT headaches, run any VM on a turnkey appliance in less than 30 minutes and remotely manage all locations with simplified workflows from a single interface.

NetApp® FAS6240 Series Scale-Out Unified Storage Systems
Powerful, affordable, flexible data storage

FAS6240 (12U base) **CALL FOR PRICING**

Highly available controller configurations with NetApp® Data ONTAP® 7.2.4 or later software and integrated automatic RAID manager.

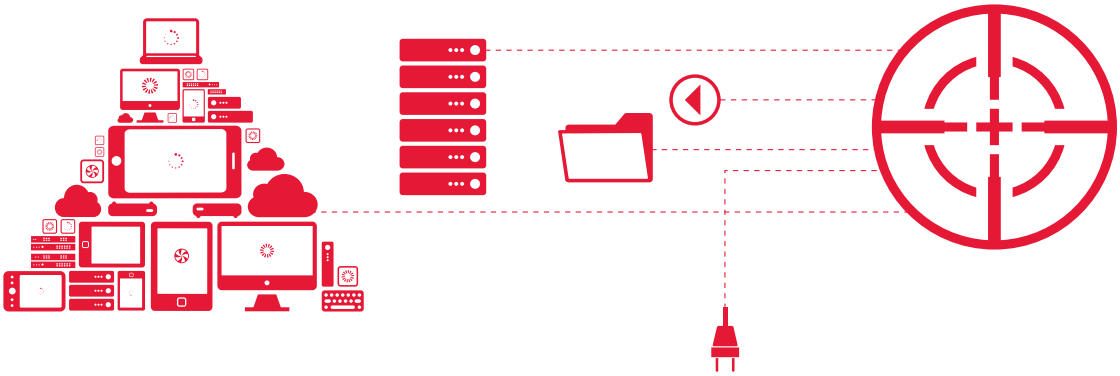
ORDER FROM THESE LEADING BRAND-NAME MANUFACTURERS:

APC	ClearCube Technology	Enterasys	Hitachi Data Systems	Liebert
Avocent	CommVault	Ergotron	IBM	NetApp
Belkin	Criticom	F5 Networks	Intel	Oracle
Blue Coat	Dell	Fluke Networks	Intermec Technologies	Polycom
Brocade	Data Domain	Fortress Technologies	Juniper	Red Hat
CA	Eaton Corporation	Hardigg	Kingston Technology	Symantec
Cisco	EMC	Hewlett-Packard	Lexmark	WYSE

For more information on IT products from these leading partners, call your dedicated CDW·G account manager.

ITES-2H

CDW·G PEOPLE WHO GET IT



MISSION OPTIMIZATION

Brick by brick, byte by byte, your organization's data storage needs expand every day — and your available space continues to shrink. Years of patchwork remodeling have left data centers with redundant and incompatible systems. And your aging infrastructure also struggles under the weight of new cloud, mobility, security, Big Data and storage solutions.

CDW•G's solution architects can rebuild your data center on a rock-solid foundation. After assessing your needs, we'll draw on our vendor partnerships and your existing resources to bring your data center optimization plan to life.

For more information, call your dedicated CDW•G account manager at **866.371.2362** or visit us on the web at **CDWG.com/ites2h**

To see how CDW•G delivers solutions for global Army customers, visit us today at **CDWG.com/federalsolutions**

CDW•G **ITES-2H** Ordering Guide

Contract #W91QUZ-07-D-0009

150213 MKT5264

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

The right tool for the job

Rather than falling back on the same old solutions, federal IT professionals should discern the best approach to achieve the desired outcome

When I was a kid, my dad used to hammer (forgive the pun) two pieces of advice into my head: "You need to use the right tool for the right job" and "there's a right way and a wrong way to get things done." They were talks I probably deserved but was sometimes reluctant to hear.

It is so easy in life, as we gain knowledge and skills, to fall back on what we know best and make the mistake of presuming that our favorite technique or approach fits all circumstances. It's like that other old adage: "If all you have is a hammer, everything looks like a nail."

For today's government workforce, being savvy about the breadth of tools available and understanding the circumstances that argue in favor of the use of a specific tool are crucially important. Interestingly, although the government technology workforce has aged, people have not retired at the rate predicted. For every government technology worker under the age of 30, there are 10 technology workers who are 50 or older, and that ratio has been increasing in recent years.

Conversely, almost 50 percent of the contracting community workforce has less than 10 years of federal experience, and half of those workers have less than five years of experience. The saw cuts two ways. The more experienced the workforce, the more likely they are to view new opportunities through the lens of their past experience. Yet less experienced workers are less likely to have the confidence to embrace a new set of tools.

Furthermore, complaints about a lack of innovation in government solutions are to some degree attributable to contracting practices that stymie the ability to offer new ideas. When the toolset being used in government contracting is unnecessarily limited, opportunities to get better results are missed.

> When the toolset used in government contracting is unnecessarily limited, opportunities to get better results are missed.

Rigid statements of work, as opposed to statements of objectives, limit the ability of industry to bring new ideas and technologies to the government. Punishing rather than rewarding the identification of alternative approaches during proposal reviews similarly narrows the aperture for new thinking.

And the misuse of contracting techniques such as lowest price, technically acceptable further limits the ability to bring the best minds and fresh ideas into government solutions.

A broader set of tools, including managed services and performance-based contracting, could yield better results.

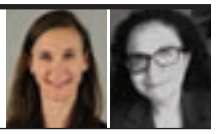
Agile is currently riding a wave of mounting enthusiasm in government, and some of its key tenets — such as a rapid, iterative approach; placing a premium on customer collaboration; and the flexibility to navigate uncertainty and adapt to change — have broad applicability to the program management process.

Too often, though, the fact that agile techniques come from the world of software development pre-ordains a solution that relies on extensive software development. In reality, the tenet of "agile discovery" is what's crucial to discerning the best approach. Sometimes the right answer might be implementation of a managed service or use of a commercial product rather than software development.

Simon Sinek, in his book "Start With Why," argues that we spend far too much time on *what* needs to be done — the specific, detailed steps to be used in delivering a solution — and not enough on *why* and *how*. By starting with *why* — the outcome we need to achieve and the reason it matters — we will be better able to discern the contracting approach that will deliver the mission results we seek. ■

Commentary | KRIS VAN RIPER AND AUDREY MICKAHAIL

KRIS VAN RIPER is a managing director and **AUDREY MICKAHAIL** is director of the IT practice at CEB.



Exploring the next wave of IT cost cutting

By applying a long-term mindset to strategic cost-saving initiatives, agencies can reshape how IT supports mission delivery

Since 2010, the Defense Department has been pressured to cut costs. To preserve funding for military operations and training, officials have targeted other areas for cutbacks, including IT. DOD's IT team has responded by eliminating waste and identifying a wide range of quick fixes with the hope of increasing the value of its IT spending.

DOD's initial cost-cutting efforts, like most organizations', focused on reducing obvious waste (e.g., consolidating duplicative contracts) and physical consolidation. Since sequestration in 2013, DOD has also sought to reallocate nearly $2 billion of IT spending, largely through identifying and reducing unnecessary or uncoordinated spending. In 2014, DOD cut 2 percent from its IT budget and has reported that it will cut another 3 percent in 2015.

Although DOD's efforts have been important and necessary, enduring cost-saving initiatives yield greater returns when they are part of longer-term plans to increase portfolio efficiency. Without those plans, an organization can lose business value and flexibility, and ultimately create more cost and risk.

In the next wave of cost-saving initiatives, DOD officials must focus on the 74 percent of their IT budget that covers operations and maintenance of legacy assets to create long-term savings. That approach will also make it possible to reallocate funding to new development and innovation projects, such as mobile computing.

The next generation of cost-saving initiatives will take longer but, if executed effectively, will be more transformative. In our work with hundreds of IT departments, CEB has identified a set of tactics that are essential to effective IT portfolio optimization:

• Streamline existing assets. Leading organizations know that legacy portfolios can introduce unnecessary and costly complexity, so they regularly assess their assets by cost, value and risk to identify top candidates for retirement. Although attempts to retire technology are often met with resistance, progressive organizations include clear business cases that highlight the financial and user benefits of retirement and the risks associated with inaction.

> Organizations are more likely and able to be innovative when their IT portfolios are operating efficiently and effectively.

• Minimize waste from new investment. IT teams should enhance the value of new investments throughout projects' life cycles. Leading organizations design frameworks that explain a project's cash flow impact and help sponsors make trade-offs on cost and delivery speed.

• Encourage a culture of reuse and shared-services delivery. Although many organizations aspire to share services, that activity falls under the category of transformative initiatives, which means cost-saving benefits will take time to accrue. In the meantime, all organizations can prepare for the changes shared services will produce by encouraging sharing and reuse at the system and asset levels.

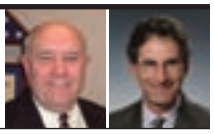
By successfully implementing longer-term cost-saving initiatives, agencies can ensure widespread positive effects. First, cost savings will unlock an agency's potential to operate as a leaner, more flexible organization with the ability to invest more resources in innovation platforms. Second, the agency will be further equipped to drive innovation. In fact, CEB research has found that organizations are more likely and able to be innovative when their IT portfolios are operating efficiently and effectively to support mission delivery.

And finally, agencies can introduce new capabilities faster by effectively allocating resources and rationalizing and consolidating their existing IT portfolios to minimize integration and security complexity.

DOD has achieved cost savings by eliminating waste and instituting better asset management. The next stage of efficiency initiatives can unlock even greater potential. ■

Commentary | JOHN LAINHART AND DAN CHENOK

JOHN LAINHART leads IBM's Public Sector Cybersecurity and Privacy Services, and **DAN CHENOK** is executive director of the IBM Center for the Business of Government.



Legislation and the future of federal cybersecurity

New laws promise to strengthen agencies' efforts to block network intruders, share information and build a top-notch cybersecurity workforce

Cybersecurity continues to be at the forefront of national focus, thanks to Congress' passing and the president's signing of three cybersecurity-related bills last December.

Those statutes are now being implemented to continue the progress agencies have made in protecting government networks and working with state and local agencies, critical infrastructure operators, and other private-sector partners to achieve similar progress.

First, the **Federal Information Security Modernization Act** of 2014 moves government forward in adapting to the ever-changing landscape of the cyber world. Its importance is evidenced by the increasingly complex vulnerabilities, threats and actions against federal networks.

The act enables federal agencies to be more effective in developing and implementing protective strategies against network intruders. It continues and updates the risk management framework that has been a core tenet of the Federal Information Security Management Act and encourages agencies to use automated security tools to continuously diagnose and mitigate security vulnerabilities. It also codifies the Department of Homeland Security's role in overseeing the implementation of policy and guidelines for federal civilian agencies.

Concurrently, the **National Cybersecurity Protection Act** codifies the activities of DHS' National Cybersecurity and Communications Integration Center and strengthens DHS' ability to coordinate incident response and provide technical assistance to agencies.

It authorizes DHS' existing center to act as a critical interface for sharing cybersecurity information among federal civilian agencies and key stakeholders. The law also includes provisions for:

- Promoting situational awareness to enable real-time, integrated and operational actions across the federal government.
- Sharing cybersecurity threat, vulnerability, impact and incident information and analysis by and among federal, state and local government agencies, and private-sector entities.
- Conducting analysis of cybersecurity risks and incidents.
- Providing recommendations on security and resilience measures to federal and non-federal entities.

> Three cybersecurity statutes will continue the progress agencies have made in protecting government networks.

Finally, the **DHS Cybersecurity Workforce Recruitment and Retention Act** authorizes actions to enhance the government's pool of talented cybersecurity professionals. It provides additional authorities to the DHS secretary to assist in the recruitment, training, education, development and retention of a highly qualified federal cybersecurity workforce.

The act also requires the secretary to evaluate efforts to improve the department's cybersecurity workforce and submit an annual report to the appropriate committees of Congress detailing DHS' progress.

DHS' Continuous Diagnostics and Mitigation program is a prime example of the government's efforts to operationalize cybersecurity protection in a way that reinforces the provisions of these three important statutes. Implementation of this and similar programs — as reinforced by the new laws — will continue to strengthen the way federal agencies protect their networks, systems and data from ever-evolving threats in cyberspace.

The government's efforts to build a more effective cybersecurity posture are evident in the implementation of these three bills. By openly collaborating across agencies, coordinating incident response and increasing the pool of cybersecurity professionals, the government will grow its capacity to operate in cyberspace at a rapid rate.

Cohesive implementation of these bills will enable agencies to mitigate cybersecurity risks and proactively plan for vulnerabilities by providing increasingly responsive tactics for addressing cyberthreats. ■

Can the Pentagon keep pace on biometrics?

The Defense Department has launched an improved version of its biometrics repository, but the system still lacks the latest technology

BY SEAN LYNGAAS

The Automated Biometric Identification System handles everything from iris scans of suspected combatants in Afghanistan to visitor screening at select U.S. military bases.

Biometrics are critical to the Defense Department's global intelligence-collection efforts. U.S. soldiers in Afghanistan, for example, take iris scans of field subjects and send the data to a DOD-wide database, where it is checked against a list of suspected terrorists.

Biometrics technology and its applications for security are at a crucial juncture, experts say. The private sector is driving rapid improvements in the algorithms that determine the accuracy and speed of facial and iris scans, while DOD is gradually deploying a biometrics database whose accuracy and cybersecurity need improving, according to a DOD auditor.

For DOD to reap the benefits of this promising field in the coming years, it must address those shortcomings and find a way to use commercial technology to feed information into the database, according to practitioners and observers.

Along those lines, Undersecretary of Defense for Intelligence Michael Vickers recently listed biometrics as among a handful of technological challenges facing DOD and the intelligence community.

Roger Mason, a former senior adviser to the director of national intelligence and a biometrics expert, said that although law enforcement agencies have used fingerprinting for decades, the anonymity that is possible on the Internet has made biometrics intelligence more difficult in recent years.

"The challenge that [Vickers] is referring to is that when you think about the ubiquity that biometrics now plays in all of our lives and combine that with the way that we interact with the Internet in terms of our personas, the challenge of anonymity and the challenge of trying to detect other identities becomes much more difficult," said Mason, who is now a senior vice president at science and technology nonprofit Noblis.

Mobilizing a DOD database

The Army's Program Executive Office for Enterprise Information Systems is in charge of a DOD-wide biometrics database that has been in the works for half a decade. The Automated Biometric Identification System is a central repository for biometrics data from various combatant commands and military services. The system can process as many as 30,000 daily submissions and hold as many as 18 million records, according to PEO EIS.

For example, a soldier on patrol in Afghanistan uses a device known as the Biometrics Automated Toolset to collect biometrics. Its hardware, called the Secure Electronic Enrollment Kit II, automatically captures and formats fingerprints and iris and facial images, and has a keyboard for soldiers to type in biographical information about the subject.

The handheld device connects to a central workstation that links up with any of the several dozen servers across Afghanistan for storing biometrics data. The data is then sent to the ABIS database in West Virginia for correlation. The FBI and the departments of State and Homeland Security, among other agencies, use ABIS to identify biometrics matches for criminal cases and people on intelligence watchlists of suspected terrorists.

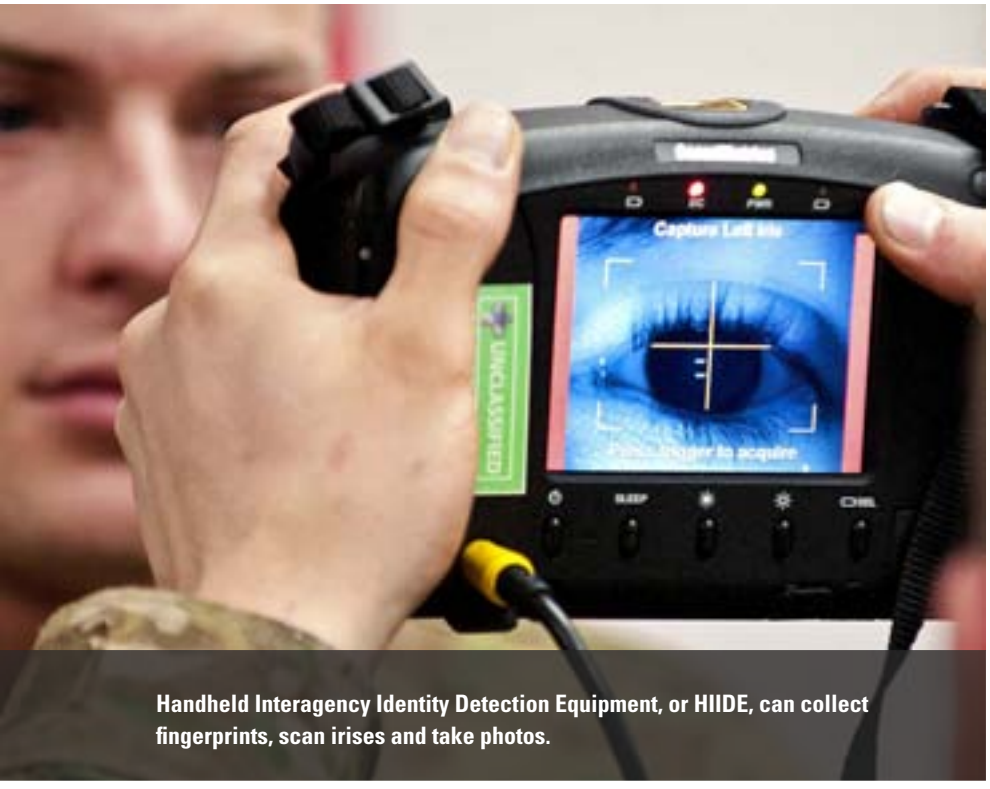
ABIS, in short, is a giant initiative for collecting and sharing data, and its efficacy depends on the quality of the technology on which the system is built.

The Army deployed its latest version (ABIS 1.2) in October 2014. It has demonstrated increased throughput and capacity, and offered an opportunity to refresh the system's hardware, said Col. Sandy Vann-Olejasz, DOD biometrics program manager at PEO EIS. Full deployment of the system will occur no later than the first quarter of fiscal 2016, she added.

The Army launched the initial version of ABIS (1.0) in January 2009, and DOD issued acquisition guidelines for ABIS 1.2 in January 2011, but the system was not deployed until three and half years later. Along the way, there were at least four failed attempts to deploy ABIS 1.2, according to a fiscal 2013 review by DOD's director of operational test and evaluation (OT&E).

In one botched attempt, the two versions of the database failed to operate in tandem.

Vann-Olejasz said ABIS 1.2 overcame an important hurdle by requiring less manual labor to get a positive



Handheld Interagency Identity Detection Equipment, or HIIDE, can collect fingerprints, scan irises and take photos.

identification on biometrics samples than a previous version of the repository. ABIS filters biometrics samples as either an automated match or not. Anything in between must be scrutinized by a biometrics examiner, a process Vann-Olejasz said was slow and laborious.

Better algorithms explain ABIS 1.2's improved accuracy, which in turn gives the Army's experts more time to analyze the sample matches and incorporate them into intelligence reports. But there is still plenty of room for improvement. OT&E's fiscal 2014 review of ABIS said the database had significant cybersecurity vulnerabilities, and ABIS 1.0 and 1.2 were not fully consistent in matching individuals to a watchlist of suspected terrorists.

The private sector and nonprofit research and development organizations, meanwhile, are trying to meet DOD's demand for faster and more accurate processing of biometrics data. Mason said he has challenged his colleagues to develop algorithms that can accurately process 1 billion facial scans per second, a goal he expects his researchers to hit by the end of this year.

Although iris scans are considered the most accurate of the three main categories of biometrics, their intrusiveness and relatively high cost have slowed adoption, said Mark Clifton, vice president of the Products and Services Division at SRI International, an R&D nonprofit. He added that the U.S. military is using SRI's technology to scan the irises, faces and fingerprints of entrants to military bases but declined to specify which bases are using the technology or the quantity of products sold.

Another challenge is to develop iris scanning that can be done more remotely. Clifton said his organization has recently demonstrated iris-scanning capabilities from more than 30 yards with a stationary subject, but "unfortunately, it took nearly telescope-size optics to get that, so it's not that practical." The Pentagon is still a few years away from deploying any sort of midrange iris-scanning technology, he added.

The ABIS requirements do not call for remote iris or facial scanning, Vann-Olejasz said, but that could change with an ongoing Army-run "analysis of alternatives" review of acquisition options for biometrics. The review will help the Army determine "the next capability gap that we need to close with this technology," she said, adding that the review should be finished by year's end.

Speed vs. accuracy

Much of the ABIS software and hardware is commercial rather than custom-built for the military, Vann-Olejasz said. Of the algorithms being honed by industry, those underpinning iris and facial scans have seen the most improvement recently, whereas fingerprint algorithms have hit a plateau of sorts, she added.

Mason said the key for defense and intelligence officials will be to better integrate the three nodes of data — iris, fingerprint and facial imaging — to develop a more composite "pattern of life" profile of a person.

There is also a trade-off between speed and accuracy when it comes to processing facial images. The industry products that will be "the most valuable to the [intelligence community] in the future are the ones that are going to be able to push the axis on" speed and accuracy, he said.

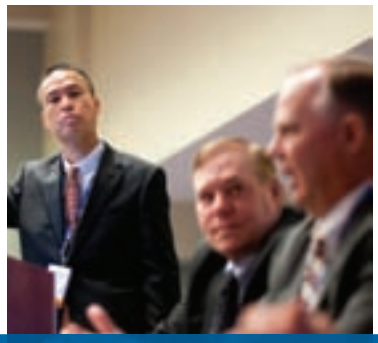
As with many IT advances, the next step might be a move to mobile devices. Clifton said that in the medium term he expects iris scanning to be commercially available on mobile devices for identity verification.

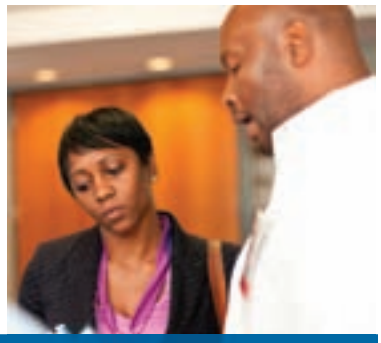
As for ABIS, its underlying technology will inevitably need updating. The current version "will only take us so far due to software obsolescence and potentially hardware things," Vann-Olejasz said. The ongoing review of acquisition strategy for ABIS will determine whether a new approach is needed or "whether or not we will continue to, if you will, bolt on to the DOD ABIS architecture and framework," she added. ■

INAUGURAL 2015

ENTERPRISE ARCHITECTURE WEST

SPECIAL GOVERNMENT PRICING ENDS SOON





EA EDUCATION NOW ON THE WEST COAST!

WORKSHOPS: APRIL 20
CONFERENCE: APRIL 21
SACRAMENTO, CA
CITIZEN HOTEL

At Enterprise Architecture West, enterprise architects, project managers and industry experts will convene to discuss contemporary EA and how to apply it to make the mission possible.

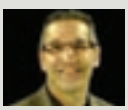
Trending topics impacting the EA community to be discussed include:

- Increasing efficiencies and fostering innovation by using cutting-edge EA methodologies
- Using enterprise architecture as a medium for restructuring

TUESDAY KEYNOTE DETAILS

Enterprise Architecture: 30 Years Young – Moving from the Age of Compliance to the Age of Outcomes

John A. Zachman
Chairman, Zachman International and Executive Director, FEAC Institute



Carl E. Engel
Chief Strategy Officer, Zachman International

Covering:

- How integrating framework approaches will yield better results.
- EA's current compliance mindset and how to give greater emphasis to its outcome-yielding role.
- And more!

Don't Miss This Inaugural Event — **Register NOW** for Best Savings!

govEAconference.com/west
USE PRIORITY CODE: EAW15

PRESENTING PARTNERS
FEAC Institute · Zachman International Enterprise Architecture

SPONSORS
PHASEONE · PrinterLogic

PARTNERING MEDIA
Defense Systems · FCW · GCN · Washington Technology · OMG

PRODUCED BY Public Sector Events Group

ENDURING SECURITY

Content Management & Analysis

Network & Information Security

Mission Operations

Critical Infrastructure & Borders


www.boeing.com/security
UNITED STATES & CANADA
ALL CLEAR
Internal Corporate Server 1
Gateway
BOEING

Consolidation, culture and one very big co

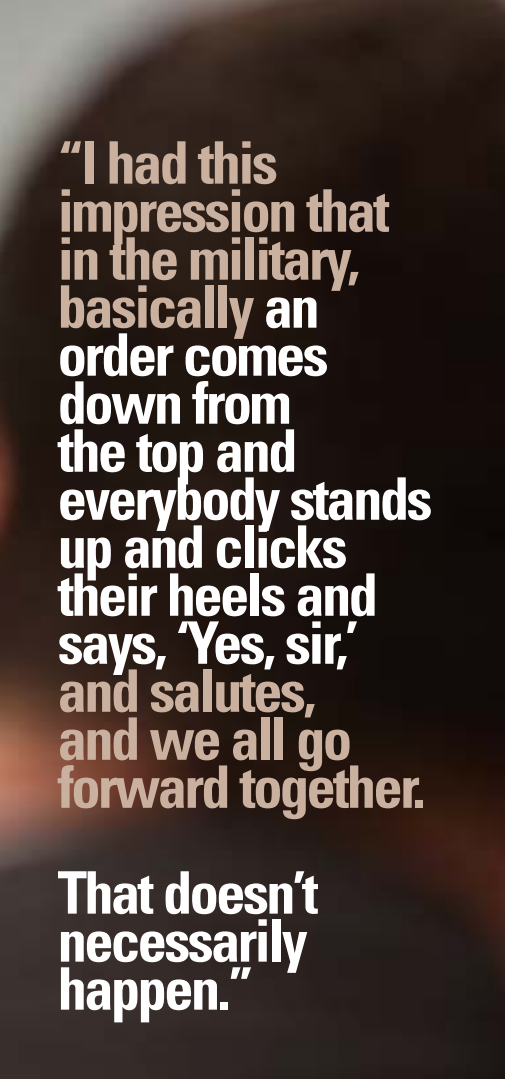
David Bowen, the Defense Health Agency's director of health IT, has a seriously complex to-do list

BY ADAM MAZMANIAN

Defense Department officials will make a decision in the summer or fall of this year to award the coveted $11 billion electronic health record contract to a team of vendors. The acquisition, called the DOD Healthcare Management System Modernization (DHMSM), is one of the most closely watched in government and industry. It is being run by a special office that reports to the undersecretary of Defense for acquisition, technology and logistics, and it has attracted bids from diverse, integrated teams across industry.

Once an award is made and the initial deployment completed, it will be up to the Defense Health Agency to make it work. And that puts serious responsibilities squarely on the shoulders of David Bowen.

Bowen is director of health IT at DHA, which is a relatively new entrant in the military's alphabet soup of acronyms. It launched Oct. 1, 2013 — the same day HealthCare.gov opened for business — with the mission of



ontract

transforming the way the military delivers health care by operating 10 shared services across the Military Health System (MHS). A medium-sized operation by military standards, DHA has a $219 million budget for fiscal 2015 and $186 million requested for next year. It is headquartered in a low-slung office building just inside the Capitol Beltway in the Virginia suburb of Falls Church.

"Our job is to have the infrastructure in place and operational at the facilities so that the electronic health record people can come in and install the electronic health record and a platform," Bowen told FCW.

The EHR system is not just a big piece of software and a data repository. For service members wounded in combat, it is a vital link for caregivers. It will serve a population of 9.5 million beneficiaries at almost 700 military treatment facilities and 380,000 Tricare providers, and it will have to operate consistently on a variety of computers, including PCs in stateside hospitals and mobile devices in combat zones.

"One of our goals is to get the electrons to the doctors before the patient arrives," DHA Director Lt. Gen. Douglas Robb told FCW. "While the patient is in transit or still on the battlefield, the health care team can prepare for their arrival and treatment."

He added that Bowen and his team are working to make sure military health care providers can collect and transmit medical information to battlefield care facilities in theater and to hospitals back home.

"The ability to transmit this critical data often means the difference between life and death," Robb said.

Anthropology, not technology

The business case for the new agency is consolidation. Some of that activity supports the arrival of the new EHR system, but the agency is also consolidating management, contracts, business processes, infrastructure and applications. Complicating matters is the fact that the work is being done across the military services. The Army, Navy and Air Force have all retained their medical structures and hierarchies, which now operate within MHS.

"When you start putting the services together, these differences in processes, procedures, customs really start coming out and becoming a factor," Bowen said. "Things like performance management systems, how the services rate their officers, the way they fund their operations, the way they run technology — there are big differences there that we had to and still have to overcome. Quite frankly, it's been a challenge. I tell people...that my job is not around technology, it's around anthropology."

In addition to being director of health IT at DHA, Bowen is CIO of MHS, although he describes his job as serving a single mission rather than wearing two hats. He did not serve in uniform, and his previous stint in government was as CIO of the Federal Aviation Administration. He is a trained commercial pilot and a flying enthusiast, but his professional background is in health IT. He's been the CIO of hospital systems and a Blue Cross Blue Shield plan.

"I know health care really well, both from the provider standpoint and from the health plan standpoint, having run IT operations in both of those environments," he said.

When it comes to managing organizational change, Bowen added that there are more similarities between DOD and the commercial world than he would have thought.

"I had this impression that in the military, basically an order comes down from the top and everybody stands up and clicks their heels and says, 'Yes, sir,' and salutes, and we all go forward together," he said. "That doesn't necessarily happen. We do a lot more consensus building in the military than I thought we would, frankly."

PHOTOS BY DAVID WIEGOLD

One consolidation now underway involves centralizing computer network operations for medical facilities. The Army and Navy use DHA networks while the Air Force maintains its own structure. That is a manifestation of a larger cultural difference, Bowen said.

"The Air Force is a lot more decentralized, and the base commanders have a lot more leeway," he said. "You've got more centralized, standardized management in the Army and in the Navy. [Eventually,] we're going to end up pulling the Air Force facilities off the Air Force network and consolidate them on our medical network."

Infrastructure consolidation is a big part of DHA's work in fiscal 2015. The agency just finished moving MHS to the email system operated by the Defense Information Systems Agency. Bowen and his colleagues are also consolidating multiple help desks into a single global service center.

So far, the consolidation is saving money: In fiscal 2014, DHA reported net savings of $236 million, with health IT contributing $39.19 million in savings.

"In many areas, you have three chunks of infrastructure [and] three sets of applications, and so our job is to bring a lot of this together and drive operating efficiencies and dollars out of the operation," he said.

EHRs and the cloud

The EHR project intersects with one of the Pentagon's most high-profile IT initiatives. It will operate on the Joint Information Environment (JIE) network, which is still a work in progress and will offer "end-to-end information sharing and interdependent enterprise services across the department that are seamless, interoperable, efficient, and responsive to joint and coalition warfighter requirements," according to budget documents.

"We're the tip of the spear for JIE now because we've got some pretty near-term objectives we've got to achieve," Bowen said. "We're working with [DOD CIO Terry] Halvorsen's office to make that happen."

However, there are some question marks when it comes to data centers and cloud services. DHA will be bound by DOD cloud policy, still under development, when evaluating proposed enterprise hosting strategies for DHMSM. But the contract doesn't include enterprisewide or Tier 1 hosting services for DOD data centers and approved commercial hosting facilities. Instead, the contractor is responsible for proposing a network and infrastructure solution that corresponds to the requirements outlined in the solicitation.

The government plans to procure enterprisewide services separately, "based on the footprint proposed by the DHMSM contractor," a Pentagon spokesperson told FCW. "The government anticipates that proposed system architectures may range from a centrally hosted to a regionally deployed solution based on the proposed EHR system's ability to scale functionally, geographically and administratively."

That gives DOD time to refine its still evolving cloud strategy in the event that the EHR system involves commercial cloud providers. But on the ground, where the records are being used, DHA is standardizing the technology.

"We're going to be looking at basically managing what we call 'data center to desktop,'" Bowen said. "This is new for us. This is something we haven't done in the past. The facilities have been allowed to manage their own medical infrastructure however they so choose."

The EHR system will undergo a testing period in military health centers in the Pacific Northwest in 2016 before opening up to the entire military. "We've had teams out there the last couple weeks looking at the infrastructure," Bowen said. "We had a symposium on that and the findings last week. Our near-term objective is to have that infrastructure in place and operational [in the Pacific Northwest] by the end of calendar year 2015."

By government standards, the DHMSM procurement appears to be on schedule. Bowen credits the integration of the teams that are sharing in implementation. There are monthly progress meetings with Undersecretary of Defense Frank Kendall, the project managers, DHA officials and the surgeons general of the military services.

"Obviously, it's a very visible project. It's a very expensive project," Bowen said. "I think it's a credit to our organization and the fact that DOD does have a lot of these project management skills that they can bring to the table. You may have a contracting glitch or something like that, but given all the resources that we've got on here, we're still running the way we should be running." ■

Visual Studio LIVE!

EXPERT SOLUTIONS FOR .NET DEVELOPERS

vslive.com/lasvegas

Las Vegas MARCH 16 - 20

BALLY'S HOTEL & CASINO LAS VEGAS, NV

LAS VEGAS Code Trip

NAVIGATE THE .NET HIGHWAY

Code on the Strip

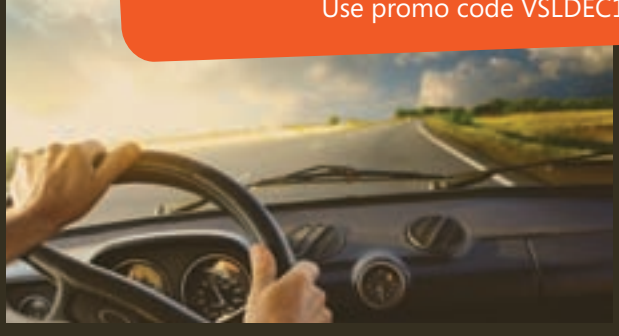
Visual Studio Live!'s first stop on its 2015 Code Trip is Las Vegas, situated fittingly near Historic Route 66. Developers, software architects, engineers, and designers will cruise onto the Strip for five days of unbiased and cutting-edge education on the Microsoft Platform. Navigate the .NET Highway with industry experts and Microsoft insiders in 60+ sessions and fun networking events – all designed to make you better at your job.

TRACKS INCLUDE:

- Visual Studio / .NET
- JavaScript/HTML5
- ASP.NET
- Cross-Platform Mobile Development
- Windows 8.1/WinRT
- Database and Analytics
- Cloud Computing
- Windows Phone

Register NOW and Save $500!

Use promo code VSLDEC1



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

SUPPORTED BY

Microsoft Visual Studio msdn magazine Visual Studio MAGAZINE

PRODUCED BY

1105 MEDIA

vslive.com/lasvegas

SEWP: An acquisition pioneer is still going strong

Protests have delayed SEWP V, but industry experts say the contract vehicle offers agencies service and value that are hard to find

BY MARK ROCKWELL

What do NASA's Solutions for Enterprisewide Procurement program and the Mars rovers have in common? More than you might think.

Many recall NASA's Spirit and Opportunity rovers, which launched in 2003 with a tightly focused, 90-day mission yet continued to explore the red planet for years. The agency's SEWP contract is far less famous, but it too was launched with a smaller, more focused job in mind — and that was more than 20 years ago.

The multiple-award, indefinite-delivery, indefinite-quantity (IDIQ) governmentwide acquisition contract (GWAC) has been a pioneer in its own right and has proven durable and effective well beyond its initial expiration date.

The program was authorized in 1993 by the Office of Management and Budget to help the agency buy computers more effectively. The acronym originally stood for Scientific and Engineering Workstation Procurement, and the contract provided technical and engineering-related IT products but not associated services. The acronym changed to its current form in 2007 after computer technology blossomed and firm-fixed-price services became available.

SEWP is now in its fifth iteration. Under the contract vehicle, all federal agencies can buy IT products, including tablet and desktop computers, servers, peripheral devices, network equipment, storage systems, security tools, software, cloud-based services and videoconferencing systems. They can also get training, maintenance and installation services.

Even after 22 years, analysts say, SEWP still matters to federal IT buyers because it fills a critical need. Agencies have access to a reliable source of a wide range of products gathered in one place where they can pick and choose what they want, and it's all backed by scrupulous customer service.

SEWP timeline

SEWP I (February 1993–February 1997)

- Emphasized Unix systems to replace proprietary VAX and IBM systems
- $800 million, four-year delegation of procurement authority (DPA)
- No small-business or 8(a) awards

SEWP II (November 1996–July 2001)

- Included higher-end systems and administrative IT classes
- $1.8 billion, four-year DPA as GWAC
- Two small-business set-asides and five 8(a) awards

SEWP III (July 2001–April 2007)

- Increased Web and database enhancements
- $4 billion, five-year term
- Three small-business set-aside competitions (with two awarded to seven companies) and three 8(a) noncompeted set-asides

"SEWP is the leader in the GWAC space," said Erica McCann, director of federal procurement at the Information Technology Industry Council's IT Alliance for the Public Sector. SEWP's top management "has a refreshingly nongovernmental take" on IT acquisition, she added, and instead of acting like a large federal bureaucracy, SEWP behaves more like a small business that is determined to get and keep its customers' business, making it a standout for federal users.

SEWP Program Manager Joanne Woytek said other GWACs, such as the General Services Administration's Alliant and the National Institutes of Health IT Acquisition and Assessment Center's contracts, tend to be more services-oriented.

Nevertheless, SEWP does have some overlap with the other GWACs, and all the programs share a common goal of reducing the thousands of agency-specific contracts that can bog down federal operations.

"All three agencies are more concerned with the continued proliferation of non-GWAC contracts and the even larger use of open market purchasing than about GWAC competition," Woytek said. "We each have our own strengths and provide the government with a well-established set of options that agencies can select from based on their particular needs."

Because it behaves more like a small business that is determined to get and keep its customers' business, "SEWP is the leader in the GWAC space."

ERICA McCANN, IT INDUSTRY COUNCIL

A contentious market

After two decades of successful service, however, SEWP faces some challenges as the federal IT market and the federal acquisition world change dramatically.

"The key challenge is the introduction of the SEWP V contracts," Woytek said. "We will more than double in size in terms of number of contracts." SEWP V will have more competition, important contract-tracking options and other improvements, but the agency will have to retool its internal processes to manage the new contracts, she added.

Alan Chvotkin, executive vice president and counsel at the Professional Services Council, said that as the SEWP V contracts take shape, vendors are feeling the effects of agencies' budget constraints. Because agencies have less money to spend, it is imperative for technology resellers and manufacturers to be included in large GWACs and other IDIQ contracts so they can show off their wares in as many places as possible. That's not easy or inexpensive, he added.

Partly as a result of those pressures, bid protests have become a significant part of the federal acquisition process,

SEWP IV (May 2007–April 2015)

- Expanded into Linux and security
- $17 billion in sales
- One small-business set-aside competition, resulting in 14 awardees
- One set-aside competition for small businesses owned by service-disabled veterans, resulting in six awardees
- Two full and open competitions, resulting in 25 awardees

SEWP V (May 2015–April 2025)

- Increased focus on cloud- and product-based services
- $30 billion, 10-year term anticipated
- One small-business set-aside competition
- One set-aside competition for small businesses owned by service-disabled veterans
- One set-aside competition for companies in Historically Underutilized Business Zones
- Two full and open competitions
- Awards scheduled to be announced in early April (as of Feb. 8)

Source: NASA

Chvotkin said. "The larger the opportunity, the greater value to the incumbent" providers — and the harder they fight.

That pressure was evident in November when NASA decided to re-evaluate dozens of contracts it had awarded under SEWP V in response to protests. On Oct. 1 and Oct. 15, NASA had approved 73 contracts for hardware, software and related services in three categories based on company size. Protests started almost as soon as the contracts were announced, with 17 firms filing in various categories.

As a result, the agency extended SEWP IV until April as it works through the SEWP V protests. NASA officials have also made some efficiency improvements to SEWP IV operations and lowered the fee built into product prices from 0.45 percent to 0.39 percent.

SEWP's situation isn't unique in the current contentious market, McCann said. Companies "are scrapping about where they are" on federal contracting vehicles overall.

Woytek said GWACs are no more susceptible to protests than any other federal contract, and Chvotkin agreed that there's no reason to expect SEWP V to be hit by more protests. Ultimately, "it's up to the agencies to get [contracting vehicles] right," he said, adding that SEWP V might have an advantage because its creators included vendors in the development process.

The impact of strategic sourcing

Another potential hurdle for SEWP is the growing influence of GSA's efforts at strategic sourcing, which include detailed, price-oriented category management. GSA has been steadily building detailed product "hallways" where federal IT buyers can find details about specific applications, products and, perhaps most important, prices other agencies paid for the same or similar equipment and services.

GSA officials hope to bolster the agency's standing as the default source for federal IT managers looking for solutions. The agency also has its own GWAC and the Schedule 70 IDIQ, which is the most widely used acquisition vehicle in the federal government.

GSA's efforts to build information on product categories do not necessarily come at the expense of other GWACs because GSA officials have said they want to include information on all federal GWACs.

In fact, McCann and Chvotkin said GSA's efforts will probably aid SEWP. "Category management hallways will bring more visibility to a host of IDIQ GWACs, including SEWP," Chvotkin said.

He and McCann agreed that SEWP will almost certainly endure. The GWAC continues to respond to the marketplace and federal users' demands, McCann said, and Woytek "knows how to adapt to changing needs."

McCann also credited Woytek with creating a culture of scrupulous customer service that has built a loyal following among federal buyers. "That's something you don't see in government every day," she said. ■

SEWP IV facts

BY THE NUMBERS:

37
contract holders

4,700
companies with products and/or services on one or more contracts

2.7 million
unique products

At least 97
distinct agency customers, including all Cabinet-level departments, commissions and independent agencies

TOTAL BUYING UNDER SEWP:

$2.35 billion
Fiscal 2013

$2.52 billion
Fiscal 2014

WHAT'S IN A NAME?

The acronym soon came to be associated with the saying "as easy as duck soup." The Marx Brothers' movie "Duck Soup" also became linked to the effort, which makes SEWP's cartoon rubber ducky logo a little more understandable.

FCW

THE BUSINESS OF FEDERAL TECHNOLOGY

Everywhere you want us to be.

Mobile

Tablet

Desktop

Print

Drawing back the curtain on cyberwar

Shane Harris' book "@War" details the personalities and turf battles behind the government's conclusion that cyberspace is a national security asset

BY SEAN LYNGAAS

Journalist Shane Harris has written a richly detailed, page-turning recent history of the militarization of cyberspace. The combination of thoroughness and accessibility makes "@War: The Rise of the Military-Internet Complex" an important contribution to the ever-changing, seemingly unfathomable field of cybersecurity.

Harris offers an inside account of how, over the course of more than a decade, U.S. military, intelligence and civilian agencies have ramped up their cyber capabilities to try to stay ahead of threats posed by criminal hackers and nation states. But the book does more than chronicle that transformation. It also picks up on the personalities and bureaucratic turf battles behind it and reflects on the broader implications for the security and openness of the Internet.

The book's subtitle is a variant of President Dwight Eisenhower's warning against the potentially outsize influence of industry on U.S. defense policy. The military-Internet complex treats the Web as a battlefield, writes Harris, a senior correspondent at The Daily Beast. That battlefield is full of government and corporate secrets, and it has spawned a lucrative market for protecting them.

FCW readers will appreciate the book's detailing of the interagency tensions that come with grappling with a new domain. The 2009 birth of U.S. Cyber Command under the leadership of the National Security Agency director gave NSA even more clout among agencies in cyberspace. But Jane Holl Lute, who became deputy secretary of the Department of Homeland Security that year, challenged the notion that NSA was uniquely suited to defend civilian cyberspace, Harris writes.

"Pretend the Manhattan phone book is the universe of malware," she is quoted as telling colleagues. "NSA only has about one page of the book."

That turf battle is likely far from settled, and DHS has continued to expand its own cyber-defense capabilities.

Cyberwarfare is not a new

concept, but it is a fairly new practice. One of the pivotal moments came in 2007, during the surge of U.S. forces in Iraq, according to Harris. He profiles Bob Stasio, then an Army lieutenant whose signals-intelligence platoon is credited with tracking down hundreds of insurgents. He used cell phone signals to determine insurgents' locations and sent reports back to commanders to correlate the data with a wider view of the battlefield.

Stasio's handiwork was made possible by President George W. Bush's decision to unleash NSA's cyber capabilities, Harris writes. In a May 2007 meeting with then-Director of National Intelligence Mike McConnell, Bush signed off on NSA's use of computer viruses and spyware to penetrate the communication networks of Iraqi insurgents.

That cyber arsenal helped quell the Iraqi insurgency at the time, but it was not without hazards. Collateral damage is as real a possibility in cyberspace as in other types of warfare, and the malware risked infecting the devices of innocent Iraqis and spreading further.

The U.S. military's surge in Iraq allowed NSA to use cyber weapons it had been stockpiling for years, Harris writes, and he describes how NSA buys them from defense contractors that acquire them from third-party vendors. The hoarding of cyber weapons bolsters U.S. offensive capabilities but leaves Internet users in the dark about software and hardware flaws that then remain unpatched.

Harris also details other turning points in federal cybersecurity policy, including Operation Buckshot Yankee, the Pentagon's response to a 2008 breach of its classified systems. One of the most important lines in "@War," however, comes in its preface and is informed by the dogged reporting that gives the book such value. Pushing back against the tendency of government officials to decline to discuss cybersecurity because it pertains to "classified" information, Harris writes, "The public cannot understand these issues, and governments can't make sound law and policy, without candid and frank discussions in the light of day."

Shane Harris

"The public cannot understand these issues, and governments can't make sound law and policy, without candid and frank discussions in the light of day."

If every journalist covering cybersecurity had those words hanging above his or her desk, cyberspace would be less murky. "@War" does use extensive anonymous — along with many on-the-record — sources, but Harris explains his criteria for offering anonymity while noting the considerable risk that intelligence sources take in talking to journalists.

The refrain from government officials that classified information gives them a unique ability and privilege to combat cyberthreats needs to be evaluated against public evidence. Harris makes this point by recounting a 2009 meeting between federal officials and security personnel from some of the top U.S. banks. When an FBI official asked how a program to share cyberthreat information between the government and the financial industry was progressing, a bank representative expressed disappointment, Harris writes.

The report the FBI had shared with the banks had drawn on classified information and included threat-signature details, but the banks had already obtained that information by sharing it with one another or buying it from private security firms.

That meeting illustrates a theme that courses through Harris' book: There is no hegemon in cyberspace. The Tor network, a routing tool originally funded by the U.S. government, has thwarted NSA's efforts to identify Internet users. Chinese hackers have dealt costly blows to Internet leviathans such as Google. Cyberspace is as contested as ever. And that's what makes this account of its militarization so important. ■

How open source delivers for government

The real story in IT innovation is open-source software, and it might just be the mega-trend in technology for this century

BY STEPHEN FROST

Amid the well-deserved hype about the impact of cloud technology and big-data analytics, casual industry watchers might have missed the real story behind the recent wave of IT re-architecting.

Enabling many of these recent, powerful trends is a newly validated embrace of open-source software technology. The movement to OSS solutions is empowering system designers and solution architects to re-examine methodologies that evolved out of the legacy proprietary, closed-source software license model. Simply put, OSS allows developers of IT systems to create better results and cut costs.

Enterprise IT leaders in business and government have taken notice of the benefits of OSS. For example, the recently launched U.S. Digital Service published a Digital Services Playbook that urges agencies to "consider open-source software solutions at all layers of the stack." The General Services Administration extended that thinking in the recently introduced "open source first" policy as part of its effort to modernize its organization, processes and technologies.

Defense policy-makers have gone further, directing those within the Defense Department to identify barriers to the effective use of OSS within DOD so that the military can continue to increase those benefits.

More flexibility

One of the key drivers of OSS adoption has been cost. But although the savings can be dramatic, cost reduction is not the whole story. OSS also creates the possibility of more reliable, more trustable, more functionally appropriate and just plain better solutions.

Historically, companies needed to factor in the cost of closed-source software at peak license distribution even if they routinely needed a smaller number of licenses. On top of that were support fees tied to the peak distribution. Therefore, solution designers had an incentive to constrain distribution of software even if the use case was under-served.

That is clearly not the case in an open-source world. Both the solution architect and budget manager only need to consider the support costs, not the licensing costs, and vendor support is generally more cost-effective than internal capability. In the case of a distributed database solution, the difference in cost can really add up.

A simple example of how the move to OSS can improve IT architecture is with regard to database backups. In the legacy regime of closed-source software, each license of an incremental database came with a cost — often a steep one. In the world of OSS, enterprise users can maintain replicas of databases as backups with no incremental license cost.

The more copies of the database software you have, the more options you have when things go wrong. The more copies of the data management or analytics software you have, the more choices you have to efficiently move your data around.

Security and reliability

Cost alone can carry the day for some projects, but security and dependability are the main drivers for many mission-critical needs.

Here, too, open source is a great alternative to closed source. Contrary to a common myth of OSS, most of the development and support is performed by dedicated, highly trained professionals who are on par with the development shops of any of the top tech firms. In fact, many of the best OSS projects have the support of leading commercial enterprises such as Red Hat, Google and Salesforce.com.

Still, OSS must pass the close

testing and rigorous examination of many interested parties. Researchers and scientists of all types are familiar with the withering gaze but necessary value of peer review, which involves open and independent examination by many experts. With OSS, users in business, government and academia and even hobbyists get to look at and make judgments about OSS, and users are the ultimate beneficiaries.

Walmart's Eran Hammer, senior architect for the Node platform, echoes that idea and said Walmart enjoys a "significant quality and stability boost" from the efforts of early OSS adopters.

Even some leaders in the national security community are taking advantage of open source and crowdsourcing. For example, the National Geospatial-Intelligence Agency uses OSS to help it develop apps for geospatial analysts.

"While there are some security concerns, I believe the way we deployed this architecture really addresses those security concerns," said Dave White, NGA's CIO. "The risk is very manageable, but what we are getting in return is innovation, and it's really advancing our mission."

Of course, no matter how well-trained the solution developers are and no matter how carefully scrutinized the solution is, users might discover vulnerabilities in software — whether it was developed under the closed or open model. If those vulnerabilities are in proprietary software, "the only people who can identify and fix the problem are employed by the company that wrote it," said Gunnar Hellekson, chief strategist for Red Hat's U.S. Public Sector Group. "They can be smart, they can be well-trained and highly skilled and use only the best of the best practices of software development, and they still couldn't muster the number of eyeballs commanded by a high-functioning open-source community."

Healthy open-source software projects are subject to constant, ongoing examination and communication among many invested parties, and that openness benefits all users.

In contrast, an enterprise that is supported by an expert in-house team backed by an active, well-functioning open-source community will be well served by the number and diversity of solution seekers.

By the same logic, it is more difficult to hide vulnerabilities in open-source code because the source is readily available. That means no party can build in a back door or other security exposure without the prospect of peer review and user examination ringing an alert for all users to see.

Users of closed-source products know that they are entirely reliant on the ongoing commitment of the developer and have limited control over some of the risks involved. Independent testing methodologies and certifications can help, but they are only valid for the exact code certified — not for the next version or the next patch and certainly not for the advanced features acquired separately.

Healthy OSS projects are subject to constant, ongoing examination and communication among many invested parties, and that openness benefits all users.

Growing market support

The road to broad adoption of OSS has had a few speed bumps and potholes, but it has followed a well-established adoption curve, complicated perhaps by the mix of technologies involved in its distribution. Nonetheless, OSS' journey has been characterized by early adopters who were both tech-savvy and confident that they could respond to any difficulties. That is a proven strategy for testing new ideas.

As early adopters give way to the early majority, the market is recognizing the need for professional support options to supplement its skills base and permit more scaled deployment. Enterprise support from qualified providers is the leading value multiplier for OSS adopters. Fortunately, a growing community of support companies, staffed by experienced IT leaders, is providing first-rate services.

OpenStack, Hadoop, Linux, PostgreSQL and many other open-source projects are creating new and innovative ways to serve business and government.

OSS saves IT users billions of dollars every year, frees resources for other purposes and delivers better outcomes. Could OSS be the megatrend in technology for this century? ■

Stephen Frost is chief technology officer at Crunchy Data Solutions.

GAO brings the hammer down on IT acquisition

By putting the government's management of IT acquisitions and operations on the High Risk List, GAO has ensured it will finally get the attention it deserves

BY RICHARD A. SPIRES

The Government Accountability Office finally did it. "Improving the Management of IT Acquisitions and Operations" is now on the High Risk List, and GAO's latest report states that "federal IT investments too frequently fail to be completed or incur cost overruns and schedule slippages while contributing little to mission-related outcomes."

For those of us who were involved with items on the High Risk List, this is a significant development.

During my government career, I dealt extensively with two items on the list: IRS modernization (now off the list) and the need to strengthen the Department of Homeland Security's management functions. In both cases, there was intense congressional scrutiny, and significant attention shown by the Office of Management and Budget and the agencies that found their programs on the High Risk List.

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.

Although agencies always grouse about it, I have found that having a program on the High Risk List focuses valuable attention and resources on systemic problems. One of the reasons for the grousing is that once a program is on the High Risk list, it is quite difficult to remove it. The IRS spent more than a decade maturing its acquisition and program management, and along the way demonstrated improved capabilities to deliver successful programs, before finally coming off the list in 2014.

And IT acquisition deserves that level of sustained attention. Deeply embedded cultural and skills issues must be addressed if we are to improve the government's score card in delivering IT programs. Those changes, while certainly doable, take sustained leadership over time to have a major positive impact.

In reviewing GAO's report, I was pleased to see that auditors documented a set of concrete evaluation criteria:

- OMB and agencies should, within four years, implement at least 80 percent of GAO's recommendations related to the management of IT acquisitions and operations.
- Agencies should ensure that a minimum of 80 percent of the government's major acquisitions deliver functionality every 12 months.
- Agencies should achieve no less than 80 percent of the more than $6 billion in planned PortfolioStat savings, and 80 percent of the more than $5 billion in savings expected from data center consolidation.

Those are high bars, but GAO is not asking for perfection. And the targets are specific enough that an administration could drive action in each of the areas, set measurements and objectives by year, and track progress. The implied four-year time frame is aggressive but not impossible.

I do not know our new federal CIO, Tony Scott. Having come to the government from the private sector myself, I admire him for wanting to step into government and help. Yet I know how daunting the learning curve is — core technologies and human nature might be the same, but there are significant differences between government and the private sector.

My advice to Scott is simple: Start by focusing on the proper implementation of the Federal IT Acquisition Reform Act to strengthen CIOs' authorities. If we have weak IT organizations, IT management will not improve. I also recommend focusing on addressing the three evaluation criteria listed above to set the foundation for removing federal IT acquisition from the High Risk List.

Success will likely not be realized for years beyond Scott's tenure. But he has a chance, even so late in this administration, to make a difference. ■

FCW Index

People

Agencies/Organizations

Advertisers

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

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

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

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

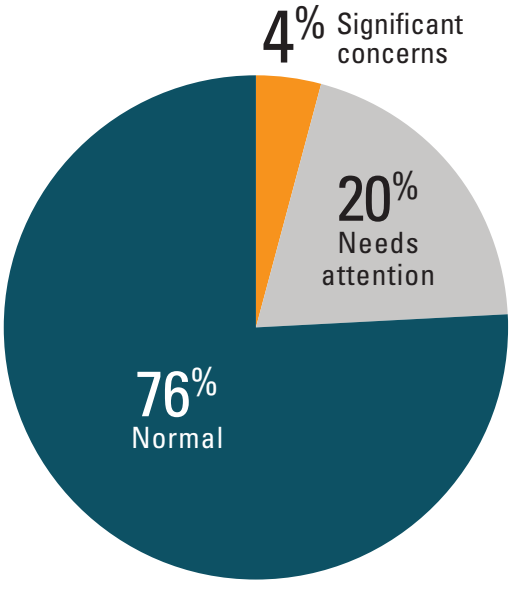
High risk, by the numbers

Improving the management of IT acquisitions and operations was added to the Government Accountability Office's 2015 High Risk List. Here's why — and what to watch for next.

730+ recommendations have been made by GAO regarding IT management in the past five years.

23% have been fully implemented.

183 of agencies' 759 major IT investments were flagged as needing management attention, with 34 of them prompting serious concerns:

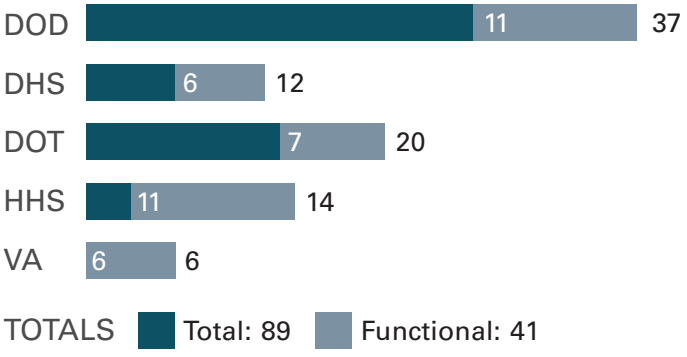


34 investments
($1.5 billion)

149 investments
($10.8 billion)

576 investments
($28.7 billion)

Less than half of the IT investments GAO examined were delivering functionality within 12 months:



GAO's magic number for improvement?

80%

of GAO's IT recommendations should be implemented

of major acquisitions should deliver functionality every 12 months

of projected savings from PorfolioStat and data center consolidation should actually be achieved

But don't hold your breath. For the 23 areas that have made it off the High Risk List, it took an average of **nine years** for them to do so. And six of the areas on the list have been there since 1990.

The interoperability to make decisions with complete data

We offer a platform for Strategic Interoperability. Our technology is essential if you want to make breakthroughs in strategic initiatives such as coordinating care, managing population health, and engaging with patient and physician communities.

Add our HealthShare platform to your EMRs. InterSystems HealthShare® will give you the ability to link all your people, processes, and systems – *and* to aggregate, analyze, and share all patient data. With HealthShare, your clinicians and administrators will be able to make decisions based on complete records and insight from real-time analytics.

InterSystems®

InterSystems.com/Ability4CC

Is Your Agency's Data Safe from Mutating Threats?

Over the past few years, malware has rapidly evolved from broader threats to more targeted attacks. To keep pace, your agency needs to move beyond simple antivirus protection. Symantec Endpoint Protection brings enhanced security, blazing performance, and smarter management to provide protection that blocks mutating threats. With over 20 years of experience developing Information Assurance solutions for the Federal Government, Technica Corporation can customize a solution for your agency that is both FISMA compliant and works with your legacy security infrastructure. And as a prime contractor on the DHS CDM-CMaaS BPA, we can help you navigate the often complex government buying process.

To find out more, visit our website: **technicacorp.com/CMaaS**

Symantec™ DHS CDM MaaS BPA Technica®