FCW
THE BUSINESS OF FEDERAL TECHNOLOGY

CONTRACT SPOTLIGHT:

OASIS

PAGE 27

The root causes of IT insecurity

PAGE 31

IT buying trends

PAGE 34

Back to school

How IT professionals can get smarter on everything from acquisition to machine learning

PAGE 14

AUGUST 30, 2015 • VOLUME 29 NUMBER 14

LAUNCH YOUR >

ADVANCED NETWORK

Do you have concerns about your network performance? Are you looking to replace aging equipment, and upgrade your network infrastructure to provide for new services such as VoIP?

Then PCMG's Network Assessment is for you. Our Network Assessment Offering provides:

- A full analysis of current network infrastructure, including identifying systems that are End of Life, End of Sale, End of Support
- Configuration and potential product recommendations to improve operational efficiency
- Specific analysis to incorporate enhanced configuration (VoIP for example)
- Improved understanding of existing infrastructure as well as options for potential consolidation and centralization
- Recommendations based upon risks, costs, and opportunities for improvement

PCMG can provide consulting services in which PCMG will:

- Review of agency goals and objectives, prioritize needs to ensure that the network caters to the services that are critical to agency functions
- Review design(s), including network diagram(s) and documentation reflecting solution performance, scalability, and services support
- Provide a collaborative design with the client to ensure that agency needs are met

PCMG's approach is based on proven methodologies for identifying bottlenecks and configuration concerns, deploying new services, and optimizing network solutions. Our goal is fast deployment to reduce overall costs and help you plan for future growth.

Federal Government Wide Acquisition Contracts
- GSA Contract: GSA-35F-5946H
- NASA SEWP V Contracts: NNG15SC18B and NNG15SC44B
- Netcents-2: FA8732-14-D-0006

PCM-G

1-800-625-5468 | www.pcmg.com

Trending

30% of government IT buyers expect their budgets to increase next year, by an average of 6.2 percent

Cyber sprint laggards explain their results

Some agencies started at zero but rocketed upward during the federal government's sprint to improve two-factor authentication levels. Other agencies started high and stayed there.

And some agencies saw their two-factor authentication levels actually drop.

According to the results of the cybersecurity sprint, the departments of Education, Justice and Energy were three of the biggest losers in terms of two-factor authentication levels.

- Education's total implementation fell from 71 percent in April, before the sprint, to 57 percent in July. For privileged users, the figure dropped from 14 percent to 11 percent; for unprivileged users, it ticked up from 76 to 77 percent.
- Justice's total implementation fell from 36 percent to 31 percent. The implementation level for privileged users shot from 26 percent to 83 percent, but unprivileged implementation dropped 6 percentage points.
- Energy's total implementation plunged from 32 percent to 12 percent. Although privileged user implementation jumped from 8 percent to 13 percent, unprivileged user implementation fell 23 percentage points.

Those figures stand in contrast to most other agencies. Several reached two-factor authentication levels of 100 percent for privileged users, and 14 surpassed U.S. CIO Tony Scott's 75 percent overall target. The Defense Department saw a small drop in overall two-factor authentication, but unlike Education, Justice and Energy, total DOD two-factor authentication levels were above the 75 percent target.

An Energy spokesperson told FCW that "the numbers fail to tell the whole story. The actual number of users using [personal identity verification] multifactor authentication went up during this period, but the drop in percentage reported to [the Office of Management and Budget] was a result of DOE expanding the scope of users held accountable to this standard to capture DOE's entire enterprise, including contractor accounts, laboratories, sites and plants."

An OMB official echoed Energy's assertion that a new understanding of the underlying numbers affected some agencies' performance.

"Every CFO Act agency made progress toward the goals of the 30-day sprint," the OMB official said. "Where some agencies appear to decrease in their implementing strong authentication…agencies may have realized a larger universe of users."

Furthermore, "the sprint allowed OMB and federal agencies to gain a clearer understanding of challenges — from limited resources, institutional challenges, cyber proficiency, and complex legacy networks and systems — facing an agency's ability to enhance its cybersecurity."

An Education Department official offered the same "larger universe" explanation, and said it made progress during the sprint. Justice, on the other hand, said it did not uncover previously uncounted users.

"DOJ has approximately 3,000 privileged and 160,000 general users, of which 83 percent and 30 percent, respectively, are enabled for PIV two-factor authentication," a Justice official said. "While the numbers fluctuated some during the cyber sprint,

Continued on Page 6

FCW CALENDAR

9/2 Acquisition
Washington Technology's Department of Health and Human Services IT Day will dig into specific fiscal 2016 acquisitions at the Food and Drug Administration, Centers for Medicare and Medicaid Services and other HHS components. Falls Church, Va. http://is.gd/WT_HHS_IT

9/23 Defense IT
David DeVries, DOD's deputy CIO, and DISA Director Lt. Gen. Alan Lynn are among the speakers at Defense Systems' discussion of DOD's Joint Information Environment. Arlington, Va. http://defensesystems.com/JIE

9/24 Customer experience
ACT-IAC is hosting a half-day summit on "The CX Journey: Understanding Customers and Engaging Employees" to explore best practices, tactics and tools for better CX design. Washington, D.C. http://is.gd/FCW_cx

Contents

TRENDING

DEPARTMENTS

FCW
THE BUSINESS OF FEDERAL TECHNOLOGY

SALES CONTACT INFORMATION

MEDIA CONSULTANTS

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

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

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

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

EVENT SPONSORSHIP CONSULTANTS

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

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

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

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

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

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

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

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

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

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

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

31% of federal employees are satisfied with their opportunities for advancement

Cyber sprint laggards

Continued from Page 3

the changes were not material, and they were the result of normal staff turnover."

Instead, Justice merely prioritized privileged-user two-factor authentication. "We have made tremendous progress with our general-user community in enforcing two-factor authentication," the official said. "We expect to improve significantly by the fall of 2015."

Some experts argued that fixating on the numbers was simplistic. "Generally speaking, there's too much focus on these numbers and percentages, which can be misleading," said Monzy Merza, chief security evangelist at software firm Splunk. "These problems are a little more complex than [they] might appear."

Merza said every agency is different, and some already had strong security initiatives they could build on for the sprint. Furthermore, two-factor authentication is not a panacea.

The emphasis on beefing up security for privileged users is good, he said, but other considerations, including improving remote-access security, should also take precedence.

Merza noted that the sprint likely revealed deeper issues that agencies can begin to improve. For example, using smartphone apps as a form of authentication is extremely useful but challenging.

"What if your employees don't have smartphones?" Merza asked. "Or what if you work for an agency that doesn't allow smartphones for security reasons?"

However, Merza said, even the lackluster results at Education, Justice and Energy could be the start of real security improvements. It all depends on what those agencies do next.

— Zach Noble

ITAPS recommends vast changes to federal cybersecurity

In the wake of the unprecedented breaches of Office of Personnel Management systems, the Obama administration has turned to industry for ideas for shoring up federal cybersecurity. The Information Technology Industry Council's IT Alliance for Public Sector offered a slew of ideas, including establishing a permanent position that directs cybersecurity activities across the government.

Trey Hodgkins

ITAPS sent its recommendations to Acting OPM Director Beth Cobert, U.S. CIO Tony Scott and White House Cybersecurity Coordinator Michael Daniel on July 30. The advice came from experts at 20 tech firms, including IBM, Microsoft and Oracle.

ITAPS recommends separating the functions of agency chief information security officers from CIOs, enabling CISOs to send their security concerns directly to agency heads and making IT security part of performance reviews for government employees and contractors.

Furthermore, ITAPS said that like the Department of Homeland Security, agencies should use pay incentives to recruit and retain talented cybersecurity professionals.

The recommendations also recognize that the clock is running out on the Obama administration, which has prioritized cybersecurity while responding to a series of large hacks of federal agencies. "In the remaining time for this administration...the government must move boldly with speed, transparency in action, unity of effort and clarity in purpose," ITAPS advised.

Trey Hodgkins, ITAPS' senior vice president for public sector, said in a statement that cybersecurity "can no longer be viewed as an isolated issue. It should be a top priority governmentwide."

— Sean Lyngaas

INK TANK

The Federal IT Acquisition Summit

Exploring Strategies, Options & Innovations

October 20, 2015

Washington Hilton, Washington, DC

EDUCATION & TRAINING FOR KEY CONTRACT VEHICLES

This second event in the Federal IT Acquisition Summit series provides government IT decision makers with contract-specific training opportunities as well as insights on key issues that are reshaping the federal acquisition environment. Featured vehicles include GSA Alliant (including an Alliant 2 update), NASA SEWP V, and NIH CIO-CS.

Free for Government & Military Attendees

Supporting Agencies

SEWP V

NITAAC
OMB Authorized GWACs for IT Acquisition

FCW GCN Washington Technology DEFENSESYSTEMS FederalSOUP

For Sponsorship Opportunities Contact

Alyce Morrison: amorrison@1105media.com or Kharry Wolinsky: kwolinsky@1105media.com

For More Information Visit: http://fcw.com/fias

Trending

4,000 personnel who work for the Joint Chiefs of Staff lost email access for nearly two weeks due to a cyberattack

IGs: Administration stymies access

A long-simmering controversy between the inspector general community and the Obama administration is heating up. At issue is the access IGs have to agency documents.

Justice Department IG Michael Horowitz has been outspoken about a lack of access to certain materials that are needed to conduct oversight of law enforcement agencies such as the FBI and the Drug Enforcement Administration. He said access to those materials has been severely curtailed since 2010.

A recent memo from the Justice Department's Office of Legal Counsel states that the department is justified in withholding or putting conditions on the release of grand jury, credit and wiretap information because competing statutes protect that information.

The department "has grappled with two different, and potentially conflicting, sets of statutory commands" when dealing with IG information requests, Associate Deputy Attorney General Carlos Uriarte said during a Senate Judiciary Committee hearing earlier this month.

Judiciary Committee Chairman Chuck Grassley (R-Iowa) was clearly unhappy with the memo and noted that in the fiscal 2015 bill funding the Justice Department, appropriators "essentially bolded and underlined section 6A of the IG Act that ensures access to records."

Horowitz said document production has been speeding up, but lack of access continues to be a problem. And he warned that whistleblowers might be deterred from disclosing information about malfeasance if it it could later be determined that the material could not be shared with agency watchdogs.

Dozens of confirmed and acting IGs signed a letter to the leaders of the House and Senate government watchdog committees asking for legislation that "affirms the independent authority of inspectors general to access without delay" all information sought by an IG.

— Adam Mazmanian

EDITOR'S NOTE

The fundamental challenge of federal IT training

One of the best things about journalism is that going out and learning new things every day effectively IS the job description. And although not all jobs are quite so centered on building knowledge, it would be the rare position in federal IT that does not demand the near-constant cultivation of new skills and expertise.

It's not hard to understand why continuous learning is such a necessity. Federal agencies have a special set of ever-changing circumstances — from FITARA implementation and cybersecurity protocols to budget politics and acquisition guidelines — but the fundamental technology is evolving even faster.

A decade ago, no one needed to worry about cloud security, few had contemplated how to procure software as a service, and predictive analytics were an intriguing idea — not something to implement this fiscal year. Is it any wonder that a 2014 survey of IT professionals found that fully 59 percent feared their skill sets would become obsolete?

Although the demand is clear, the supply side is a bit more complicated. Traditional degrees are an obvious but expensive solution and one that sometimes lacks the agility working professionals demand.

Certificate programs remain a critical part of the IT equation, but sorting the valuable skills from the empty credentials can be a daunting task.

The government offers its own training, of course, and massive open online courses (MOOCs) from sources such as edX and Coursera dangle the prospect of free learning from top-flight universities — so long as you're not among the 90-plus percent of MOOC students who fail to complete the courses!

Hands-on learning and committed mentors are arguably the most valuable resources, but they are maddeningly difficult to both find and measure. And all of it comes against a backdrop of tepid training budgets and a "do more with less" culture that leaves precious little time to pursue the training these jobs demand.

You won't find an answer to the time-and-money conundrum in this issue, I'm afraid. But you will find a wealth of information on current opportunities and some of the efforts to make more training available. As the FCW team learns more through our expanded coverage of training and education, we'll be sure to share that knowledge here.

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

13TH ANNUAL
ENTERPRISE ARCHITECTURE
EA TODAY: MAKING THE MISSION POSSIBLE

EVENT BEGINS IN 1 MONTH!

EA TODAY: MAKING THE MISSION POSSIBLE

How? Find Out at the Enterprise Architecture Conference!

WORKSHOPS: OCTOBER 5
CONFERENCE: OCTOBER 6–7
WASHINGTON, DC
WALTER E. WASHINGTON CONVENTION CENTER

THE 13TH ANNUAL ENTERPRISE ARCHITECTURE EVENT IS THE PREMIER educational forum for enterprise architects and project managers to convene and learn from expert practitioners in EA on the latest methods, frameworks and policies impacting the EA community.

EDUCATION TRACKS INCLUDE:
- Achieve Mission Outcomes
- Strengthen Enterprise Management

SESSION TOPICS WILL INCLUDE:
- Agile
- Security and Privacy
- Business Analytics
- Big Data
- Role of the Chief Data Officer

… just to name a few!

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

Reserve Your Seat Today — Space is Limitied!

GovEAconference.com
USE PRIORITY CODE: EAE15

PRESENTING SPONSORS
FEAC Institute
Zachman International Enterprise Architecture

EVENT SPONSORS
In2itive
software AG Government Solutions

PARTNERING MEDIA
OMG We Set the Standard

PRODUCED BY
Public Sector Events Group

$70 million in annual cost avoidance is being attributed to FedRAMP

CRITICAL READ

WHAT: An Office of Personnel Management sources sought notice for support of its electronic Official Personnel Folder.

WHY: The eOPF system contains records that cover a civilian federal worker's employment history. OPM and agency human resources departments refer to those documents to make decisions about employee rights, benefits and entitlements. More than 100 federal agencies use eOPF to track 2.5 million employees.

OPM is seeking information from potential vendors that could handle development, program management and data management for eOPF, which is built on Northrop Grumman's e.Power platform.

The company handles a broad spectrum of OPM work, but the sources-sought notice estimates that the eOPF support is worth $6.5 to $7 million.

The current contract expired Aug. 23, and OPM had anticipated issuing a request for proposals and making a contract award by that date.

VERBATIM: "Through on-demand Web-based access to personnel folders, eOPF enables 24/7 concurrent access to personnel information by human resources staff and employees. It also allows the electronic transfer of the eOPF from one agency to another when the employee moves from one organization to another."

READ THE NOTICE:
is.gd/FCW_eOPF

VA launches cybersecurity strategy squad

LaVerne Council, the new CIO at the Department of Veterans Affairs, has assembled a team charged with developing a cybersecurity plan for the agency.

The new Enterprise Cybersecurity Strategy Team will be led by Susan McHugh-Polley, a senior executive program manager at VA. The team includes executives and subject-matter experts from VA's Office of Information and Technology.

"The team's scope includes management of current cybersecurity efforts as well as development and review of VA's cybersecurity requirements and operations holistically — from desktop to software to network protection," a VA spokesperson told FCW.

A summary of the plan will be made public once it is completed and presented to Congress, the spokesperson added. The plan is due to be completed in 45 days, according to an article in FedScoop, which first reported on VA's new cybersecurity effort.

The current strategy, dubbed "defense-in-depth," uses the Einstein 3 network-protection system offered by the Department of Homeland Security as its perimeter defense. Additional layers of protection surround local networks, devices, data centers and servers.

Stephen Warren, who served as acting CIO at VA for more than two years, published monthly reports on intrusion detection under Einstein 3, as well as potential data loss as a result of mishandled files and lost or stolen computer equipment. Warren left VA at the end of August for the CIO position at the Treasury Department's Office of the Comptroller of the Currency.

According to a fact sheet released in July, the department has encrypted all of the more than 438,000 laptops and desktops on its network, and has decreased its critical or high vulnerabilities by 71 percent.

Despite some gains, VA's inspector general gave the agency a failing grade on information security in the most recent security audit because of multiple outstanding recommendations going unfulfilled over several years.

VA's most recent public report — for June 2015 — said 2,076 veterans had been affected as a result of mishandled information.

None of the potential data loss incidents were the result of cyberattacks, according to the report.

— Adam Mazmanian

Mike Rogers
@RepMikeRogers

Now our own government is going to work against itself for God only knows how long, again... more via @FCWnow: http://bit.ly/1HnMwzU

Reply Retweet Favorite

6:11 AM - 5 Aug 2015

Join the conversation

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

1 exaflop of supercomputer processing power is the goal of the newly created National Strategic Computing Initiative

FCW Insider: People on the move

Stephen Warren, the senior executive who led IT at the Department of Veterans Affairs over a rocky period, left VA on Aug. 28 to take the CIO post at the Treasury Department's Office of the Comptroller of the Currency.

As deputy CIO, Warren ran VA's $4 billion IT department for almost two-and-a-half years on an acting basis. His exit came just after **LaVerne Council**, a former top private-sector CIO, took the reins at VA's Office of Information and Technology.

Warren had been closely identified with VA's cybersecurity efforts and briefed reporters monthly on the threats identified and thwarted by the use of the Einstein 3 network defense provided by the Department of Homeland Security.

Warren, an Air Force veteran, worked at VA for more than seven years. He told FCW that the death of his brother in Iraq led him to the department. He became acting CIO at VA after the departure of **Roger Baker** in March 2013.

Warren's time at VA was marked by run-ins with Congress and criticism over IT security. For more than four years, information security has been identified as a material weakness by VA's Office of Inspector General.

In June 2013, only a few months after Warren took over as acting CIO, former Deputy Assistant Secretary for Information Security **Jerry Davis** revealed that nation-state-sponsored cyberattackers had penetrated VA networks, which put personal data on 20 million veterans at risk.

However, VA's use of the Einstein system has thwarted millions of penetration attempts, and after years of wrangling, VA has reported 100 percent success in encrypting laptops and desktops connected to the VA network.

"Even with these successes there are areas where we need to continue to up our game," Warren told FCW. "Technology continues to change, services to veterans continue to increase and improve, [and] the threat to our data never diminishes."

At Treasury, Warren will lead a department responsible for a $106 million IT budget, according to the federal IT Dashboard. He is taking over the CIO post left vacant by **Edward Dorris**, who now leads IT at the National Credit Union Administration.

Clockwise from top left: Stephen Warren, LaVerne Council, Zalmai Azmi and Jason Matheny.

Another top IT official has departed the executive ranks at VA. **Stan Lowe**, the agency's chief information security officer, retired from federal service on Aug. 22. He had served at VA for 25 years.

Lowe led IT security when VA was trying to restore its reputation after several key incidents involving lost or compromised data, failing grades on information security from VA's inspector general and attacks from nation-state-sponsored hackers. VA activated the Einstein 3 network-defense system on Lowe's watch, and he presided over efforts to encrypt 100 percent of the desktops and laptops connected to VA networks.

"Our workforce has done an outstanding job in the face of significant adversity," Lowe wrote in an email message to colleagues that was obtained by FCW. "In two-and-a-half years, we have made more strides toward improving VA's information security posture than ever before."

Glenn Gerstell, the new general counsel at the National Security Agency, has worked on cybersecurity issues for the District of Columbia and DHS' National Infrastructure Advisory Council.

For the past two-and-a-half years, he served as a commissioner on the D.C. Homeland Security Commission, and he spent nearly 40 years at law firm Milbank, Tweed, Hadley and McCloy.

Zalmai Azmi is now president and chief operating officer at IT consulting firm IMTAS.

A native of Afghanistan who served as the FBI's CIO from 2004 to 2008 and led the bureau through an IT transformation, Azmi said he is pleased and excited about his new role. He has also served as CEO of Nexus Solutions, a senior vice president at CACI and CIO at the Executive Office for U.S. Attorneys.

Jason Matheny is the new director of the Intelligence Advanced Research Projects Activity. He previously served as director of IARPA's Office for Anticipating Surprise, which develops new forecasting capability for national security threats, and worked at the Office of Incisive Analysis, an analytics shop that works with old and new datasets.

In addition, Matheny has held positions at Oxford University, the World Bank and the Applied Physics Laboratory at Johns Hopkins University, where he earned a doctorate in applied economics. He also co-founded two biotechnology firms.

— FCW staff

ANDREW CHANG is managing partner at Eastern Foundry.

Removing acquisition roadblocks — together

Government innovation is a no-go unless agencies, prime contractors and startups come together to clear the path

The federal government's procurement pathway is riddled with roadblocks for companies seeking to do business with agencies.

That restrictive climate makes it difficult for startup companies to pursue and win contracts, and it is the catalyst for a slow and costly process for prime contractors and agencies to locate new partners. In other words, that route is not the fast track to innovation that the government needs.

Many startups launch with a technology that they know can make our nation safer, more efficient or healthier. Those entrepreneurs pursue government contracts believing that the market's needs and the ingenuity of their solutions will propel them forward. But they immediately run into 1,800 pages of the Federal Acquisition Regulation and the need to register with the System for Award Management and request a Commercial and Government Entity Code, to name a few.

Many are deterred by those complexities and simply turn away from government contracting.

The companies that are not deterred still face costly challenges. Federal business expert Olessia Smotrova-Taylor said it best: "Companies that believe that they can find an opportunity on FedBizOpps when an RFP comes out, submit a proposal and win the contract are wasting a lot of energy."

Instead, entrepreneurs are often frustrated when they find themselves directing their efforts toward identifying the correct agencies to target, establishing professional relationships with the right procurement officers and properly positioning their companies to achieve a competitive advantage.

Even when companies are fortunate enough to win a contract, many are not equipped to handle the bureaucracy that permeates every level of government contracting. Some reach out to their colleagues for guidance.

> Many companies are not equipped to handle the bureaucracy that permeates every level of government contracting.

"I had to talk to others going through the process to learn how to handle it," said Matthew Stanton, co-founder of energy startup SolePower. "That peer-to-peer advice was invaluable."

Until recently, that protracted procurement process has been the only way. Essentially, the message was: Play by the rules or go home. But with the appointment of Secretary Ashton Carter, the Defense Department's plans to engage Silicon Valley, particularly with regard to cybersecurity, are poised to evolve.

Technology incubators and accelerators along the Eastern Seaboard are providing entrepreneurs with the knowledge and network to get started. Those initiatives all have a common objective of identifying a more collaborative approach to procurement that, when successful, will save agencies time and money and enable entrepreneurs to bring their technologies to bear.

For an example, I'll point to Worden Technology Solutions, a contractor that specializes in streamlining IT services. Worden has won several contracts, including one for the Navy's Space and Naval Warfare Systems Command, and owner Chris Worden believes in the power of collaboration in the government contracting space.

"Instead of slogging along alone and becoming bitter, you have other companies around you to network with and take advantage of those relationships," he said. "It's a game-changer."

Cases like Worden's attest to the idea that it is time to apply a more collaborative approach to government contracting.

Even successful contractors face roadblocks that include protracted payment cycles after winning contracts, but helping them get to the door is a start. With collaboration, entrepreneurs and agencies could achieve a more accelerated innovation pace to keep our nation on the cutting edge of progress. ■

DAVE GWYN is vice president of Nutanix Federal.

The new RFI: Request for innovation

The natural tendency of RFPs and RFIs to protect outdated architectures must be overcome if FITARA is to succeed

The Federal IT Acquisition Reform Act (FITARA) is expected to help modernize the government by establishing new technology and acquisition policies that reduce duplication and drive significant cost savings. It's an effort to streamline and strengthen how government buys and manages technology that is long overdue.

More than 75 percent of the government's IT budget, or about $62 billion, is spent on maintaining legacy IT systems, according to the Government Accountability Office. Obsolete software and hardware are expensive, inefficient and time-consuming to maintain, and they do not allow agencies to be agile enough to compete in today's rapidly changing marketplace.

Whether or not you are a fan of FITARA, it's hard to disagree that agencies should embrace modernization. Although requests for information and proposals should be the starting point for that transformation, they have become a shelter for the status quo — a place where innovation goes to die.

People have a natural tendency to stick with what's comfortable. Thus, FITARA's progress will be slowed because acquisition professionals will stick with the familiar in terms of vendors, architectures and technologies.

In fact, current RFIs and RFPs still call for the same old stuff. A prime example is the data center space, where solicitations require expensive and inefficient three-tiered architectures rather than the new scalable, simple and less costly hyperconverged solutions used in the world's largest data centers.

Furthermore, a standard that might have been an undisputed high priority only a year or two ago could be considered antiquated today. For example, Fibre Channel connectivity might sound efficient, but those requirements are in fact obsolete and no longer exist in the scalable, agile infrastructures used by the most efficient data centers.

> Asking for an obsolete capability by the old terminology could eliminate more modern and effective technologies.

With technology changing so rapidly, federal IT leaders cannot possibly be expected to stay abreast of all that is available. Therefore, it's not uncommon or unexpected for vendors to know more about which requirements are truly critical and which ones have been superseded through innovation. However, when one vendor says a particular requirement is obsolete and can be fully replaced with a newer, more efficient technology and another vendor says the opposite, how can federal IT professionals know what's true? And without knowing that, how can they safely drop the "obsolete" requirement without creating risk for their initiative?

Similarly, although a requirement might have been necessary years ago when certain software was written, it's possible — even probable — that the software will run as well as or better atop newer technology. But if new technology uses new techniques and terminology, asking for the obsolete capability by the old terminology could eliminate those more modern and effective technologies.

There are multiple ways to address those conundrums. Some require behavioral changes while others are more tactical in nature. For example, legacy applications should be tested on the latest technology platforms in advance of solicitations, so that when the solicitations are written, agencies know whether the old documentation is no longer useful.

If FITARA is to succeed, RFIs and RFPs must be the wide-open doors through which new technology passes — not the gates that block it. And for that to happen, IT leaders must be able to discern obsolete standards from necessary ones. Congress should strongly consider financial support for Federally Funded Research and Development Centers to help agencies answer those questions. And agency IT leaders should make clear to their teams that only those who embrace innovation will be rewarded. ■

BACK TO SCHOOL

Training budgets are tight, but the need to keep skills current is stronger than ever. FCW looks at the many options available — for both IT leaders and their teams.

BACK TO SCHOOL

CYBERSECURITY

6 SCHOOLS WITH THE RIGHT STUFF

The federal government craves more cybersecurity professionals. These six schools are helping meet that demand.

BY SEAN LYNGAAS

For all of the finger-pointing and blame-shifting that followed the massive hacks of the Office of Personnel Management, lawmakers and officials agree on this much: The federal government needs more cybersecurity professionals.

That obvious and seemingly insatiable demand has spawned a variety of cybersecurity training programs, some of which cater to veterans and others to active-duty military personnel.

Trainees hoping to land a federal cyber job can take heart in two developments at the departments of Defense and Homeland Security. One is the Pentagon's goal of building a cyber workforce of approximately 6,200 — and officials say they are already about halfway there. The other is the hiring authority DHS received from Congress late last year that allows DHS to pay cybersecurity experts more than was previously possible and retain them with bonuses.

Although competition for those slots at DHS and DOD will likely be fierce, a good training program can boost an applicant's chances. Here are six schools that are making an impact.

1. CHAMPLAIN COLLEGE

Cybersecurity is part of the 60 online certificate, bachelor's and master's degree programs for which Champlain College in Burlington, Vt., is offering steep discounts to federal participants. The cybersecurity "specialization" for undergraduates covers topics such as ethical hacking, introductory programming and information assurance, including risk assessment and government policy.

Sydney Smith-Heimbrock, OPM's chief learning officer, has touted the college's online courses as a means of reaching "every civilian employee regardless of their duty station."

Champlain College is no upstart in cybersecurity: Back in 2007, the National Security Agency and DHS

SO MANY CREDENTIALS...

For many IT jobs, specialized certifications remain the coin of the realm. The 23 that follow are in especially high demand, in both government and the private sector.

INFORMATION SECURITY

Certified Ethical Hacker

Audience: Information security specialists

Focus: Ability to use hacking techniques to conduct penetration testing on a network's defenses with the goal of discovering and securing vulnerabilities

Requirements: At least two years of information security-related experience and an educational background that reflects specialization in information security. The EC-Council offers an optional five-day course exploring ethical hacking techniques and security issues.

Certifying organization: EC-Council (eccouncil.org)

Certified in Risk and Information Systems Control

Audience: Experienced IT and business professionals

Focus: Ability to identify, assess and evaluate risk throughout the life cycle of information systems control. Exams are offered annually in June and December.

designated it a National Center of Academic Excellence in Information Assurance.


Champlain College

2. UNIVERSITY OF MARYLAND UNIVERSITY COLLEGE

Before its partnership with Champlain College, OPM worked with the University of Maryland University College to offer discounts on training for federal employees.

Washington, D.C.-area public transit riders will be familiar with UMUC advertisements touting its cybersecurity credentials, and the college contends that it was one of the first to build cybersecurity into its curriculum.

"UMUC recognized the crisis that we were having with human capital in the cybersecurity-related area," said retired Lt. Gen. Harry Raduege Jr., former director of the Defense Information Systems Agency, in a promotional video for the college. "I was impressed by that because others may have recognized it, but they weren't bold in moving and committing so many university resources to addressing this growing area of concern."

UMUC also boasts partnerships with industry heavyweights, including Cisco, Google and SAIC.

NSA and DISA are among the cyber-related agencies based in Maryland, and UMUC notes that a good number of cybersecurity jobs (about 5 percent as of 2014) are in that state.

3. LOUISIANA TECH RESEARCH INSTITUTE

Louisiana Tech University and the Cyber Innovation Center, a research and development outfit in Bossier City, La., announced the creation of the nonprofit Louisiana Tech Research Institute in July. It will provide office and lab space for research, "workforce development efforts and external partnerships with industry and government," according to the announcement.

The institute will be located at the Cyber Innovation Center's headquarters at the 3,000-acre National Cyber Research Park, which is already home to several large firms, defense contractors and cybersecurity startups. Computer Sciences Corp., meanwhile, is building a technology center next door.

It is all part of the plan to build an ecosystem of innovation, Louisiana Tech University officials said.

In the statement announcing the institute, officials said: "This integration of academia and industry is critical to support the overall 'ecosystem' that furthers innovation, creates entrepreneurship and spin-off companies, and attracts additional federal research funding — all of which drives the expansion of a knowledge-based, 21st-century economy."

4. UNIVERSITY OF SAN DIEGO

The University of San Diego's new Center for Cyber Security Engineering and Technology will support master's

PROFESSIONAL CERTIFICATIONS

Requirements: At least three years of cumulative experience incorporating three of five performance areas: risk identification, assessment and evaluation; risk response; risk monitoring; information systems control design and implementation; and information systems control monitoring and maintenance.
Certifying organization: ISACA (isaca.org)

Certified Information Security Manager

Audience: Information security managers
Focus: Ability to develop, build and manage enterprise information security programs
Requirements: At least five years of experience in information security, three of which must have been served as an information security manager. Exams are offered annually in June, September and December.
Certifying organization: ISACA (isaca.org)

Certified Information Systems Security Professional

Audience: Security managers, auditors, network architects, chief information security officers and similarly skilled professionals
Focus: Managerial competence and the technical aptitude to design, engineer, implement and oversee information security programs
Requirements: At least five years of cumulative work experience in two of the following eight areas: security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, and software development security
Certifying organization: (ISC)2 (isc2.org)

FACE TO FACE

Face-to-Face Event Series

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

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

FCW.com/events

UPCOMING EVENTS

DOD: Joint Information Environment
SEPTEMBER 23

Cybersecurity
OCTOBER 27

Big Data
DECEMBER 2

For event sponsorship information, contact:
Alyce Morrison
Event Sponsorship Consultant
703.645.7873
amorrison@1105media.com

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

degrees in cybersecurity engineering and IT leadership, and the latter will be available online.

"The community can access USD's cybersecurity expertise through degree and certificate programs, inviting USD's cyber experts to participate in projects focusing on the evaluation and development of their own systems and strategies to mitigate cyberthreats, and developing internal leadership on cybersecurity IT, cybersecurity law, forensics and incident response," said Jason Lemon, the university's dean of professional and continuing education, in a statement.

5. NORTH CAROLINA STATE UNIVERSITY

North Carolina State University is the site of NSA's Laboratory for Analytic Sciences and offers a master's degree in big-data analytics.

NC State was one of four major universities to receive funding from NSA last year for cybersecurity research in five key areas: scalability and composability, policy-governed secure collaboration, security metrics, resilient architectures, and understanding and accounting for human behavior.

The university had previously received a grant of $2.5 million for research ranging from fault-tolerant computing to security context. An NC State professor told FCW that the 2014 funding would be used for similar research, with a focus on the design of trusted IT systems.

NC State lies in North Carolina's Research Triangle, which is a magnet for engineering and, increasingly, cybersecurity talent.


George Mason University

6. GEORGE MASON UNIVERSITY

Like UMUC, George Mason University's proximity to Washington, D.C., makes it a convenient potential pipeline for federal agencies.

The State Council of Higher Education for Virginia approved GMU's master of science degree in management of secure information systems in 2011. "This isn't just a technical cybersecurity program," said Daniel Menasce, who was a senior associate dean in GMU's Volgenau School of Engineering at the time and is still a computer science professor at the school. "Cybersecurity is not just a technical problem, it is also a policy and management problem."

The Fairfax, Va., university's cybersecurity curriculum has since expanded. Officials say GMU is the first college in the country to "offer a cybersecurity engineering degree that focuses on cyber-resilience engineering design."

The staff of the Volgenau School of Engineering includes Associate Professor Angelos Stavrou, who is also a guest researcher at the National Institute of Standards and Technology's Computer Security Division. ■

PROFESSIONAL CERTIFICATIONS

CyberSecurity Forensic Analyst

Audience: highly experienced digital forensic professionals

Focus: Ability to conduct a thorough and sound forensic examination of a computer system and other digital/electronic devices, properly interpret the evidence, and communicate the examination results effectively and understandably

Requirements: Practical experience in the field of digital forensics

Certifying organization: CyberSecurity Institute (cybersecurityforensicanalyst.com)

EC-Council Certified Security Analyst and Licensed Penetration Tester

Audience: Information security professionals

Focus: Various penetration testing and security auditing methodologies for ECSA, and report-writing skills and the ability to perform penetration tests in real-time scenarios on an active cyber range for LPT. Successful candidates will receive two certifications.

Requirements: Basic ethical hacking skills. Certified Ethical Hacker certification is highly recommended.

Certifying organization: EC-Council (eccouncil.org)

GIAC Certified Penetration Tester

Audience: Information security professionals

Focus: Penetration-testing methodologies, the legal issues surrounding penetration testing, how to properly conduct such tests, and technical and non-technical techniques

BACK TO SCHOOL

VETERANS

CYBER TRAINING FOR VETS FOCUSES ON ANALYTICS

BY SEAN LYNGAAS

A cybersecurity course for veterans run by NS2 Serves has honed in on analytics as it heads into its fourth session.

Potential employers have shown a tremendous amount of demand for analytical skills, said Mark Testoni, president of SAP National Security Services, a subsidiary of the software giant that created the independent, nonprofit organization to train veterans in high-tech careers.

The course gives veterans the "basic skills to approach…the new generation of jobs," he added.

The first NS2 Serves courses, conducted last year, focused on enterprise resource planning, but after conversations with prospective employers, NS2 Serves has shifted the curriculum to focus on analytics, said Laura Carmack, the organization's vice president of recruitment and assessment.

The latest three-month course trains students in how to use search tools to find and analyze information in data warehouses. At a time when companies and agencies are awash in data and looking to make sense of it, a trained database curator can come in handy.

IT experience is not a prerequisite for the NS2 Serves program. And although many other programs focus on preparing veterans for the workforce, Testoni said few target the "hard-to-employ" veterans that NS2 Serves does.

Of the 56 veterans who have successfully completed the organization's training, the majority do not have college degrees and a few have been homeless, he said.

The program builds on "those good skill sets that they get in the military and [adds] an important technical skill on top that would allow more employability," he said.

All 56 graduates have gotten jobs, mostly with companies that use SAP National Security Services products. Testoni said those companies include Accenture, Computer Sciences Corp., Lockheed Martin, Northrop Grumman and SAP.

For veterans who are tech savvy but not necessarily computer whizzes, training programs like NS2 Serves can be crucial to getting their resumes a second look. Carmack said IT professionals use certifications as calling

Requirements: No specific training is required
Certifying organization: Global Information Assurance Certification (giac.org)

GIAC Security Essentials

Audience: Security professionals who want to demonstrate they are qualified for hands-on roles with respect to IT security tasks
Focus: An understanding of information security beyond simple terminology and concepts
Requirements: No specific training is required
Certifying organization: Global Information Assurance Certification (giac.org)

Information Systems Security Engineering Professional

Audience: Senior systems engineers, information assurance officers and senior security analysts
Focus: Ability to incorporate security into information and business processes, systems and projects. The certification was developed in cooperation with the National Security Agency.
Requirements: At least two years of engineering experience
Certifying organization: (ISC)2 (isc2.org)

IT MANAGEMENT AND COMPLIANCE

Certified Information Systems Auditor

Audience: Information systems specialists
Focus: Managing vulnerabilities and offering processes and controls that ensure compliance with standards while delivering value to the enterprise. The certification is often a prerequisite

BACK TO SCHOOL

PEOPLE

WHAT CIOs ACTUALLY STUDY

A degree in IT or administration can help, but top CIOs have degrees in everything from religious studies to zoology

Jonathan Alboum, Agriculture Department CIO, is a University of Virginia alum; he studied systems engineering as an undergraduate and earned a masters in IT management.

Darren Ash, CIO at the Nuclear Regulatory Commission, majored in international studies at American University and holds two master's degrees: in public administration from Syracuse University and information systems from George Washington University.

Department of Health and Human Services CIO **Frank Baitman** studied political science and English as a State University of New York at Albany undergraduate, then went to the University of Maryland for a master's degree in public management.

Sonny Bhagowalia, Treasury Department CIO, has both a bachelor's and a master's in electrical engineering from Louisiana State University and another master's — this one in information resources management — from Syracuse University.

Interior Department CIO **Sylvia Burns** double-majored in geology and a special honors curriculum at Hunter College, and has a master's in business management and policy from Stony Brook University.

Commerce Department CIO **Steve Cooper** has a bachelor's degree in zoology from Ohio Wesleyan University.

Department of Veterans Affairs CIO **LaVerne Council** has a trio of business degrees: a bachelor's from Western Illinois University, an MBA in operations management from Illinois State University and a doctorate in business administration from Drexel University.

THERE ARE 2 LAWYERS AND 2 PH.D.s.

Rafael Diaz, CIO at the Department of Housing and Urban Development, was a biology major at the University of Illinois, earned a master's in human services administration from Spertus College and holds a computer career program certificate from DePaul University.

Environmental Protection Agency CIO **Ann Dunkin** is a two-time graduate of the Georgia Institute of Technology, with a bachelor's in industrial systems engineering and a master's in manufacturing systems engineering.

Defense Department CIO **Terry Halvorsen** focused on history and pre-law at Widener University, then earned a master's degree in educational technology at the University of West Florida.

Danny Harris, the Education Department's CIO, majored in communications at North Carolina A&T State University, then went to Howard University for both a master's and a doctorate in organizational management.

Energy Department CIO **Michael Johnson** has a master's in computer science and engineering.

Joseph Klimavicz, the Justice Department CIO, attended Virginia Tech for both a bachelor of science and a master's degree in engineering.

Labor Department CIO **Dawn Leaf** did her undergraduate studies at McDaniel College and earned a master's degree in systems engineering at Johns Hopkins University.

Renee Macklin, the Small Business Administration's CIO, majored in computer systems technology at the Rochester Institute of Technology and earned her master's in information systems management from American University.

Jay Mahanand, CIO at the U.S. Agency for International Development, has a bachelor's degree in engineering from the University of Maryland.

Luke McCormack, CIO at the Department of Homeland Security, has an MBA from the University of Maryland's Smith School of Business and certifications from Columbia University and National Defense University.

Transportation Department CIO **Richard McKinney** studied political science at Ohio State University before earning a bachelor's degree and a master's degree in public administration from Tennessee State University.

National Science Foundation CIO **Amy Northcutt** went to Smith College for her undergraduate studies, earned a master's degree in religious studies

MANAGEMENT AND ADMINISTRATION DEGREES FAR OUTNUMBER ENGINEERING AND COMPUTER SCIENCE.

5 CIOs WENT TO A BIG TEN SCHOOL. THERE ARE NO IVY LEAGUE ALUMNI.

from the University of Chicago and holds a law degree from Boston College Law School.

Federal CIO **Tony Scott** majored in information systems management at the University of San Francisco and also has a J.D. in computer law from Santa Clara University.

Office of Personnel Management CIO **Donna Seymour** earned a bachelor's degree in computer science from George Mason University, where she has also continued graduate-level studies in operations research and management sciences.

David Shive, the General Services Administration's CIO, majored in physics as a California State University undergraduate, earned a master's in research meteorology at the University of Maryland and holds a post-graduate management certificate from the Carnegie Mellon Graduate School of Industrial Management.

NASA CIO **Larry Sweet** was a visual communications major at Texas Lutheran University.

State Department CIO **Steven Taylor** majored in business management as an undergraduate and holds a master's degree in information systems; he earned both degrees at Boston University.

Social Security Administration CIO **Bill Zielinski** was a psychology major at Washington State University.

Eli Gorski conducted the research for this article.

cards, and even a modest amount of training can boost employment prospects. She recalled how employers who had previously overlooked a candidate began taking notice of him once he received a certification.

What's more, she said, employers once skeptical of hiring trainees without a college degree are now warming to the idea.

Graduates act as ambassadors for the NS2 Serves program by spreading the word among their peers. In its first year, the program drew significantly on a Labor Department database of roughly 1 million veterans, but recruiting is increasingly happening through word of mouth, Carmack said.

Current and former policymakers have also backed the program. Former Defense Secretary Robert Gates met with NS2 Serves participants last year, while cybersecurity-minded lawmakers Rep. Dutch Ruppersberger (D-Md.) and Sen. Richard Burr (R-N.C.) serve as co-chairmen of the program.

The only real hurdle the program's backers face is funding. Conducting each course for about 20 veterans costs $30,000 to $35,000 per student, Testoni said. But the program has secured enough support to expand from two courses to three this year, he added. ■

ONLINE LEARNING

CAN MOOCs MAKE THE GRADE FOR FED TRAINING?

BY BIANCA SPINOSA

A massive open online course is just that — up to several thousand people can take the same MOOC, simultaneously and without cost, through sites such as Coursera, edX and Udacity.

One MOOC on machine learning, for example, has 27,323 students enrolled, according to Udacity's website.

So given the increasing demand for workers with cybersecurity and data analytics skills, could MOOCs be one of the keys to federal training needs?

Ryan Corey believes they can help. Corey has been in the cybersecurity field for 13 years, and in January, he co-founded Cybrary, a company that offers free courses on a range of cyber skills.

Corey said he launched Cybrary in part because he thinks people — and federal workers in particular — shouldn't have to pay big bucks for IT and cybersecurity training and because it was clear that cyber skills should be more broadly distributed.

"You've got some of the United States' most talented professionals

who are protecting these organizations, and yet attacks are getting through," Corey said.

Cybrary has thousands of participants with .gov and .mil email addresses, he said. Yet he believes the government should be doing more to train IT professionals in cybersecurity.

"I know for a fact they're not doing enough," he said. "It's too expensive to send somebody to a class. It's relatively inaccessible, and it's very impractical. [Agencies are] working with restricted budgets."

Corey noted that during the budget sequestration and government shutdown of 2013, training was one of the first things to be cut. He was working at a brick-and-mortar cybersecurity training company at the time.

"No one came to training the entire length of it," he recalled. "You had no one from any government agency there with us taking classes."

So far, Corey said, Cibrary averages 1,000 to 1,200 new registered users a day. In July, 84,000 people took classes through the company.

To stay afloat without charging tuition, Cybrary relies on advertising and fees students must pay if they want certificates of completion. The company also offers an enterprise platform that teaches compliance with the Federal Information Security Management Act and end-user security awareness training for organizations. He has even turned to Kickstarter for funding.

Working professionals who are already trained in a field and want to increase their expertise tend to use MOOCs the most. But providers are still learning how to attract and, more important, retain students for the duration of a course. According to a 2013 report by the President's Council of Advisors on Science and Technology, MOOCs only average a 6 percent completion rate.

MIT and Harvard University, however, published a report earlier this year analyzing data from 68 MOOCs offered by those two schools and found that participation tends to decline initially and then stabilize. The study also found that computer science courses are more likely to have better participation — 68,000 compared to 19,000 for other types of courses.

Certification also affects participation rates. More than half of MOOC students are looking for a certification of some kind, and most programs charge for that proof of accomplishment. Those fees are relatively modest — usually less than $100 — and students seeking a certificate complete courses at a far greater rate.

But not all certificates will translate into the continuing education credits that are recognized for federal training purposes. Therefore, interested students must work with their agencies to confirm credit or else dive into MOOCs strictly for the learning and skip the credentials.

MOOCs TO TRY

For those who want to boost their IT skills for free, MOOCs offer a vast array of relevant courses:

- Coursera and the University of Virginia's Darden School of Business offer **"Fundamentals of Project Planning and Management."** The course teaches students what is required to plan and execute large-scale projects and gives them an understanding of agile project management principles.
- Coursera and the Georgia Institute of Technology offer **"Human-Computer Interaction: User Experience and User Interface Design."** This course teaches the design cycle of user interface design and requires participants to take a capstone exam to earn a certificate.
- Cybrary offers more than a dozen courses in cybersecurity, including

PROFESSIONAL CERTIFICATIONS

for employment as an information systems auditor.
Requirements: At least five years of experience auditing, controlling, monitoring and/or assessing enterprise IT and business systems
Certifying organization: ISACA (isaca.org)

Information Technology Infrastructure Library Qualification

Audience: IT professionals
Focus: A modular approach to the ITIL framework comprising a series of qualifications focused on different aspects of ITIL best practices
Requirements: Vary by level of qualification being sought
Certifying organization: Axelos (axelos.com)

Microsoft Certified Solutions Expert

Audience: IT professionals
Focus: Ability to build innovative solutions across multiple technologies, both on-premises and in the cloud. Certifications are offered in the areas of server infrastructure, desktop infrastructure, private cloud, enterprise devices and applications, data platform, business intelligence, messaging, communication and SharePoint.
Requirements: Hands-on experience with Microsoft technology. Optional online or classroom training is available.
Certifying organization: Microsoft (microsoft.com)

Project Management Professional

Audience: Project managers
Focus: Complete life cycle of project

cryptography, malware analysis and computer forensics. There is also free online training toward becoming a Certified Information Systems Security Professional.

• edX and MIT teach **"Introduction to Probability: The Science of Uncertainty,"** a course on probabilistic modeling and statistical interference and their role in analyzing data to make sound predictions. College-level calculus is a prerequisite.

• edX and Microsoft offer **"Data Science and Machine Learning Essentials,"** which teaches data acquisition, preparation, exploration and visualization using Microsoft's Azure Machine Learning, R and Python to create a cloud-based data science solution.

• FutureLearn and the Open University offer an introductory cybersecurity course on **understanding online security and how to protect one's digital life**. It introduces participants to different types of malware and core concepts such as network security, cryptography and risk management.

• Udacity's **"Data Visualization and D3.js"** course explains the fundamentals of data visualization and teaches students how to use the popular JavaScript-based library of visualization tools. ■

BACK TO SCHOOL

PROCUREMENT

GETTING SMARTER ABOUT IT ACQUISITION

BY MARK ROCKWELL

It's been 15 months since Joanie Newhart, an associate administrator at the Office of Federal Procurement Policy, and Tony Grayson, acquisition program executive at the Federal Acquisition Institute, announced big plans for updating the certification for federal procurement professionals.

At the 2014 FOSE conference, Newhart talked about how FAI would revamp the Federal Acquisition Certification in Contracting (FAC-C), which hadn't been updated since 2008, to include specialized training for IT procurement, among other improvements.

The week before, Lesley Field, who was OFPP's acting administrator at the time, had issued a memo citing the importance of better aligning FAC-C with the Defense Department's contracting certification curriculum to strengthen the development of civilian agencies' acquisition professionals.

The new curriculum has been in place for more than a year, and efforts to improve acquisition continue to evolve.

Newhart recently told FCW that

oversight, including initiating, planning, executing, monitoring and controlling projects

Requirements: 35 hours of project management education and a bachelor's degree with 4,500 hours of project direction or a secondary degree with 7,500 hours of administration

Certifying organization: Project Management Institute (pmi.org)

NETWORKS

Certified Novell Engineer

Audience: Network engineers

Focus: Planning, installation, configuration, troubleshooting and upgrade services for networks and the ability to solve advanced support and high-level network problems

Requirements: Novell-authorized courses are available but not required.

Certifying organization: Novell (novell.com)

Cisco Certified Design Associate

Audience: Network design engineers, technicians and support engineers

Focus: The skills necessary to build basic campus, data center, security, voice and wireless networks

Requirements: A valid Cisco Certified Entry Networking Technician or a Cisco Certified Network Associate Routing and Switching certification

Certifying organization: Cisco Systems (cisco.com)

the new and improved FAC-C is part of a broader initiative to recruit, train, develop and retain talented members of the acquisition workforce at civilian agencies. The effort extends beyond FAC-C to include updated certifications for program managers and contracting officer's representatives.

FAI is also establishing core-plus certifications in certain areas, with the first being IT specialization for program manager certification, Newhart added.

"The FAC-C refresh, which is broader than just IT-specific procurement training, strengthens the development and professionalization of civilian agency contracting professionals while better aligning the FAC-C to the DOD contracting certification," she said. "For example, we now require Level I and Level II courses on cost and price analysis, and Level II courses on supply and service contracting. Overall, we require roughly 25 percent more hours of training than in the original FAC-C."

The extended training and development reflect the increasing complexities that the federal acquisition workforce faces in using taxpayers' money effectively in support of agency missions, she added.

The new program will dovetail with another OFPP effort — this one in partnership with the U.S. Digital Service — to create a Digital Service Contracting Professional Training and Development Program through a multi-phased challenge.

Traci Walker, lead contracting officer at USDS, said the challenge offers participants as much as $360,000 in prize money for ideas that will help USDS and OFPP better understand what the landscape will look like for IT acquisition professionals in the next several years.

In July, USDS announced three finalists that will move into Phase II of the program — GovLoop, Team ICF and ASI Government, and Management Concepts. Each finalist receives $20,000 to design their proposed program in more detail. The goal is to develop methods that USDS can use to teach federal contracting personnel to understand digital services, measure contract success based on industry standards and encourage commercial best practices in the federal procurement process.

At the end of Phase II, one winner will move into Phase III and "will pilot [its] approach with federal acquisition professionals" with the goal of creating a training and development program that can be implemented governmentwide in 2016, Walker told FCW. In addition, elements of the challenge might be incorporated into the core-plus certification program, she said.

Newhart also said the results of the challenge will figure prominently in how FAC-C addresses digital services. "We will be developing a core-plus specialization in digital for the FAC-C" after the challenge is completed, she said. "The program designs submitted during the challenge and the design of the completed pilot will help inform our specialized certification for digital."

In addition, FAI plans to develop a core-plus specialization in other areas where specialized certifications might be helpful. "The drive to specialize is a part of our broader effort to train and develop our acquisition workforce more innovatively given what we've been hearing regarding how our workforce prefers to learn," Newhart said.

Officials are open to other innovations for training and developing acquisition personnel. "We're looking at cross-functional training involving the entire acquisition team, rotational assignments across functions (for example, a contracting officer on a detail to an IT program office), building career pathways for contracting professionals and developing more training offerings in agile methodology," Newhart said.

Larry Allen, president of Allen Federal Business Partners, said the upgrades and new outreach efforts have been needed for some time. "Improving the federal acquisition workforce's skill sets and engaging acquisition [workers] as agency partners" is a valuable shift from "basement-level buying [to] a 360-degree view of what an agency is doing," he said.

The biggest problem for any program that seeks to keep up with IT, however, is the rapidly evolving nature of the technology itself. FAI and USDS have realized that "training isn't static," Allen said.

"Let's not set it and forget it," he added. ■

FACTS ABOUT THE FEDERAL ACQUISITION INSTITUTE

- Established in 1976 under the Office of Federal Procurement Policy Act.
- Charged with fostering and promoting the development of the federal acquisition workforce.
- Facilitates and promotes career development and strategic management of the acquisition workforce.
- Coordinates with organizations such as the Office of Federal Procurement Policy, the Chief Acquisition Officers Council and the Interagency Acquisition Career Management Committee to develop and implement strategies to meet the needs of the current and future acquisition workforce.

Learn more at FAI.gov.

BACK TO SCHOOL

WORKFORCE

HOW OPM HOPES TO CULTIVATE CYBER TALENT

BY ZACH NOBLE

Feds are becoming eligible for retirement in waves, and cybersecurity skills are in desperately short supply. Importing talent is one solution, but another is developing the skills of the people who already work for the government.

"Over the next five years, four in 10 federal employees will be eligible for retirement," said Sydney Smith-Heimbrock, chief learning officer at the Office of Personnel Management. "OPM has identified cybersecurity as the highest-risk skills gap."

To help remedy that growing gap, OPM has pursued partnerships with higher education institutions, first with University of Maryland University College and now with Champlain College via a truED Alliance.

"Champlain College's nationally ranked, online education programs closely align with OPM's need to offer high-quality, affordable education opportunities for employees that focus on mission-critical areas," Smith-Heimbrock said. "This includes its No. 1-ranked cybersecurity higher education program by SC Magazine (which also includes its digital forensics program), as well as its health care management, human resources management and appreciative inquiry-based MBA programs."

The truED partnership allows feds to take online courses from the Burlington, Vt., college at substantially reduced rates — $10,000 for a bachelor's degree and $11,000 for a master's degree, according to the college.

"It's definitely less than I paid for my degree," said Mika Nash, academic dean in Champlain College's Division of Continuing Professional Studies.

Nash said roughly 90 federal students have enrolled in the inaugural summer for the government's truED alliance, with some 400 signed up for fall classes and hundreds more in the pipeline. OPM declined to provide its own enrollment figures.

"If you have someone in your agency who has demonstrated savvy in your workforce, either at keeping the bad guys out or at figuring out how they got in, that's the person you want to invest in," Nash said.

At the beginning, cybersecurity was the 10th most popular program offered through truED, but it has since rocketed up to fourth, she added.

PROFESSIONAL CERTIFICATIONS

Cisco Certified Network Professional Routing and Switching

Audience: Network engineers, support engineers, systems engineers and network technicians

Focus: Ability to plan, implement, verify and troubleshoot local- and wide-area enterprise networks

Requirements: At least one year of networking experience. Applicants must also pass three additional examinations in routing, switching and troubleshooting.

Certifying organization: Cisco Systems (cisco.com)

Juniper Networks Certified Internet Associate — Junos

Audience: Networking professionals

Focus: Knowledge of Juniper Networks' Junos OS, networking fundamentals, and basic routing and switching

Requirements: Beginner/intermediate knowledge of networking

Certifying organization: Juniper Networks (juniper.net)

SOFTWARE DEVELOPMENT

Certified ScrumMaster

Audience: Project managers

Focus: Managing complex projects within an open, interactive environment and gaining an understanding of the Scrum framework, including team roles, activities and artifacts

Requirements: Attending an in-person, two-day course taught by a certified Scrum trainer and then passing a CSM test

Certifying organization: Scrum Alliance (scrumalliance.org)

The most popular programs pertain to business, but Nash said students do not just gain knowledge that will help them advance their own careers. They also learn soft skills that will benefit the federal workforce.

As part of its cybersecurity curriculum, the college offers a digital forensics degree to teach students how to dust for cyber fingerprints after breaches.

"Ideally, you should put a lot of resources on the front end and minimize breaches," said Ric Messier, a cybersecurity program director at the college. However, he acknowledged the seeming inevitability of breaches and the importance of being able to determine the scope and severity of one after it has happened.

"OVER THE NEXT FIVE YEARS, FOUR IN 10 FEDERAL EMPLOYEES WILL BE ELIGIBLE FOR RETIREMENT. OPM HAS IDENTIFIED CYBERSECURITY AS THE HIGHEST-RISK SKILLS GAP."

— SYDNEY SMITH-HEIMBROCK, OPM

Messier touted Champlain College's "boots-on-the-ground approach to security." He said the college puts students through real-world drills rather than sticking to academic abstraction, and copious lab work deals with intrusion detection, emerging threats and more.

Nash said she expects the numbers of feds using truED to grow, while Smith-Heimbrock stressed the program's value in developing the talents of the existing federal workforce.

"Lifelong learning is a staple of today's federal workforce," she said. "Champlain College's programs place an emphasis on developing both hard skills as well as soft skills, like critical thinking and problem solving, that are equally important to future agency leaders and mission success." ■

PROFESSIONAL CERTIFICATIONS

Certified Secure Software Lifecycle Professional

Audience: Security professionals and software developers

Focus: Ability to develop an application security program, reduce production costs and vulnerabilities for applications, and diminish loss of revenue and reputation from an organizational software breach

Requirements: At least four years of cumulative full-time work experience in one or more of the eight CSSLP domains

Certifying organization: (ISC)2 (isc2.org)

Check Point Certified Security Expert

Audience: IT administrators

Focus: Ability to build, test and troubleshoot various Check Point Security Systems' deployments; configure and maintain security acceleration solutions; and manage, test and optimize corporate virtual private network tunnels

Requirements: Security administration course or Check Point Certified Security Administrator certification (R70 or later); Windows Server, Unix and networking skills and TCP/IP experience; and certificate management and systems administration experience

Certifying organization: Check Point Software Technologies (checkpoint.com)

EC-Council Certified Secure Programmer

Audience: Software developers and programmers

Focus: Ability to identify security flaws and implement countermeasures throughout the software development life cycle to improve the overall quality of products and applications

Requirements: Experience designing and building secure Windows and Web-based applications using the Microsoft .NET framework

Certifying organization: EC-Council (eccouncil.org)

VIRTUALIZATION

Citrix Certified Professional — Virtualization

Audience: IT solution engineers and consultants

Focus: Ability to install, configure and launch common Citrix XenDesktop solutions

Requirements: Complete the recommended coursework online or in person and pass an exam

Certifying organization: Citrix (training.citrix.com)

VMware Certified Professional — Data Center Virtualization

Audience: IT administrators

Focus: Ability to install, deploy, optimize, scale and manage VMware vSphere environments

Requirements: Completion of a VMware-authorized training course and a minimum of six months of hands-on experience with VMware technologies

Certifying organization: VMware (https://mylearn.vmware.com)

Jonathan Lutton conducted the research for this article.

The outlook for OASIS

The $60 billion vehicle for integrated services has already influenced other big acquisition efforts, but fiscal 2016 will be critical for OASIS' own future success

BY MARK ROCKWELL

The General Services Administration's $60 billion One Acquisition Solution for Integrated Services (OASIS) contract was one of the most anticipated agreements the agency has produced in the past decade. And despite being barely a year old, the service-oriented acquisition vehicle is already reshaping the way GSA handles other massive multiple-source procurements.

From the beginning, GSA wanted to use OASIS to show how the agency was reinventing itself as a more efficient smart shopper for its government customers. Observers say it has succeeded and the OASIS DNA can already be seen in other big upcoming contracts, including the Enterprise Infrastructure Solutions contract that is the cornerstone of the agency's buying strategy for next-generation telecommunications services, the Alliant 2 IT governmentwide acquisition contract (GWAC), and the Human Capital and Training Solutions contract.

"With OASIS, we cracked the nut for large" IDIQ contracts.

JIM GHILONI, GSA

OASIS allows agencies to buy a wide range of vetted goods and services under one contracting vehicle.

Alan Chvotkin, executive vice president and counsel at the Professional Services Council, said OASIS is a valuable model that has demonstrated the importance of working with a broad coalition of federal agency and industry leaders to create large, complex contracting vehicles.

"OASIS is among the most significant outreach efforts" GSA has ever undertaken, he added.

A pioneering approach

The agency collaborated with industry for two years before issuing a request for proposals. During that time, GSA officials gathered comments, ideas and suggestions from meetings with stakeholder groups and individual companies. They also launched an online interactive community to solicit even more input.

"GSA was willing to attend just about any meeting," Chvotkin said.

Officials repeated that open, collaborative approach when they created the RFP for the Enterprise Infrastructure Solutions contract, which is due by the end of September. As it did with OASIS, the agency held numerous face-to-face consultations and on-the-record, open meetings with vendors. GSA also hosted an online community for interested parties where it posted proposed changes and news about the contract.

In addition, OASIS officials pioneered a new approach to accepting vendors into the various service pools in each contract. Instead of the pass/fail grade typically used to

assess vendors, GSA opted to rely on a quantitative, point-based methodology that scored vendors' proficiency and sought bids with the highest technical rating and acceptable pricing.

GSA officials said the point structure better weighed the various capabilities, experience and performance of potential offerers to identify the 40 best in each of the contracts' pools of awardees.

The framers of Alliant 2, GSA's GWAC for total IT solutions, have said they are using the same methods for that vehicle. "We watched all the protests be resolved," said John Cavadias, the GSA senior contracting officer responsible for the Alliant 2 RFP. The standard of highly technically rated and fair and reasonable pricing "was found to be innovative, but within the rules, allowable."

The OASIS contracts were awarded in May 2014 but were delayed by a tangle of protests that took a few months to resolve. Some experts were concerned that the delays might sap OASIS' momentum, but all the protests were ultimately resolved in GSA's favor.

Attracting civilian agencies

Jim Ghiloni, the OASIS program director at GSA, said the agency's efforts, even with the protests, are building steady momentum, and early commitments from the Air Force and Army were a big help.

"With OASIS, we cracked the nut for large" indefinite-delivery, indefinite-quantity contracts, he said.

In 2013, the Air Force signed a memorandum of understanding with GSA that committed the service to spending an estimated $472 million over five years under OASIS. The

OASIS basics

The One Acquisition Solution for Integrated Services vehicle is composed of contracts for professional services such as financial management, engineering, science and logistics.

OASIS Small Business is a set of contracts exclusively for small companies, including those with special socioeconomic status, such as minority-owned businesses. Contracts have been awarded to 123 small companies, which have been divided into eight groups based on size and annual revenue.

The **unrestricted OASIS** vehicle has 74 contract holders spread across six pools that are divided by type of service. Many small businesses participate in this vehicle as subcontractors working with primary contract holders, which tend to be much larger firms.

Deltek estimates that the General Services Administration could capture 5 percent to 10 percent of the services market through OASIS, which could total $6 billion a year.

OASIS and OASIS Small Business complement GSA's Multiple Award Schedule contracts for professional services acquisitions by providing a single, unified path for complex requirements.

The agency does not classify OASIS as a governmentwide acquisition contract because GWACs are specific to IT requirements, and OASIS contracts are aimed at broader professional services and the ancillary products and services that go with them.

Historically, professional services procurements have been notorious for requiring multiple contracts to fulfill, leading to costly duplication.

According to GSA, **OASIS contracts are optimal** for requirements that:

- Cover multiple disciplines.
- Contain significant IT components but are not solely IT requirements.
- Include other direct costs.
- Must be performed on a cost-reimbursement basis.

Agencies benefit because OASIS:

- Offers a single acquisition platform.
- Maximizes small-business opportunities.
- Offers a focused number of awardees and contract holders.
- Reduces the lead time and administrative effort necessary to acquire complex professional services.
- Supports customers with a robust Web-based library of helpful features, including sample documents and templates.

AECOM

URS

URS Federal Services, Inc. is an AECOM Company. AECOM is a premier, fully integrated infrastructure and support services firm, with a broad range of markets, including transportation, facilities, environmental, energy, water and government. The recent incorporation of URS furthers AECOM's standing as a leader in all of the key markets that it serves. With nearly 100,000 employees — including architects, engineers, designers, planners, scientists and management and construction services professionals — the company serves clients in more than 150 countries around the world. AECOM provides a blend of global reach, local knowledge, innovation and technical excellence in delivering solutions that create, enhance and sustain the world's built, natural and social environments.

URS Federal Services Inc. is an OASIS awardee in Pools 1, 3, 4, and 6.

Jim Daly, OASIS Program Manager
FS.OASIS.COPM@urs.com
732.259-0795

Kyle Renehan, OASIS Contracts Manager
FS.OASIS.COCM@urs.com
301.944.3224

Jasmine Miller, Business Development Manager
Jasmine.Miller@urs.com
703.201.1984

OASIS℠
One Acquisition Solution for Integrated Services

Intel Community
- Facility Operations and Maintenance
- Language and Translation
- Open Source Intelligence & Analysis
- Document Declassification
- Cybersecurity
- Logistics
- Atmospherics
- Air Bridge Services
- Information Technology
- CI/HUMINT Analysis

Global Field Services
- Installations Managment/BOSS
- Policy Development & Institutional Support
- Economic Growth & Governance
- Crisis Response and Stabilization
- Threat Reduction/Second Line of Defense
- Global Contingency Support
- Renewable and Conventional Power Generation
- Water & Sanitation Support

Mission Readiness
- Aircraft Maintenance
- Depot-level Maintenance
- Surface Area Maintenance
- Facilities Operations & Maintenance
- Military Training
- Worldwide Logistics & Supply
- Transportation Management
- CAD Services
- Rapid Deployment Tiger Teams
- Security Services
- Range Support

SETA
- Systems Engineering
- Project Managment
- Technical Support
- Systems Integration
- IT Infrastructure
- Electromagnetic Spectrum
- Contingency Ops
- Training & Simulation
- Network Ops
- Systems Integration

Energy & Environment
- Environmental Remediation
- Chemical & Radioactive Clean-up
- Decontamination
- Nuclear Decommissioning
- Surveillance & Maintenance
- Technology Apps
- Technology Development

Army followed suit soon after with its own agreement. Those early commitments helped the contract "hit the ground running," Ghiloni said.

However, he added, those agreements also meant OASIS ran the risk of being viewed as a Defense Department-centric contract. Although he said the numbers could be higher, civilian agencies have made nearly 80 awards under OASIS Small Business, with $160 million in obligations so far. The unrestricted OASIS vehicle has seen 13 awards totaling $56 million in obligations from civilian agencies.

Ghiloni said some large task orders are still under evaluation and are due by the end of the fiscal year.

The contract got a valuable bump in July when the largest civilian agency of all, the Department of Homeland Security, signed a memorandum of understanding to use OASIS. DHS has also said it will not issue a follow-on contract for its Technical, Acquisition and Business Support Services contract and will instead rely on OASIS and other resources.

Ghiloni said agencies' OASIS task orders receive an average of five bids and generally take 90 days to 120 days to be completed. Anecdotal data indicates that customers save about 10 percent through OASIS compared to other contracts, he added.

The toughest challenge facing OASIS might be its own success. "GSA's biggest competitor is GSA."

ALAN CHVOTKIN, PSC

Building better tools

To help agencies with the decision-making process, GSA is expanding its online tools and making it easier to sort through pricing, purchasing and market research data, he said.

GSA unveiled a dashboard tool in early July that allows federal procurement professionals to customize OASIS data by federal agency and industry partner, and use it to build individualized, downloadable reports that can be exported to spreadsheets.

Ghiloni said the dashboard provides interactive, near-real-time information on the status of OASIS and OASIS Small Business task orders, including obligation values, the receiving agency and the industry partner for individual orders. Users can filter the data in multiple ways, drill down from the agency to the bureau level, and look at both the number and dollar value of task orders awarded to a particular industry partner.

Ghiloni said he intends to add even more electronic tools to help OASIS users and potential users see more deeply into the contract's data when making their buying decisions.

He added that it has been a challenge to build systems that are better at capturing data because OASIS is breaking new ground. "We're building this stuff from scratch," he said. "It's gone pretty well. The tools are good. They'll be better in two years."

According to Chvotkin, however, the toughest challenge facing OASIS might be its own success. "GSA's biggest competitor is GSA," he said.

He said the agency's myriad other contract efforts, including its schedule contracts, might pale in comparison to vehicles like OASIS that have electronic tools to tabulate data on what products are being bought and who's buying them, then spit out pinpoint reports.

Additionally, some vendors might have to make difficult decisions about which of the new and old contracts they want to pursue and how they want to pursue them, he added.

Chvotkin said the next few months are crucial for OASIS because the contract has to show it is viable for a wider federal audience. DHS' agreement is "a bellwether test," he said.

If other civilian agencies find value in OASIS in the coming months, it could pave the way for wider acceptance, he said, adding that if a significant number of agencies don't show up by the end of the year, it might mean they're not coming anytime soon. ■

The root causes of government IT insecurity

In the first of three columns, a former government executive discusses what's really needed to prevent another massive data breach

BY RICHARD A. SPIRES

In June, I testified before the Senate Appropriations Committee's Financial Services and General Government Subcommittee about the recent Office of Personnel Management data breaches. Given that I never worked at OPM, my testimony described broader systemic issues that must be addressed if we are to better protect our government's data and IT systems.

I am presenting the substance of that testimony in a series of three columns covering the root causes of the government's IT security issues and offering recommendations to address them.

Three primary root causes have led to the massive data breaches and compromises of core mission IT systems at multiple federal government agencies.

1. Lack of IT management best practices. The very best cybersecurity defense is the result of managing IT infrastructure and software applications well. During the 1970s and 1980s, agencies could build and deploy IT systems with little regard to security issues. That was not necessarily a management failure because there were few security issues to be concerned with prior to the broad use of the Internet and the rise of ubiquitous data networks.

Beginning in the 1990s and up through the present, however, the federal government has not properly managed its IT because it has failed to effectively adapt with the changes in IT and the evolving cybersecurity threat.

For example, when I served at the IRS and then at the Department of Homeland Security, we would all too routinely discover IT systems outside the IT organization's purview that had been developed and deployed without the proper IT security testing and accreditation. That highly distributed approach to IT management has led to the deployment of thousands of data centers across the federal government.

Today federal agencies struggle to manage and maintain that dispersed infrastructure and those disparate systems. In far too many instances, hardware and software assets are not systematically tracked, software is not routinely updated and patched, and critical hardware and software have reached their end of life and, in some cases, are no longer even supported by the vendors.

And although I am a big proponent of cloud technology, I am concerned that many agencies are not necessarily using cloud capabilities to streamline and simplify their infrastructures but instead are creating new stovepiped IT infrastructures. The complexity of maintaining a sea of vastly different systems in an ocean of differing IT infrastructures makes it impossible to properly secure an agency's IT environment.

2. Misguided IT security practices. Although well intentioned and appropriate for its time, the Federal Information Security Management Act (FISMA) skewed the government's approach to securing IT information. Passed in 2002, the law set a course for how IT security effectiveness has been measured in government.

Although the law has some good components, the unintended consequence is that it forced chief information security officers to focus on the controls for individual systems. In reality, IT systems across the government were already becoming more interconnected, and viewing systems in isolation hid the impact on the larger enterprise security posture.

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.

Further, based on guidance from the Office of Management and Budget, FISMA was implemented at a time when cyberthreats were still emerging and technology had not yet evolved enough to necessitate a security development life cycle.

In fact, until very recently, systems were certified and accredited on a three-year cycle. That cycle might be manageable, but it is comical when looking at the rapid evolution of technology and the cyberthreat environment. Furthermore, FISMA required the generation of paper-based reports that diverted time, resources and personnel from effective security efforts.

At the IRS and then DHS, I was consistently reluctant to put my confidence in the yearly FISMA reports because they did not reflect the reality of our overall IT environment's security posture. That can only be accomplished through the proper use of tools that continuously monitor the IT environment and react to and mitigate threats in near-real time.

3. A slow and cumbersome acquisition process. The problem is exacerbated when funds are available to invest in IT security yet it is ponderously slow and difficult to buy commercial solutions to help address vulnerabilities. When I was at DHS, I was a proponent of the Continuous Diagnostics and Mitigation program but was dismayed to see how long it took (two-plus years) just to implement Phase 1. And then agencies had to go through an additional competitive process within the CDM program to obtain capabilities.

I am all for fair competition, but with sophisticated adversaries that will exploit any and all vulnerabilities, the government amplifies its vulnerabilities when it takes many months (if not years) to procure and deploy new IT security capabilities.

Those root causes have led us to the current situation of the government paying a huge economic cost because of inefficiency, duplication and unsecure IT systems and infrastructure. And what is worse, we will now likely pay an even greater cost in the exposure of the personally identifiable information of millions of current and former government employees — certainly in terms of those individuals' privacy and potentially in terms of our national security as well.

My next two columns will cover recommendations for addressing those root causes, including the importance of properly implementing the Federal IT Acquisition Reform Act and the update to FISMA. ■

FCW Index

People

Agencies/Organizations

Advertisers

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

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

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

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

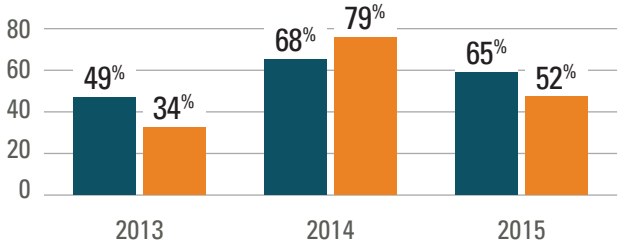
The shifting IT shopping lists

FCW's parent company polled 704 buyers of government IT and found surprising trends in the solutions being sought.

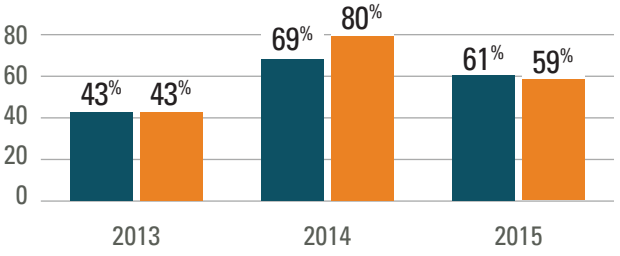
Percentage who plan to buy in the next 12 months:

DOD Civilian

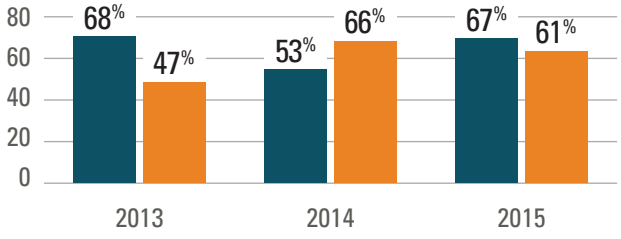
CYBERSECURITY



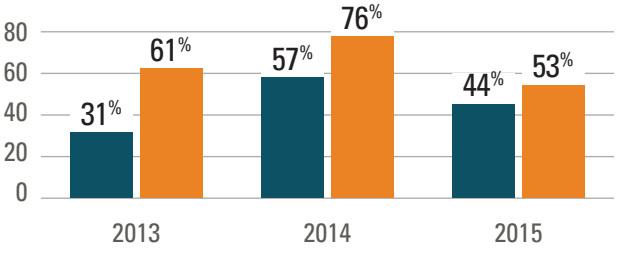
DATA CENTERS



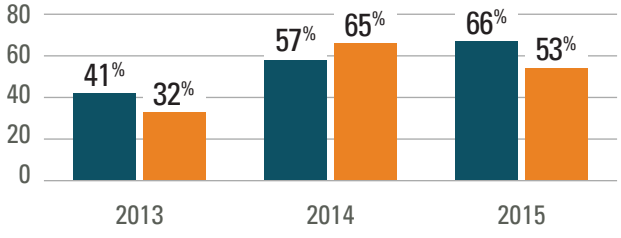
MOBILE/COMMUNICATIONS



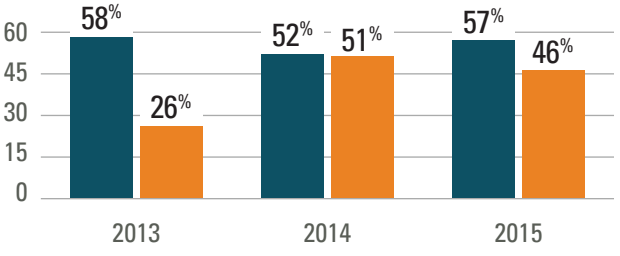
CLOUD/VIRTUALIZATION



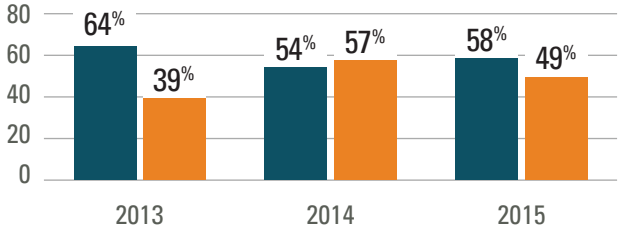
BIG DATA/ANALYTICS



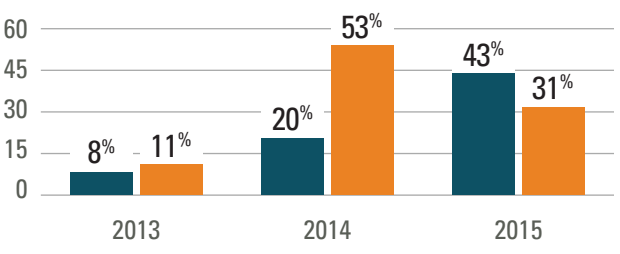
NETWORKING



STORAGE



HEALTH IT



Source: 1105 Public Sector Media Group's 13th Annual Government Technology Buying Study. To learn more about the report, contact Dana Friedman - 703.876.5078.

TRANSFORMING

Government IT

With Tegile Intelligent Flash Arrays, transform your data center with the flexibility of both disk and flash storage in one.

tegile

You need a storage solution that can strike the perfect balance between performance and economics. Tegile intelligent Flash Storage Arrays seamlessly integrate multiple types of storage media and employ an advanced flash-optimized software architecture to deliver 5x the performance of legacy storage arrays at one-third the cost.

- **5X LOWER LATENCY** compared to legacy storage array
- **5:1 DATA REDUCTION** in storage footprint in well-virtualized environments
- **5$ PER GIGABYTE** of high-endurance, enterprise grade flash
- **5 YEARS OF FRESH FLASH** with free controller upgrades
- **5 NINES OF AVAILABILITY (99.999%)**

INTELLICARE FLASH 5 GUARANTEE

tegile.com/government