

FCW

THE BUSINESS OF FEDERAL TECHNOLOGY

UNMANNED •

CYBER •

C4ISR •

LOGISTICS •

**THE VALUE OF
LEVERAGING
FULL-SPECTRUM
CYBER TO NEUTRALIZE
ENEMY THREATS.**

© 2015 Northrop Grumman Corporation

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

www.northropgrumman.com/cyber

OCTOBER 2015 • VOLUME 29 NUMBER 17





UNMANNED •

CYBER •

C4ISR •

LOGISTICS •

***THE VALUE OF
SECURING THE SEAS
BEFORE OUR SHIPS
LEAVE THE SHORE.***

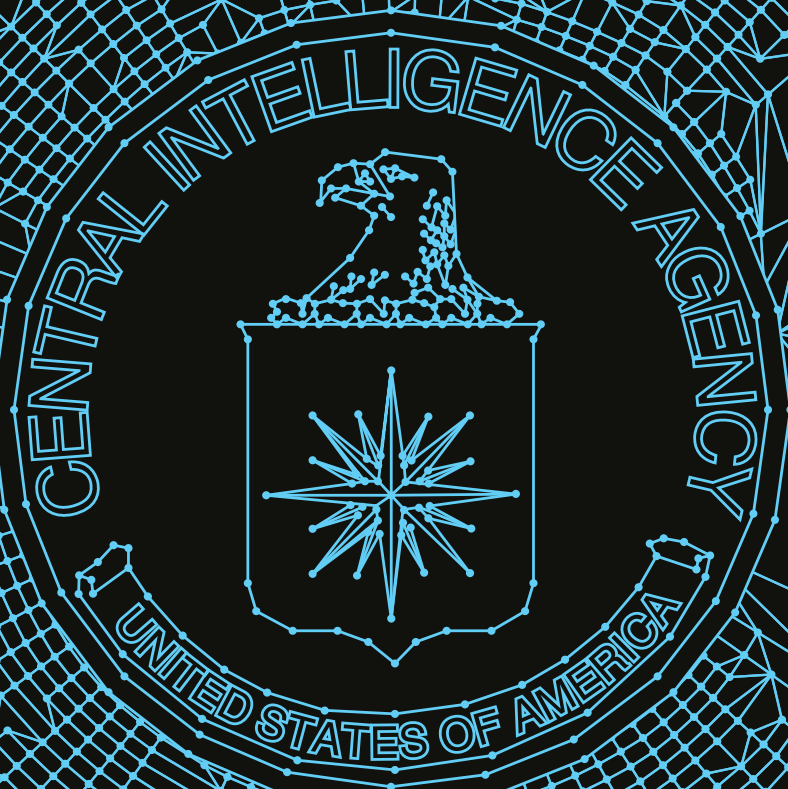
Today, the world's most advanced weaponry is taking new form. Northrop Grumman's expertise in every aspect of cyber is transforming the global battlefield. From resiliency to agile defense, we're providing an increasingly effective advantage in combating evolving threats and challenges. *That's why we're the leader in full-spectrum cyber.*

THE VALUE OF PERFORMANCE.

NORTHROP GRUMMAN

FCW

THE BUSINESS OF FEDERAL TECHNOLOGY
OCTOBER 2015 • VOLUME 29 NUMBER 17



INSIDE THE CIA'S **NEW DIGITAL DIRECTORATE**



An IT management
maturity model
for FITARA

PAGE 28

Big worries about
big data

PAGE 34

Take the complexity out of CDM.

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

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

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



Navy establishes permanent cyber division

The Navy is trying to get a handle on its cyberthreat exposure. But without a running tally of IT systems and the origins of their components, network operators don't know what's on or off and what's vulnerable or secure.

Navy officials want to build on the momentum of the yearlong Task Force Cyber Awakening to drive a lasting, secure cyber posture at the service. And so in September, the chief of naval operations established the Navy Cybersecurity Division, a 40-person office responsible for evaluating big cybersecurity investments and ensuring that policy requirements are met.

Troy Johnson leads the new cyber division. He spent 22 years as a cryptologist and information operations planner in the Navy and played an integral role in the cyber task force.

Vice Adm. Ted Branch, deputy chief of naval operations for information dominance, said one of the chief tasks for the new division's leaders will need to "make sure that they have the requirements right at the front end so we can bake in some of the cybersecurity, as opposed to having it bolted on like we have done up until now."

The task force was a deep dive into

the cybersecurity postures of the service's many components, from the Naval Sea Systems Command to the Space and Naval Warfare Systems Command. It set priorities for boosting resiliency and led the Navy to reallocate approximately \$300 million in its fiscal 2016 budget to help address cyber vulnerabilities.



"The expertise that needs to be resident in systems commands for design and engineering frankly isn't there yet."

— VICE ADM. TED BRANCH, NAVY

The task force came at "a time of need," Branch said during an Oct. 1 press briefing. "We had a lot going on without a lot of focus and pursuit of our 2013 incursion."

Branch was referring to a breach attributed to Iranian hackers of the Navy Marine Corps Intranet, the service's massive internal computer network. A months-long operation known as Operation Rolling Tide drove the hackers off the unclassified portion of NMCI and has become a blue-

print for the Navy's cybersecurity operations.

Task Force Cyber Awakening initially focused on the transport layer of Navy networks, where the 2013 breach had occurred, Branch said. Drawing on modeling done by experts at Johns Hopkins University, the task force ranked and prioritized vulnerabilities

on Navy networks and then suggested remedies. Officials later broadened the scope of the assessments to include weapons and facility systems.

The systems commands that contribute the building blocks of Navy networks need to mature, Branch said. "The expertise that needs to be resident in systems commands for design and engineering frankly isn't there yet, certainly not in the capacity that we need it to be," he added.

— Sean Lyngaas

FCW CALENDAR

11/5 Acquisition

ACT-IAC will host a discussion on "Overcoming the Challenges of Acquiring Agile Digital Services in Government," with acquisition experts from 18F, DHS and U.S. Digital Service. Washington, D.C.
http://is.gd/FCW_agile_acquisition

11/10 Cloud and mobile

EPA's Harrell Watkins, DHS' Robert Palmer and GSA's Stan Kaczmarczyk will speak at Washington Technology's Cloud and Mobility Industry Day. Falls Church, Va.
http://is.gd/WT_cloud

11/19 Public safety IT

DOD's Joseph Wassel and U.S. Marshals Service's Karl Mathias are among the speakers at AFCEA Bethesda's panel on trends in law enforcement and public safety IT. Bethesda, Md.
http://is.gd/FCW_law_IT

Contents



14 **CYBERSECURITY** Inside the CIA's new digital directorate

The CIA's Directorate for Digital Innovation brings together the agency's CIO shop, cyber capabilities and open-source intelligence

BY SEAN LYNGAAS

20 **ACQUISITION** Challenge.gov keeps eyes on the prize

The crowdsourcing site is opening doors to the federal market for problem-solvers, but can it be a vehicle for large-scale IT projects?

BY MARK ROCKWELL

TRENDING

3 CYBERSECURITY

Navy establishes permanent cyber division

FCW CALENDAR

Where you need to be next

7 MANAGEMENT

Congress vets DHS cyber reorg plans

8 THE HILL

John Boehner's surprising tech legacy

9 PEOPLE

FCW Insider news roundup

DEPARTMENTS

10 COMMENTARY

Next-generation IT governance

BY KRIS VAN RIPER AND JOHN TAYLOR

So many chiefs, so little coordination

BY DAVID WENNERGREN

22 DRILL DOWN

Decision modeling: A key to better government

BY DAWN LEVY

28 CIO PERSPECTIVE

Making FITARA matter: Tools for implementation

BY DARREN ASH AND RICHARD A. SPIRES

32 FCW INDEX

34 BACK STORY

The big worries about big data





Our plans may have surprising new ways to save.

It's Open Season — the time to explore health plans that could be a better fit for you and your budget. Consider plan options from UnitedHealthcare that include:

- Low-cost options
- No-cost annual checkups
- No-cost preventive dental care
- Virtual health visits and rewards for healthy actions

Learn more at uhcfeds.com.

Open Season runs from November 9 through December 14.



Not all health plans are available in all areas. Visit uhcfeds.com to find a listing of plans available in your area.
©2015 United HealthCare Services, Inc. Insurance coverage provided by or through UnitedHealthcare Insurance Company or its affiliates. Health Plan coverage provided by or through a UnitedHealthcare company. Virtual visits are not an insurance product, health care provider or a health plan. Unless otherwise required, benefits are available only when services are delivered through a Designated Virtual Network Provider. Virtual visits are not intended to address emergency or life-threatening medical conditions and should not be used in those circumstances. Services may not be available at all times or in all locations.



Editor-in-Chief Troy K. Schneider
Executive Editor Adam Mazmanian
Managing Editor Terri J. Huck
Staff Writers Sean Lyngaas, Zach Noble, Mark Rockwell
Contributing Writers Richard E. Cohen, Will Kelly, Carolyn Duffy Marsan, Brian Robinson, Sara Lai Stirland
Editorial Fellows Aleida Fernandez, Jonathan Lutton, Bianca Spinosa
Editorial Assistant Dana Friedman



Chief Operating Officer and Public Sector Media Group President
Henry Allain
Co-President and Chief Content Officer
Anne A. Armstrong
Chief Revenue Officer
Dan LaBianca
Chief Marketing Officer
Carmel McDonagh
Advertising and Sales
Chief Revenue Officer Dan LaBianca
Senior Sales Director, Events Stacy Money
Director of Sales David Tucker
Senior Sales Account Executive Jean Dellarobba
Media Consultants Ted Chase, Bill Cooper, Matt Lally, Mary Martin, Mary Keenan
Event Sponsorships Alyce Morrison, Kharry Wolinsky

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

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

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

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

Vice President, Art and Brand Design
Scott Shultz
Creative Director Jeff Langkau
Assistant Art Director Dragutin Cvijanovic
Senior Web Designer Martin Peace
Director, Print Production David Seymour
Print Production Coordinator Lee Alexander
Chief Revenue Officer Dan LaBianca

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

FederalSoup and Washington Technology
General Manager Kristi Dougherty

OTHER PSMG BRANDS

Defense Systems
Editor-in-Chief Kevin McCaney

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

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

Federal Soup
Managing Editors Phil Piemonte, Sherkiya Wedgeworth

THE Journal
Editorial Director David Nagel

Campus Technology
Executive Editor Rhea Kelly



Chief Executive Officer
Rajeev Kapur

Chief Operating Officer
Henry Allain

Senior Vice President & Chief Financial Officer
Richard Vitale

Executive Vice President
Michael J. Valenti

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

Chairman of the Board
Jeffrey S. Klein

SALES CONTACT INFORMATION

MEDIA CONSULTANTS

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

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

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

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

EVENT SPONSORSHIP CONSULTANTS

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

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

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

MEDIA KITS

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

REPRINTS

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

PARS International

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

LIST RENTALS

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

SUBSCRIPTIONS

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

REACHING THE STAFF

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

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

CORPORATE OFFICE

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

Congress vets DHS cyber reorg plans

Members of a key House panel agreed that a reorganization of the Department of Homeland Security's directorate in charge of cyber and physical security is overdue, but some lawmakers are concerned that Congress is not being kept in the loop.

DHS officials are considering a makeover of the National Protection and Programs Directorate that would include "cultural, governance and process changes" in how the directorate operates, said DHS Undersecretary for NPPD Suzanne Spaulding. She testified at an Oct. 7 hearing of the House Homeland Security Committee's Cybersecurity, Infrastructure Protection and Security Technologies Subcommittee.

The plan would empower the directorate's National Cybersecurity and Communications Integration Center, the 24/7 hub for analyzing and disseminating cyberthreat information, by giving the center its own office and aligning it with two multibillion-dollar DHS programs that have been deemed central to federal civilian cybersecurity: Einstein and Continuous Diagnostics and Mitigation.

Rep. John Ratcliffe (R-Texas), the subcommittee's chairman, and other lawmakers sent a letter to DHS in September complaining that they were being kept in the dark about the reorganization. The hearing was a chance to clear the air.

"Several members of the committee and I were very disappointed to learn about this proposal through leaked reports in the media," Ratcliffe told DHS officials at the hearing.

Spaulding said she would keep the subcommittee apprised of the reorganization plans and acknowledged that some changes to the directorate would require congressional approval.

The proposed NPPD shakeup reflects the Obama administration's ongoing quest to work more closely with the private sector on cybersecu-

rity challenges. For instance, a proposed NPPD infrastructure security office would offer training and assistance to owners and operators of critical infrastructure.

"Within NPPD, we need to take a holistic approach across cyber and physical risks," Spaulding said. The private sector increasingly takes such a view, which "reflects the world that they face, a world in which cyber and physical...are increasingly intertwined."

Acquisition is another focus area of the NPPD makeover plan. The department is "proposing an acquisition program management function to enable greater effectiveness and accountability in acquisition programs and ensure that operational programs have the tools required in a timely manner," Spaulding said in her prepared testimony.

That new function would help NPPD work with the department's Science and Technology Directorate on research and development, she added.

Chris Currie, a homeland security expert at the Government Accountabil-

ity Office, said DHS would be wise to consider how the reorganization will affect acquisition management.

"Our experience at DHS and other agencies has shown that it's often the management issues that can creep in as problems later on, after [reorganizations] are done, in areas like human capital and acquisition," he told lawmakers.

John Cohen, a former acting undersecretary for intelligence and analysis at DHS, told FCW that better aligning NPPD's cyber and physical security missions by encouraging coordination among field personnel is a worthy goal. "However, any reorganization should also clearly reflect how NPPD will work with other DHS elements," he said.

Cohen, who is now a professor at Rutgers University, added that DHS officials must also consider how NPPD interacts with "other federal organizations engaged in activities such as active-shooter response, private-sector outreach, cybersecurity and critical infrastructure protection."

— Sean Lyngaas

INK TANK



John Boehner's surprising tech legacy

Outgoing House Speaker John Boehner might be better remembered for public bouts of weeping and a private fondness for red wine and cigarettes. But as the Ohioan prepares to leave office amid a political struggle over the direction of the Republican caucus, it's a good time to reflect on a surprising aspect of his legacy: promoting open data in government.

"From the start of his speakership, Boehner has been a leader in pushing the house toward adopting structured data formats for legislation," Hudson Hollister, founder and executive director of the Data Transparency Coalition, told FCW.

Hollister is a former House staffer who helped draft early iterations of the Data Accountability and Transparency Act. He dreams of a day when legislative bills are linked and searchable, new legislation automatically updates the online text of the laws modified and federal dollars can be tracked from

appropriations through obligations to actual spending.

Boehner helped get the House closer to that vision, Hollister said.

Only a few months after taking over as speaker, Boehner joined then-Majority Leader Eric Cantor (R-Va.) in sending a letter to the Clerk of the House calling for open legislative data standards. It took three years, but the Boehner-Cantor team helped shepherd the Data Act into law.

Despite the bill's steep price tag — \$300 million over four years — Boehner rallied the House to pass the bill three times before the Senate finally took up the legislation.

Matt Rumsey, a senior policy analyst at the Sunlight Foundation, said, "Both sides of the aisle worked together" on data and transparency issues under Boehner's leadership.

Improving data quality is one part of Boehner's legacy, Rumsey added, while the openness of the House

itself is another. However, Rumsey acknowledged that "these issues are never going to rise to the level of public notice" that mainstream, hot-button issues enjoy.

"These policy changes are technical, they're not sexy politically, and yet they're so consequential when it comes to connecting Congress to the people they serve," Hollister added.

Boehner's leadership helped move those issues forward, but of course, government has a long way to go.

Agencies are still hashing out how they'll present financial information to the American people, Data Act definitions still need hammering out, and the House and Senate need to join forces on a unified data structure to reach the holy grail of sensible open governance, Hollister said.

But in the House, Boehner "laid the groundwork," Hollister said, adding that "the House is worlds ahead of the Senate" on the issues of recording, publishing and tagging video.

— Zach Noble



John Boehner

EDITOR'S NOTE

Help us find the heroes of federal IT

The nominations for the 2016 Federal 100 awards are now open. So please help the most exceptional women and men in our community get the recognition they deserve!

For more than a quarter-century, the awards have honored individuals who go far beyond their assigned duties to make a difference. The Federal 100 are the most prestigious awards in federal IT — for good reason. But it all starts with a great pool of nominees. So if you

know people you believe should be among the 2016 Federal 100, please make sure our judges know about them, too.



Not certain what it takes to make the Federal 100? Here are five points to remember:

1. Anyone in the federal IT community is eligible: career civil servants, political appointees, contractors, academics, even members of Congress.
2. The awards are for individual accomplishments in 2015.

3. Winners go above and beyond, whatever their level or rank. A fancy job title is not required, and just doing one's job well is not enough.
4. You can make multiple nominations. Do so early and often.
5. Impact matters. Tell us what a nominee did and what that work accomplished.

The deadline for submissions is Dec. 23. Go to FCW.com/2016fed100 for details, and get started on your nominations today.

— Troy K. Schneider
tschneider@fcw.com
[@troyschneider](https://twitter.com/troyschneider)

FCW Insider: People on the move

The Partnership for Public Service announced its Samuel J. Heyman Service to America Medals to eight public servants in recognition of their outstanding achievements and efforts to improve the lives of Americans and the global community.

Edward Hugler, deputy assistant secretary for operations at the Labor Department, received recognition for his work on securing sensitive economic data before its release to the public; preventing Labor's financial system from collapsing after its service provider's bankruptcy; and leading the creation of Benefits.gov, which links citizens to more than 1,200 government assistance programs.

Ron Ross, a fellow at the National Institute of Standards and Technology, was honored for developing the first set of unified information security standards and guidelines that aim to protect federal agencies from malicious actors and reduce operating costs.

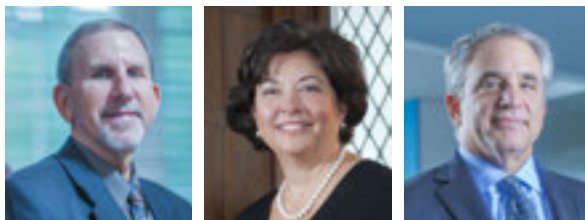
Ross also won GCN's Government Executive of the Year award. Accenture Federal Services CEO **David Moskowitz** took the industry honor, while NASA's New Horizons mission team won GCN's Tenacity Award for the decade-plus of IT planning and execution needed to make this summer's rendezvous with Pluto. More details on all the 2015 GCN Award winners are available at GCN.com.

The General Services Administration and the Defense Contract Management Agency were among the winners of this year's Excellence in Enterprise Architecture Awards, presented by FCW parent company 1105 Media, the Federated Enterprise Architecture Certification Institute and Zachman International.

GSA's application rationalization project, led by Chief Enterprise Archi-

tect **Kevin Wince**, trimmed 30 applications from the agency's portfolio and produced a nearly 1,600 percent return on investment. DCMA, led by Chief Enterprise Architect **Theon Danet**, was honored for its overall achievements in using EA, including its commitment to monitoring technology markets.

President Barack Obama named **Michael Missal** to take over the Office of Inspector General at the Department of Veterans Affairs. Missal, a partner at Washington law firm K&L Gates, has conducted internal investigations on behalf of corporate clients, including those in the financial services, government contracting and technology fields.



From left: Ron Ross, Martha Dorris, David Moskowitz.

VA's OIG has been without a Senate-confirmed leader since January 2014. Acting Director **Richard Griffin** stepped down in July amid charges that he whitewashed internal probes into allegations that personnel tampered with scheduling software at VA medical centers.

Former Department of Homeland Security CIO and current FCW columnist **Richard Spires** has been named CEO of Learning Tree. Spires has remained close to federal IT issues since he left DHS in 2013. He recently testified at a congressional hearing on the Office of Personnel Management data breach and is involved with ACT-IAC's efforts to develop strategies for implementing the Federal IT Acquisition Reform Act.

Renee Wynn took over as NASA's CIO in September. Before joining the

agency in July as deputy CIO, she worked for 25 years at the Environmental Protection Agency.

As NASA's top IT official, Wynn will focus on some of the same areas her predecessor, **Larry Sweet**, had stressed, including increasing collaboration among NASA's centers, strengthening the agency's IT security posture, and providing innovation through data analytics and visualization.

Martha Dorris, director of strategic programs at GSA's Office of Integrated Technology Services, told her staff that she will retire from government on Oct. 31.

Dorris, who took her first government job at age 18, told FCW that "GSA has been like my second home. I've grown up here." But she wants to try her hand in the private sector after 34 years of public service.

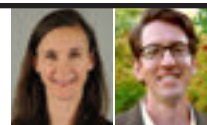
"I've had an entrepreneurial kind of mindset and spirit for a long time," she said. A firm of her own is on the drawing board — with customer experience, acquisition and digital service all part of the business plan.

Peter Tseronis, the Energy Department's CTO and associate CIO for technology and innovation, is leaving his post at the end of October. He has been a federal employee for more than 24 years and is a three-time Federal 100 award winner.

Venable has tapped **Ari Schwartz** to be the company's managing director of cybersecurity services. Schwartz is best known for serving as senior director of cybersecurity at the White House.

In his new role, Schwartz will provide cybersecurity consulting services to the firm and help clients understand risk management strategies, including implementation of the White House's Cybersecurity Framework, according to Venable.

— FCW staff



Next-generation IT governance

CIOs must find ways to nudge mission partners toward smarter investment decisions

The current IT environment's extensive business-led technology spending, multiple decision-makers and iterative planning cycles have stretched traditional IT governance to its limits. Although the core goals of good IT governance remain the same — alignment of investments with mission strategy, control over risk and efficient use of IT resources — the approaches used to ensure them must evolve.

A primary driver is the increasingly dispersed nature of IT spending and decision-making. In a recent TechAmerica survey of federal CIOs and chief information security officers, half of the respondents said the CIO controlled less than 50 percent of their agencies' IT spending. Additionally, CEB research shows that nearly 75 percent of business partners are willing to take ownership of their own IT projects.

Although business partners have a mission-led mindset when it comes to IT spending, the responsibility for ensuring its added value to the organization and adherence with data and security standards ultimately remains with the IT department.

Historically, IT governance oversight has relied on rigid processes, one-size-fits-all approaches and a single entry point for investment planning. In the new environment, those approaches can lead to over-investment in low-risk initiatives or delayed response to new opportunities, further intensifying public scrutiny of government IT.

Today's IT leaders instead should frame investment decisions in ways that encourage mission partners to adhere to good governance.

CEB research has identified key tactics to maximize returns from IT spending:

- **Allow different entry points.**

Instead of mandating a single point of entry for governance processes, IT should allow mission partners to

As IT's role in meeting organizational objectives increases, the need for adaptive and effective governance is more critical.

lead the investment process when the capabilities involved are localized and low-risk.

- **Present recommendations as trade-offs, not imperatives.**

IT typically portrays investment governance as a single standard based on technical needs, with little room for dialogue with business partners. A more productive approach frames those choices as a set of trade-offs with justification based on audience-relevant business outcomes. That facilitates better discussions around technology decisions and guides stakeholders to solutions

that are best for the enterprise.

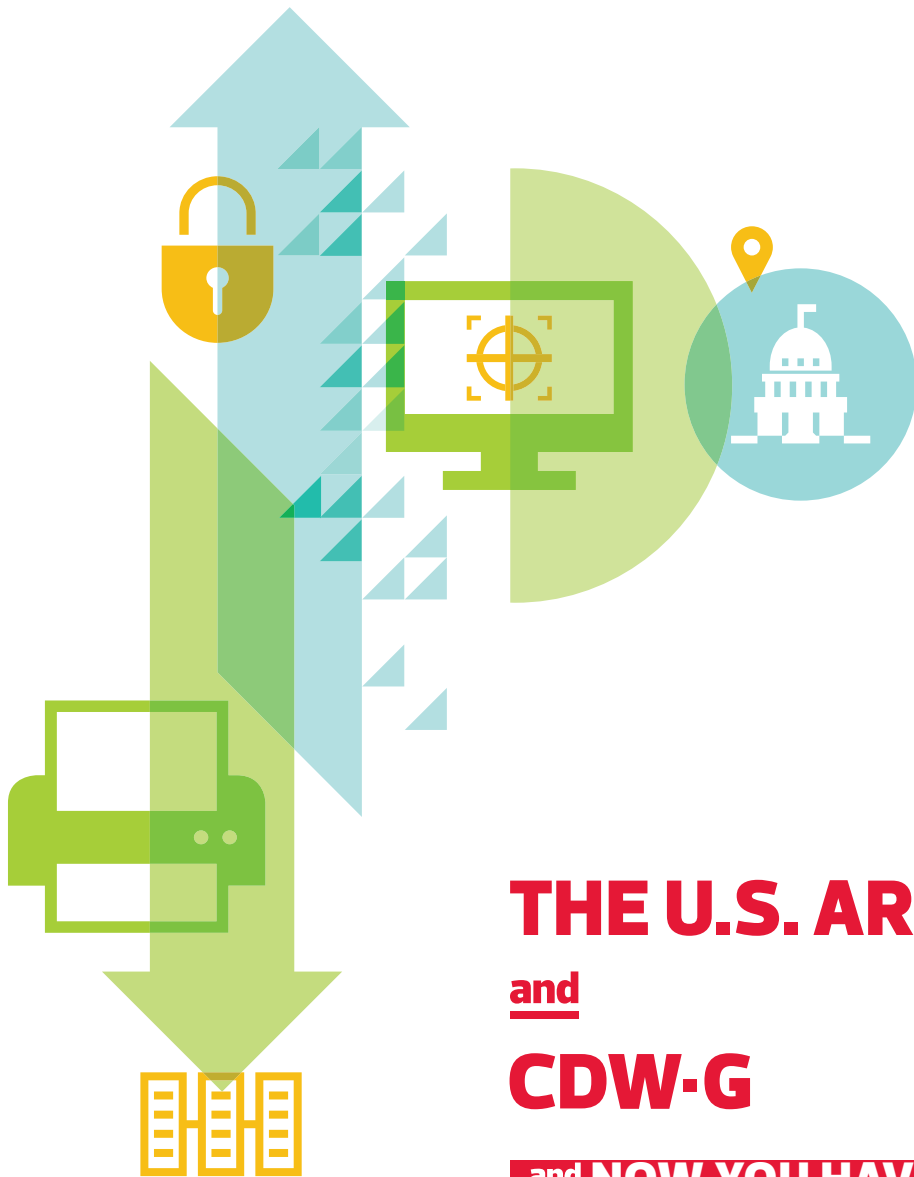
- **Minimize the burden of risk assessments through consolidation.**

Instead of repeatedly handing off risk assessments between various risk management functions, those functions should assess mission-led initiatives in parallel to speed the process. Today, a number of leading organizations are using self-service risk assessments that include interactive questions to triage initiatives that require the most attention and oversight, thereby reducing coordination costs for both stakeholders and IT.

- **Highlight continuing support requirements.**

Governance does not end when the investment is approved. IT must consider the complete life cycle and drive projects' end-of-life conversations with mission partners to avoid legacy burdens. By providing comparisons of operations and maintenance spending across mission units, business partners will have an enterprisewide view of demand. That increased transparency makes clear the ongoing costs and trade-offs involved in legacy support.

As IT's central role in meeting organizational objectives continues to increase, the need for adaptive and effective governance is more critical. By presenting mission partners with relevant options and trade-offs and reducing the level of effort required to meet governance standards, IT can ensure the success of investments, regardless of the funding source. ■



THE U.S. ARMY

and

CDW-G

**and NOW YOU HAVE
A PARTNERSHIP FOR
MISSION SUCCESS.**





IMPROVE YOUR STRATEGY WITH CDW-G.

From tactical missions to mission control, we have the technology you need for success.

We stand ready to help you safeguard combat forces with innovative technology that helps warfighters communicate from the most remote locations.

Desktops and Mobile Devices

From the latest desktops to high-performance mobile devices, we have the technology you need to keep productivity at an all-time high. Let CDW-G help you find the right devices for your needs.

Ruggedized Devices

Our wide selection of rugged, portable devices are designed to withstand even the harshest elements.

Document Processors, Printers and Accessories

Complete the solution with the latest printers, scanners and accessories to help you lower costs, improve efficiency and increase security across your organization.

CONTRACT OVERVIEW

Computer Hardware, Enterprise Software and Solutions (CHESS), in coordination with the Army Contracting Command (ACC) and the Rock Island Contracting Center (ACC-RI), awarded ADMC-2 to CDW-G to support the Army's requirements for Commercial Off-The-Shelf (COTS) products and services for purchase or lease.

CDW-G offers COTS desktops, portable and rugged systems, PDAs, Video Teleconferencing (VTC) products, printers, scanners, digital cameras, displays, transport cases and other related accessories, along with factory-orderable upgrades and related peripherals through the ADMC-2 contract.

CONTRACT INFORMATION

Issuing Agency:

Army Contracting Command – RI
1 Rock Island Arsenal
Rock Island, Illinois 61299

ACC-RI Contracting Office:

Contracting Officer: Joelle Donovan | 309.782.8582
Joelle.R.Donovan.civ@mail.mil

Computer Hardware, Enterprise Software and Solutions (CHESS):

Product Leader: Rick Klemencic | 703.806.9015
Richard.j.klemencic.civ@mail.mil

CHESS it e-mart:

<https://chess.army.mil>
888.232.4405
armychess@mail.mil

ADMC-2 CONTRACT ORDERING

Procedure highlights:

- Ordering is decentralized and is open to the Army, DoD, other federal agencies, Foreign Military Sales and authorized government contractors supporting these agencies.
- Non-DoD ordering offices must comply with the Economy Act prior to issuing orders against this contract.

Contract duration:

April 24, 2006–April 23, 2016

CDW-G ADMC-2 Sales Team:

CDWG.com/admc2
Contact your dedicated CDW-G account manager
866.371.2362 | admc2@cdwg.com
For quotes: admc2quotes@cdwg.com

CDW-G ADMC-2 Payment Information:

Contract number: W91QUZ-06-D-0003
Federal Tax ID number: 36-4230110
DUNS number: 026157235
Cage Code: 1KH72

Remit to address:

75 Remittance Dr., Suite 1515
Chicago, IL 60675-1515

Wire and EFT:

The Northern Trust Company
50 S. LaSalle St. | Chicago, IL 60675

Routing transit number:

Routing number: 071000152
Depositor account number: 91057

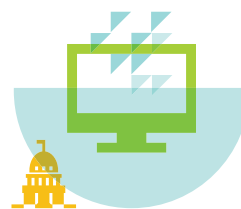
CDW-G ADMC-2 Program Management Office:

Kathy Gaston
Program Manager
703.621.8222
kgaston@cdwg.com

CDW-G Warranty/Tech Support

800.678.7220 | admc2support@cdwg.com

TECHNOLOGY TO DELIVER THE EFFICIENCY YOU NEED.



SAMSUNG BUSINESS

Samsung® S24E200BL 23.6" SE200 series LED monitor

- VESA® mount compatibility, VGA and DVI™ connections and speaker bar compatibility
- LED-backlit LCD screen delivers sharp, bright and beautiful images
- Mega infinity dynamic contrast ratio helps to ensure subtle detail even in the lights and darks
- Sleek, stylish design and low-profile stand take up less desk space and contribute to a cleaner-looking office



HP LaserJet® Enterprise 500 MFP M525dn Monochrome laser multifunction printer

- Mfr. print speed: up to 42 ppm
- Printer resolution: 1200x1200 dpi
- Duty cycle: 75,000 impressions
- 600-sheet capacity
- 8" color touch-screen display
- Preview, edit and zoom images prior to scanning



Lexmark

Lexmark™ MS610dn Network and duplex-ready mono laser printer

- Mfr. speed rating: up to 50 ppm
- Duty cycle: up to 100,000 pages per month
- 650-sheet standard paper input
- Paper saving, automatic duplex



Xerox® Phaser® 6700Dn This color printer accelerates work group productivity, giving you more time to focus on what matters most

- Mfr. printing speed: up to 47 ppm
- Max. resolution: up to 2400 dpi
- Duty cycle: up to 120,000 pages per month



ORDER FROM THESE LEADING BRAND-NAME MANUFACTURERS:

Belkin

Black Box

Brother International

Canon

Cherry

Dell

Epson

Fujitsu

Getac

Hardigg

Hewlett-Packard

InFocus

Kodak

Lenovo

Lexmark

Mitsubishi

Motion Computing

NEC

Nikon Inc.

Panasonic

Plantronics

Polycom

Ricoh Corporation

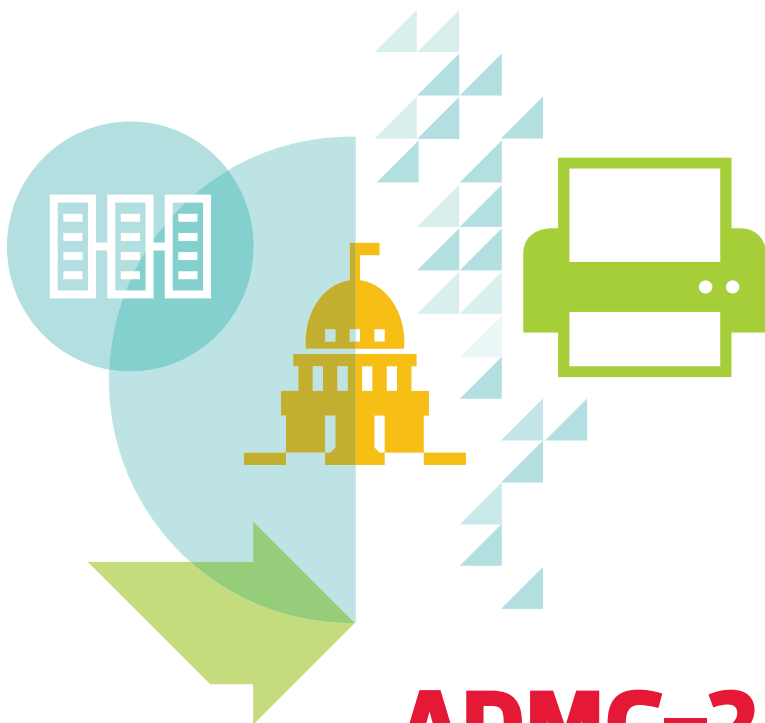
Samsung

Sharp

Targus

Xerox

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



ADMC-2 **and** **CDW-G**

**THE TECHNOLOGY FOR
TODAY'S CHALLENGES.**

Partner with CDW-G and ADMC-2 to get
the right technology for mission success.

For more information please call 866.371.2362
or visit us online at CDWG.com/admc2

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





So many chiefs, so little coordination

The growing number of roles with “chief” in the title are complicating governance and security efforts, especially when they bypass the CIO

Governance is hard. Even worse, its success hinges on a willingness to have crucial conversations about leaders’ expectations and outcomes. And as Kerry Patterson, Joseph Grenny, Ron McMillan and Al Switzler note in their book “Crucial Conversations: Tools for Talking When Stakes are High,” we are neither comfortable nor skilled in the art of such discussions.

The Navy, for instance, has surveyed senior military and civilian leaders and found that they tend to be control freaks who dislike and sometimes avoid crucial conversations about personnel-related issues.

So when we look at federal IT governance, it shouldn’t surprise us that agencies find it easier to invite someone else to the table when a new issue arises rather than directly address what’s not working. The result is a proliferation of “chiefs” in federal information management. Unfortunately, merely creating more chiefs doesn’t ensure alignment of effort across all the chiefs at the agency.

In other words, surprised? No. Concerned? Yes.

The Federal IT Acquisition Reform Act tries to address the roles of CIOs in federal agencies by requiring a relationship between bureau-level and agency-level CIOs. Although you’d be hard-pressed to conclude that CIOs at subordinate components don’t need to be in alignment with the agency CIO, the move is applauded more at agency HQs than within the bureaus.

And as though the reporting relationships between CIOs weren’t enough of a challenge, federal IT leaders now also must deal with a proliferation of other chiefs in the information management space — chief data officers, chief information security officers, chief knowledge officers, chief privacy officers, etc. And of course, if the position is important enough to warrant “chief”

It’s disconcerting to think that a chief data officer can work independently of the CIO.

in the title, then the natural inclination is to have that person report to the agency head. And this is where the trouble starts.

If agency alignment and execution suffer when subordinate CIOs are not beholden to the agency CIO, it is even more troubling if all of these new chiefs don’t have to be in sync with the CIO.

In the case of an agency creating a chief data officer position that reports directly to the agency head, it’s disconcerting to think that the data officer can work independently of the information officer. That split ensures bureaucratic stovepipes or, worse, is an indicator that despite the efforts of the Clinger-Cohen

Act and FITARA, some still define CIO as “computing infrastructure officer.” That is a tragic waste of a senior position because all substantive IT issues today require a chief who can focus on people, processes and technology.

Even more shockingly, some argue that chief information security officers should be independent of the CIO. That assertion confuses the important role of red teams, penetration testing and independent audits with the fundamental reality that if the person defending the network is detached from the person delivering information to the organization, the agency will suffer from a lack of accountability when information doesn’t flow and the mission’s not accomplished.

That bifurcation also seriously obstructs the important goals of getting security baked into IT solutions and replacing security based on denial of service with secure information sharing.

As George Labovitz and Victor Rosansky noted in their groundbreaking book, “The Power of Alignment,” “Sustained excellence emerges when all the key elements of a business are connected to each other.... You must create alignment between people, customers, strategy and process.”

It is hard enough to get things done in today’s federal environment; there’s no reason to make it harder by encouraging independent operators who further complicate governance. ■

SNAPSHOT

SOFTWARE-DEFINED PLATFORMS

Software-defined platforms define future of virtualization

As the Federal government has pushed the mantra of “more bang for the buck,” virtualization has become an accepted way of doing IT. Server virtualization is transforming the data center environment.

Software managed IT environments are now seen as a large part of the future. Software-defined networking (SDN) is an emerging practice. Software-defined storage (SDS) is quickly gaining pace. Software-defined data centers are just over the horizon.

Inevitably, that has led to thoughts about software-defined anything (SDx). As the dependency on physical hardware is reduced, so the thinking goes, software can manage entire environments. And that vastly increases IT flexibility and agility.

What once took days, weeks or months to set up and configure with physical IT can be deployed in hours, minutes or, in some cases, seconds with the virtualized world of SDx. It's also much easier to match those resources to the requirements, doing away with the costly over capacity that often has to be built in to physical environments to ensure capacity for expected future demand.

SDx is certainly more concept than reality right now, but the idea is quickly gaining ground. In 2014, market researcher Gartner listed SDx as of the 10 top technologies to watch and include as part of strategic planning.

Likewise, the Institute of Electrical and Electronics

Other Virtualization Report Articles:



- **Virtualization Helps Agencies Reach IT goals**
- **The promise of containers**
- **Service virtualization could be big for DevOps**
- **Virtualization security: The good and the bad**

FCW.COM/2015SNAPSHOTVIRTUALIZATION

Engineers (IEEE) Computer Society said interoperability issues and standards for SDx would be a top priority for 2015. Various standards groups such as the Open Networking Foundation, the Internet Engineering Task Force and the International Telecommunication Union are already working on the specs.

Government agencies are dipping their toes into specific software-defined technologies. The Defense Information Systems Agency (DISA) has set up a software-defined network working group. It included money in its FY 2016 budget request to launch pilot programs to see how Defense Department networks can use SDN. Other funds would be used to develop a Technology Environment to evaluate and characterize new technologies, including SDx.

Researchers at the Idaho National Laboratory (INL) have already gone further. They've developed a proof of concept to see how to apply SDx to the laboratory's business environment. It emulated the use and security of INL business systems accessed by

a large number of virtual machines, with software providing control intelligence that would otherwise be embedded in hardware.

In a recent issue of Government Computer News (sister publication to Federal Computer Week), Wayne Simpson, INL innovation architect, and research scientist Tammie Borders, described how the prototype solution they developed showed SDx “can be used to improve security, repeatability of process and consistency in results.” They concluded that by adopting SDx approaches, organizations could reduce employee workload, improve security controls and optimize existing IT investments.

“As the dependence on hardware for the intelligence to implement access and security controls diminishes, organizations must overcome traditional thinking and drive changes in regulatory restrictions,” according to Simpson and Borders. “As these challenges are addressed, SDx will become more widely adopted and will change how information is accessed and consumed worldwide.”



THE CLOUD

and

CDW-G

Today, government leaders aren't just looking at how to get to the cloud, but also, how to get the most out of it.

CLOUD ADOPTION ON THE RISE



\$3 BILLION

Amount spent by the federal government on cloud computing in 2014.



5X

SaaS adoption has more than quintupled in the past four years.



35%

of IT services are currently delivered via the cloud.



721

The number of cloud-based services the average public-sector organization uses.

SOURCE: ¹IDC Government Insights, Perspective: Looking Up – U.S. Federal Cloud Forecast Shows Sustained Growth Through 2018, September 2014 ²CDW, Cloud 401: Navigating Advanced Topics in Cloud Computing, February 2015 ³Source: North Bridge and Gigaom Research, The Future of Cloud Computing, June 2014 ⁴Source: Skyhigh Networks, "Cloud Adoption & Risk in Government Report," February 2015

THE CDW-G APPROACH

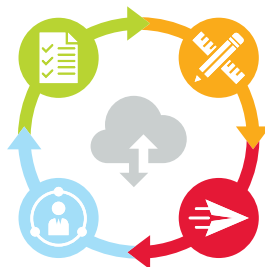
Our end-to-end cloud services are designed to help you navigate the complexities at every stage of your cloud deployment. You'll get personalized service designed and delivered by our experts and backed by our exclusive industry partnerships.

ASSESS

We start by conducting an assessment of your existing systems to better understand them and to identify areas of opportunity for improvement.

MANAGE

Our full lifecycle management support gives you more time to innovate and focus on critical tasks.



DESIGN

Our expert solution architects and engineers work with you to identify the solutions to solve your organization's specific goals, aligning with your budget and timelines.

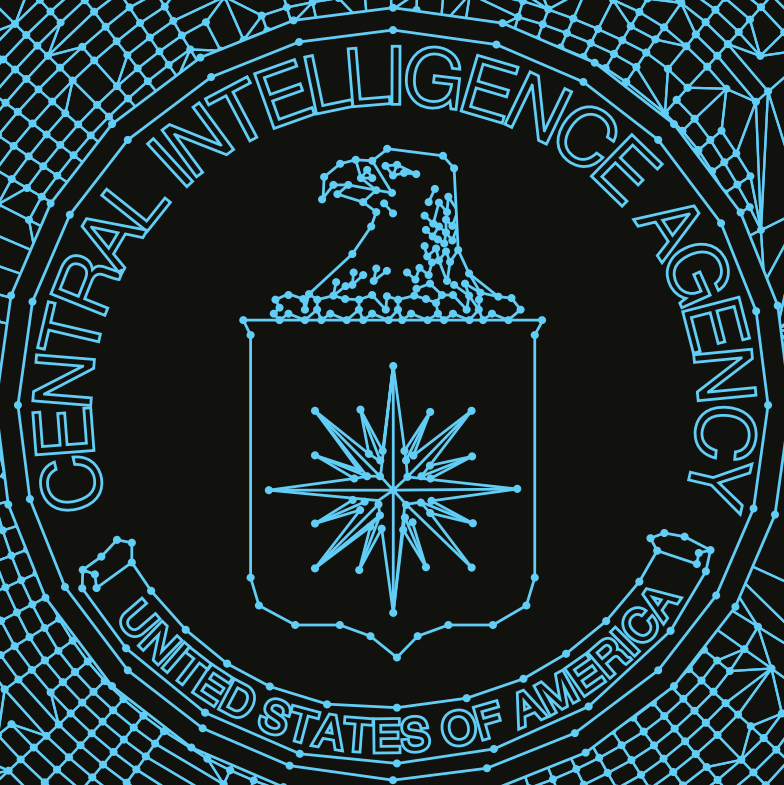
DEPLOY

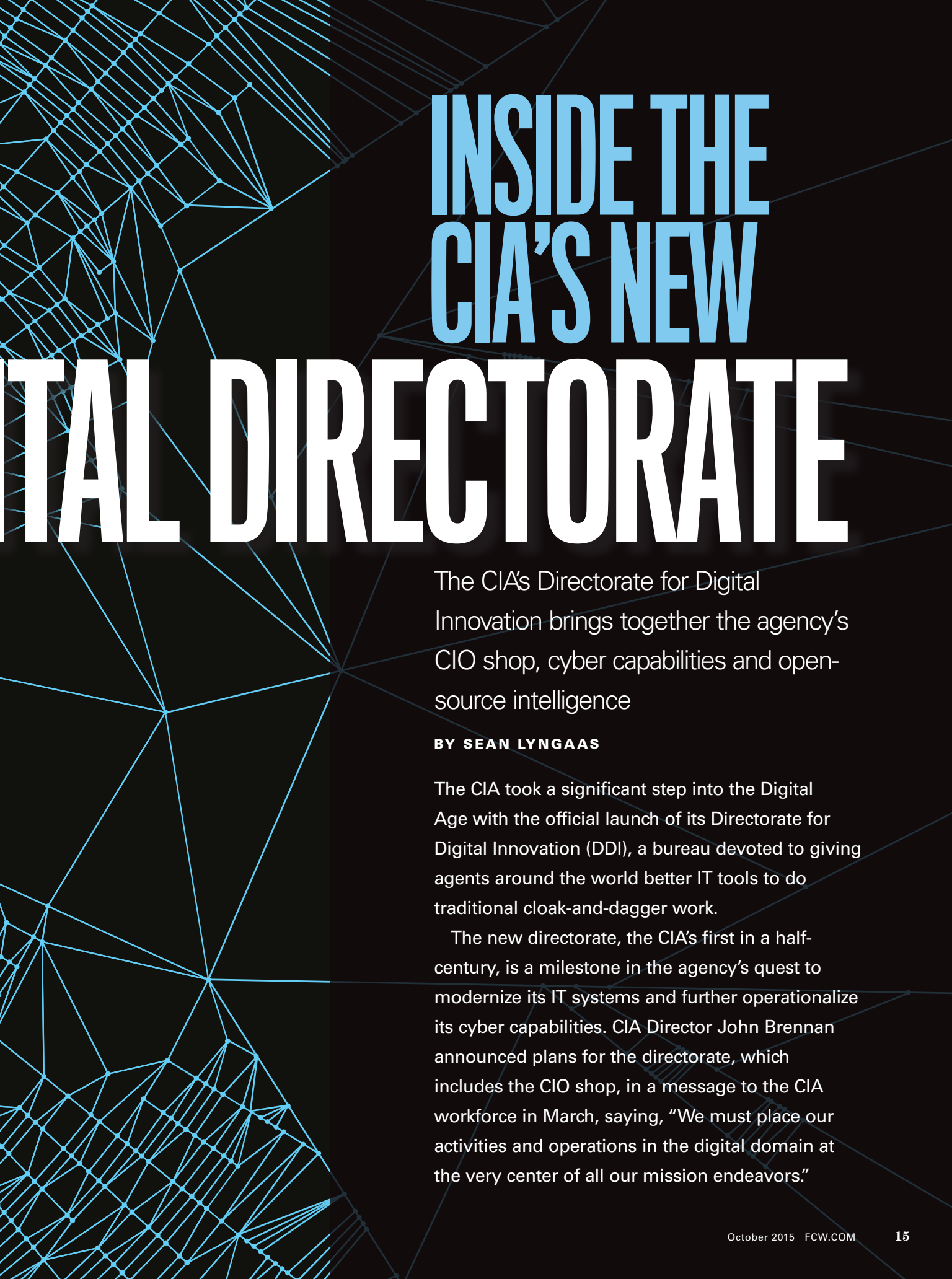
We can implement your new solution to help ensure successful integration.

For more information on our cloud offerings, visit CDW-G.com/cloud



DIGI





INSIDE THE CIA'S NEW DIGITAL DIRECTORATE

The CIA's Directorate for Digital Innovation brings together the agency's CIO shop, cyber capabilities and open-source intelligence

BY SEAN LYNGAAS

The CIA took a significant step into the Digital Age with the official launch of its Directorate for Digital Innovation (DDI), a bureau devoted to giving agents around the world better IT tools to do traditional cloak-and-dagger work.

The new directorate, the CIA's first in a half-century, is a milestone in the agency's quest to modernize its IT systems and further operationalize its cyber capabilities. CIA Director John Brennan announced plans for the directorate, which includes the CIO shop, in a message to the CIA workforce in March, saying, "We must place our activities and operations in the digital domain at the very center of all our mission endeavors."

With that mantra in mind, DDI Deputy Director Sean Roche and DDI Director Andrew Hallman have laid the groundwork to carry out the directorate's core mission of accelerating the next generation of digital solutions, as Roche put it. The directorate has been operating for months, but on Oct. 1, it formally came out of the shadows.

The directorate's goal is to provide CIA analysts with a "wide range of cyber options in the initial trade space" to help them solve problems earlier in the intelligence cycle, Roche told FCW. That means, among other things, locating and understanding the "digital dust" left behind by actors in the cyber domain. It is an open question whether the new directorate will serve as a platform for offensive operations.

There are three key components to DDI: an open-source center; a center for handling cyberthreats and operations; and the agency's IT enterprise, led by CIA CIO Doug Wolfe, whom Roche described as the Elon Musk of the agency.

The directorate is focused on the promise of data, with the goal of providing mission centers worldwide with greater insights from analytics. Roche said he is already seeing a payoff for the mission centers.

The directorate's foundation is the agency's Information Operations Center, which analyzes foreign threats to U.S. computer systems. IOC has been the traditional enclave for

IT experts at the CIA, but the agency now seeks to infuse that expertise into pretty much everything it does.


Retired Gen. Michael Hayden, who was CIA director from 2006 to 2009, told FCW that getting the digital directorate up and running was a matter of waiting until IOC's digital capabilities had sufficiently matured. "Once you get it to a certain level of maturity, then you can more productively disperse it and embed it into other activities," he said.

Now that capability is out the door, and DDI has already dispatched some of its officers to embed in mission centers overseas, Roche said.

Aggressively retiring legacy systems

Brennan likes to talk about moving the CIA into a new digital era, but just how IT-savvy is the agency? According to current and former officials, the CIA is grappling with legacy IT systems and will find it challenging to get innovative technology into the hands of officers.

"For security, cultural and occasionally budgetary reasons, it's safe to say CIA was never at or even near the cutting edge in information technology," former CIA official Stephen Slick told FCW. And although the CIA has a storied history in science and technology, "this institutional prowess...rarely translated to the individual officer's worksta-



**THE INFORMATION
OPERATIONS CENTER IS
NOT "AN ALTERNATIVE
NSA. IT'S USING A NEW
CAPACITY TO DO WHAT
CIA HAS ALWAYS DONE,
WHICH IS CLASSIC
ESPIONAGE."**

Former CIA Director Michael Hayden

tion, and that will be a challenge for the new directorate,” said Slick, who is now director of the Intelligence Studies Project at the University of Texas at Austin.

The task of getting the latest technology to agents will potentially be compounded by a loss of trust between the intelligence community and the private sector after Edward Snowden’s revelations about government surveillance.

“CIA, [National Security Agency] and other agencies will continue to labor into a headwind on digital technology until a new, more cooperative, more rational relationship develops between the government” and the private sector, Slick said.

The more tangible task of modernizing the CIA’s IT infrastructure could also prove difficult.

Roche said the CIA currently has a number of legacy processes and systems that have not kept pace with innovation. “You have to very aggressively retire legacy systems” and cannot do it gradually, he said, adding that the directorate is assessing how best to use in-house contractors. “I’d rather have [some of those contractors] sitting side-by-side with us writing code” than maintaining legacy systems, Roche said.

When Hayden was CIA director, he asked a handful of private-sector executives to review the agency’s IT posture. The outside advisers, which included former Hewlett-Packard CEO and current Republican presidential hopeful Carly Fiorina, concluded after several months of study that the agency’s IT is pretty good, but “you’re paying probably twice as much as you actually should be paying for it,” Hayden said.

Roche, for his part, will be watching to see if the new directorate reduces the time it takes the agency to deploy new applications. A challenge is understanding the “trade-craft” involved in hosting software across an enterprise, he said, adding that CIA personnel working in counterintelligence, for instance, stand to benefit if the directorate can get that project right.

Given Wolfe’s prominence in the new directorate, it is no surprise that, according to Roche, DDI is intended to be a key facilitator of the Intelligence Community IT Enterprise, an ambitious, cloud-driven quest for a single IT architecture for the community. He described the broad trend of organizations adopting more cloud computing as inevitable.

Working with Fort Meade

With news of Brennan’s plans for enhancing the agency’s cyber capabilities came questions about how the revamped CIA would interact with NSA, whose more robust cyber capabilities have been matched with greater funding. The CIA requested \$685.4 million for computer network operations in fiscal 2013, compared with the \$1 billion requested by NSA, according to a classified budget Snowden shared with the Washington Post.

The CIA has tended to use its cyber access to act, while NSA has focused on observation, Hayden said. That has at times created a tension during operations that has had to be defused through a formal process that Hayden said he oversaw when he was NSA director.

Nonetheless, the CIA’s Information Operations Center is uniquely tailored to the agency’s needs, he said, adding that IOC is not “an alternative NSA. It’s using a new capacity to do what CIA has always done, which is classic espionage.”

Susan Gordon, former IOC director and former senior adviser on cybersecurity to Brennan, said the NSA/CIA relationship in cyberspace is not so much “bigger brother and little brother” because they are driven by different missions.

The CIA’s mission is broader than that of NSA or the National Geospatial-Intelligence Agency, where Gordon is now deputy director. The CIA’s drive to modernize was therefore always going to cut a wider path and potentially raise questions about overlapping missions.

The CIA also sometimes supplements NSA’s cyber work with its own human spying, according to journalist Shane Harris. For example, the CIA’s Technology Management Office has helped an elite NSA hacking unit known as Tailored Access Operations break into computer networks to conduct cyber espionage, Harris reported in his book “@War.”


When asked if the new directorate’s mandate includes offensive cyber operations, Roche declined to comment, and Hayden would only say, “That would seem logical.”

Bringing digital personalities to Langley

Part of the rationale behind the new directorate is getting agency employees to immerse themselves in the online world rather than compartmentalize their interaction with it. Before the directorate, “CIA guys were kind of checking their digital personalities at the gate, and they had to be kind of different people inside the fence line than they were outside the fence line,” Hayden said. By contrast, DDI is meant to “allow the digital culture to permeate everything CIA does.”

The new directorate’s mission includes overseeing the career development of the agency’s cyber professionals to nurture “the next generation of digital-savvy leaders” at the CIA, Roche said.

Transforming the agency workforce for the Digital Age will be a tall but rewarding order, Slick said. “CIA’s most significant, and lasting, challenge will inevitably prove to be cultural as a workforce pursuing multiple missions adapts to a fundamentally changed global information environment,” he said. “When CIA’s culture fully embraces the Digital Age, the agency is likely to identify and exploit at least as many new opportunities as it will encounter risks.” ■



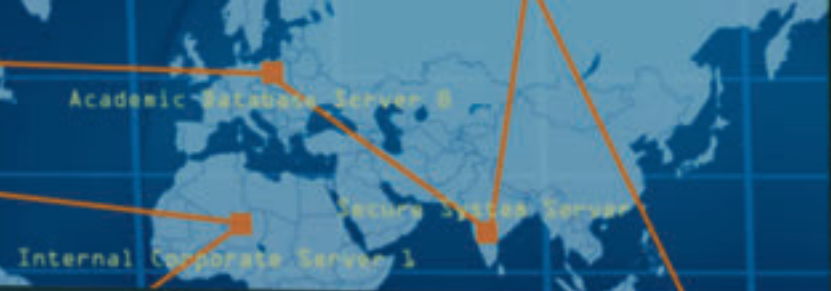
ENDING SECURITY

Content Management & Analysis

.....
Network & Information Security

.....
Mission Operations

.....
Critical Infrastructure & Borders



Challenge.gov keeps eyes on the prize

The crowdsourcing site is opening doors to the federal market for problem-solvers, but can it be a vehicle for large-scale IT projects?

BY MARK ROCKWELL

Like any five-year-old, Challenge.gov is eager to explore new things. The General Services Administration's pay-for-performance crowdsourcing portal is designed to inject innovation into the acquisition process, but it is finding that some activities are just too complex for this early stage of life.

The White House added Challenge.gov to the contracting mix in 2010 to offer a nontraditional path into the federal marketplace. The site lists competitions that seek to solve federal agencies' IT and technical challenges. They offer cash rewards to the most innovative private- and public-sector experts, who can craft technical solutions without having to invest in development or staffing.

"Instead of paying first and hoping a solution is delivered, GSA's approach minimizes risk and encourages creativity by inducing dozens and sometimes hundreds of potential solutions and leaving the government agency free to pick the best before delivering a reward," Kelly Olson, senior innovation adviser and director of Challenge.

gov, told FCW. "It's an approach that opens up space for individuals and smaller businesses to shine in a sector often crowded out by big companies."

She said the platform is a success. In a September blog



[GSA's approach] opens up space for individuals and smaller businesses to shine in a sector often crowded out by big companies.

— KELLY OLSON, CHALLENGE.GOV

post, she noted that about 80 agencies have used it for more than 440 challenges, with total prizes topping \$150 million.

About 200,000 problem-solvers — a mix of entrepreneurs, budding citizen scientists, students and others — have participated in the challenges to solve important

Top Challenge.gov competitions in fiscal 2014

PROJECT	AGENCY	TOTAL PRIZE
SunShot Prize: Race to 7-Day Solar	Energy	\$10,000,000
Cyber Grand Challenge	DARPA	\$9,750,000
Rebuild by Design	HUD	\$2,000,000
SunShot Catalyst Program	Energy	\$1,005,000
National Clean Energy Business Plan Competition	Energy	\$600,000
Food Safety Challenge (2014)	FDA	\$500,000
Follow that Cell	NIH	\$500,000
No-Petri-Dish Diagnostic Test Challenge	CDC	\$200,000
American Energy Data Challenge	Energy	\$170,000
Predict the Influenza Season Challenge	CDC	\$75,000

local, national and global problems, said Olson, who's been leading Challenge.gov since January.

Over the summer, federal agencies posted more than 20 new challenges, including apps that use open data to help farmers and algorithms that could help detect electromagnetic pulses and predict earthquakes, she added.

Despite the successes, however, some observers are skeptical that the site has actually improved innovation in federal acquisition. Others said gauging its impact requires metrics more subtle than the total number of participants.

"It's a tough question," said Roger Waldron, president of the Coalition for Government Procurement, when asked if Challenge.gov has had a significant impact on the way federal agencies acquire IT services. "The things being done are on a small scale," and to have an optimal impact, such efforts must have a larger strategic mission.

One federal CIO told FCW on background that the program was not really made to develop intricate replacements for legacy IT projects, but it could offer quick solutions and produce new, more user-friendly interfaces for those larger systems.

"[Although] you can do challenges for a better user interface to the old systems, the old system itself eventually needs hard work to get the data out and make sense of where business processes need to be re-created on a new cloud platform and things like that," the CIO said.

Olson said users do come to Challenge.gov to develop solutions for large-scale IT projects, and she's working

hard to get challenges that go beyond logo redesigns, photo competitions and other relatively straightforward solutions.

Nevertheless, she acknowledged that bigger projects present a potential problem. For one thing, agencies might not want to publicly offer Challenge.gov participants the kind of detailed look into internal operations that would be required for enterprisewide IT solutions.

However, Olson said, officials are working with GSA's Federal Risk and Authorization Management Program — which provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services — to find an open-source tool for quality checks of FedRAMP documentation.

The tool will automate a manual review process that can take more than 40 hours to complete and will cost a fraction of a traditional procurement.

In addition, it will take significantly less time to develop and tap into a broad public network of participants, according to Olson.

In the meantime, Challenge.gov is due for some change itself.

"In five years, Challenge.gov will be a broader umbrella across government," she said. It will offer new crowdsourcing, open-source and innovative solutions for agencies. The program is also adding a mentorship program that will tap 16 people working at various agencies for specific expertise, such as legal issues, prize design and other capabilities. ■

Decision modeling: A key to better government

Business decision logic is a type of data, and it's time agencies started treating it that way

BY DAWN LEVY

Tradition is good, but efficiency is better. In an annual report released in April, the Government Accountability Office examined fragmentation, overlap and duplication among government programs and identified 440 actions that agencies and Congress could take to improve operational efficiency and effectiveness.

Similarly, the Office of Management and Budget's Digital Government Strategy strives to improve IT efficiency and effectiveness for the American people. A key tenet of the strategy is ensuring that data and content are accurate, available and secure. The strategy further emphasizes the need to treat all content as data.

Experience shows that a major cause of IT inefficiency is the continual rebuilding of hard-coded, decision-based systems. Business decision logic is a type of data, but unlike traditional data elements that are stored and managed in databases, it is typically hard-coded into software.

Modifying software to reflect changes in business decision logic is costly, cumbersome and slow. Yet hard-coded software systems dominate government IT.

Those systems are largely developed by third parties under large, complex and risky contracts with lengthy software development life cycles. And until recently, hard-coding decision logic was the only option.

Moreover, compartmentalized agencies have traditionally lacked the

Modifying software to reflect changes in business decision logic is costly, cumbersome and slow. Yet hard-coded software systems dominate government IT.

incentive to coordinate system investments enterprisewide. As a result, government systems are often overlapping, fragmented or duplicative.

The trend toward standardization

A contrasting approach exists that would reduce operating costs, increase response times and improve

accuracy while empowering internal analysts and experts. Government agencies would rely on those internal decision-makers to centrally govern decision logic, with minimal technology labor. The need to continually rebuild hard-coded, decision-based systems would diminish. This prevailing alternative is known as decision modeling.

An interim step on the way to true decision modeling implementation might be rules engines, which could resolve some technical challenges by doing away with the hard-coding paradigm. However, rules engines without decision models would do little to overcome the superfluous developer costs associated with continual software rebuilds. Moreover, decision models would not replace rules engines because the two are complementary.

In fact, decision models are easy to automate in today's rules engines, so those models increase the value of rules engines. (This is because a new, agile life cycle exists from a business analyst-created decision model directly to rules engine code, with minimal IT intervention.)

Two decision modeling frameworks

Tracks Include



ACQUIRE

Acquisition & Management Show

Coming June 2016!

20
16

JUNE
8-9

WALTER E. WASHINGTON
CONVENTION CENTER
WASHINGTON, DC

Exhibit space is now available!

Contact Stacy Money for pricing & details

smoney@1105media.com 415.444.6933

ACQUIREshow.com

exist. The Decision Model, invented by Barbara von Halle and Larry Goldberg in 2011, has been successfully adopted by insurance and banking firms, and continues to spread throughout the financial industry.

The Decision Model and Notation standard, published by Object Management Group in 2014, enables organizations to access and share centralized business decisions using a common tabular format. A short list of vendors on the group's DMN committee includes IBM, Oracle and FICO. Von Halle and Goldberg were also key contributors to the specification.

Both models are suitable for government, and both exemplify the trend toward standardization of decision management.

The benefits of decision modeling

Decision modeling extracts complex business logic from software systems and allows internal business experts to manage the logic in a central repository. Business decision tables are two-dimensional and organized into simple conditional statements that result in a single conclusion. The tables are managed in a structured repository and are intuitive to maintain as the underlying policies and regulations change.

Most important, the logic in decision models is expressed in business-friendly (not technical) terms that are defined by business people and linked behind-the-scenes by technical people to actual data sources. That approach has proven invaluable. It means decision models are truly a technology-agnostic and business-aware deliverable. It means the same decision model can operate against more than one data source without any changes. And it means a data source can be replaced with a new one without making any changes in existing decision models.

Decision models are independent of data sources and independent of target technology. They are purely business driven and deploy anywhere and to many places, if need be.

In short, decision models are independent of data sources and independent of target technology. They are purely business driven and deploy anywhere and to many places, if need be.

Rob Lux, Freddie Mac's executive vice president and CIO, wrote in a 2013 blog post that, by using a decision model, it took Freddie Mac "only 17 days to write, test and deploy the 100-plus rule changes comprising Hurricane Sandy disaster relief policies for the systems lenders use to sell and service Freddie Mac mortgages. This is about 90 percent less time than it took to operationalize policy changes following disasters like Hurricane Katrina or the 2012 New England floods."

Among other things, decision modeling:

- Allows decision logic to become a managed asset, like other forms of data.
- Strengthens stewardship over decisions by internal business analysts.
- Shortens response to continually changing policies and regulations.
- Frees up otherwise fixed program costs.
- Shortens software development cycles and yields far fewer errors.
- Supplants monolithic systems.
- Reduces the complexity and number of IT contracts and the dependence on third-party labor.

To realize the potential of decision

modeling, the federal government could establish a governmentwide pilot project that would entail modeling a subset of business decision logic pertaining to a topic area subject to federal regulation, such as telecommunications, patents, acquisitions, environmental issues or taxes.

Then the government could model the chosen set of regulations in simple decision tables, in accordance with the Decision Model or DMN, and load the connected decision tables containing the regulations into a web API tool to make them centrally available and systematically accessible. The Digital Government Strategy encourages the use of web APIs to make "data assets freely available for use within agencies, between agencies, in the private sector or by citizens."

Such an architecture would allow internal business analysts to update the regulations in real time as changes occur. Upon successful adoption of the new decision model paradigm, legacy hard-coded systems could be redacted and eventually phased out. ■

Dawn Levy is a management consultant and electrical engineer with more than 20 years of service, predominantly to business and technical leaders in the federal market. She seeks to deliver efficiency and productivity to her clients and to reduce superfluous spending.

The Unsung Hero of Mobile Computing: The Notebook

The notebook computer doesn't get much respect these days. The myriad smaller, flashier mobile devices seem to get all the attention. The notebook computer may not be the sexiest mobile device out there, but for many functions, it's still the best combination of flexibility, productivity, manageability and low cost around.

Notebooks are workhorses for productivity, collaboration, creating content and much more. They're much more powerful than tablets or smartphones, with greater amounts of RAM and storage, and higher performance thresholds. With these capabilities, notebook computers can more easily support more complex operating systems like Microsoft Windows 10—a key upgrade for most federal agencies.

Because notebooks can run Microsoft Windows 10, they can easily run virtually any software, from word docu-

ments and spreadsheets to specialized apps. Larger screens also make it easier to edit images, video and documents.

GET THE MOST OUT OF THE MODERN NOTEBOOK

Today's notebooks are faster, more secure and more feature-rich than ever before. Consider these factors before choosing your agency's next notebook platform:

Performance: For workloads requiring high levels of performance, choose the fastest processor your budget allows. Intel's sixth generation dual or quad core processors, for example, provide significant performance and improvements over earlier processors. According to non-profit benchmarker BAPCo, the new processors provide 2.5 times greater performance than five-year-old mobile PCs.

RAM: For high-end graphics, database and spreadsheet users, consider at least 8GB of RAM. Document creators or

single-task users may be able to get away with 4GB of RAM. True power users should opt for 12GB of RAM.

Storage: The minimum size hard drive to consider is about 500GB, but it doesn't cost much more for 1TB. For users who need extremely high performance, consider a Solid State Drive (SSD). It's more expensive, but also faster and more reliable.

Battery life: More is always better, but larger batteries are heavier. It's a trade-off to evaluate considering each individual's preferences.

Wi-Fi connection: Choose a notebook with dual-band WiFi (2.4GHz and 5GHz), which provides the most flexibility.

Screen size: For users who toggle between several applications at the same time, a larger screen makes sense. For users who deal with images and graphics, focus on the pixel count—the higher the pixel count, the sharper the resolution.

Tablet or Notebook. Why Not the Best of Both?

Tablets make sense for some tasks, while notebooks make more sense for others. Tablets are particularly useful for fieldwork where employees have to collect data or remotely capture images and upload them to a central database. Notebooks are more useful for creating content, using RAM-intensive applications and collaborating with others.

According to Mobile Work Exchange, 76 percent of federal government workers use mobile devices of some type for work-related tasks. While these devices are essential to workers' productivity, the different use cases sometimes mean employees must carry both a tablet and notebook. That's not only expensive, but cumbersome.

Agencies are more frequently considering hybrid devices—a device that combines the strengths of the tablet with the power of the notebook. FEMA, for example, outfits its inspectors with Panasonic Toughbook 18 devices. Those are notebooks that can convert to tablet PCs. This combination of functions has helped streamline data collection and reduced data loss.

There are many other reasons for agencies to considering hybrid units—or 2-in-1s as some call them. They are the ultimate in flexibility. They let users remove the keyboard if they want. They can also remove the screen to use it as a tablet.

They are lighter than notebooks and can run Windows, which is critical for

many applications. Most have both touchscreen and keyboard input options. Weight tends to be between about 2.5 and 5 pounds, and screen size runs between about 10 and 15.6 inches. RAM ranges from 2 to 8 GB, storage from 128 to 512 GB, and processors from 1.1 to 3.1GHz.

Hybrid systems are also physically flexible. Some, like Lenovo's Yoga devices, open like a notebook but let users fold the display back around into a tablet configuration. Others, like the ASUS Transformer Book, Microsoft Surface Pro 3 and HP Envy series, have detachable screens and keyboards, so users can configure them any way they want.

Secure Mobility: Better than Before

The need for strong security is a given in today's mobile world. And for federal agencies, the stakes are higher. The proliferation of the Bring Your Own Device (BYOD) movement has been a game-changer. Without the right tools, these devices increase the risks of sensitive information getting into the wrong hands.

It's a challenge, but not insurmountable. Starting with a mobile device with built-in security and layering the latest security tools on top, agencies can be confident in securely expanding mobile programs.

The first step is to choose a solid mobile device with built-in security features like root detection, secure boot, authentication, data encryption, local/auto wipe, device lock, secure managed containers and even fingerprint identification.

With those solid security features as a baseline, the next step is to add endpoint management and security tools on top. Enterprise Mobility Management (EMM) systems include most features agencies need.

- Role-based access control
- Encrypted application transmission
- Secure application distribution
- Authentication of users before they can access documents and data

ALL OF THE TECHNOLOGY IN THE WORLD WON'T WORK IF EMPLOYEES AREN'T TRAINED IN MOBILE SECURITY.

EMM combines some of the most effective products of the past, including Mobile Device Management (MDM), Mobile Application Management (MAM) and Mobile Content Management. The typical EMM feature set includes:

- Password management
- Lock and find devices
- Remote device wipe

- Limited access to third-party applications

Of course, all of the technology in the world won't work to its full potential if employees aren't trained in mobile security. That means enforcing policies, such as avoiding public Wi-Fi, consistent password use and never clicking on unknown e-mail links.

With Mobility, the Sky is the Limit

Federal agencies today expect mobility to improve productivity and efficiency in many areas, from telework and fieldwork to telehealth and inventory management. As technology improves and developers gain experience, agencies continue to push the envelope. They're squeezing more functionality and innovation out of mobile devices and applications. Here are some examples of innovative mobility in action throughout the federal government:

Protecting the food supply: The FDA's Field Investigator Tool with Mapping (FIT-MAP) lets employees with Windows mobile devices use geo-tags to collect more detailed, location-specific data. With this information, the agency can analyze and create situational awareness of threats to the food supply.

Keeping our borders safe: Immigration and customs enforcement agents now have a mobile biometrics app. The app can quickly process fingerprints, transfer

photos, and compare them with existing records. Instead of taking hours or longer to identify persons of interest, it now takes only minutes.

AS TECHNOLOGY IMPROVES AND DEVELOPERS GAIN EXPERIENCE, AGENCIES CONTINUE TO PUSH THE ENVELOPE.

Saving lives: PTSD and suicide prevention are genuine concerns for the military. Using an app called POS REP, veterans can get push notifications of peers and activities near their location. Its developers call it "the social network for the 0.5 percent."

Fast, automated building upkeep: Instead of individually checking every component of a building to ensure it's

ready for occupancy, GSA's Public Building Service will use a system based on Google Glass. This lets inspectors take photos, scan barcodes and dictate notes

by voice. The report is then sent to a content management system.

Connecting with citizens via social media: The Interior Department recently experimented with Periscope; a live streaming video app that lets users watch and broadcast video from all over the world. The goal is to improve citizen interaction. Other agencies are watching this carefully.

Mobile security: Take nothing for granted

The ubiquitous mobile computers continue to pose unique security challenges

Work is much more mobile these days, and technology has risen to meet the mobile demand. While laptops and notebook computers have been part of the mobile infrastructure for some time now, the challenges of managing and securing these mobile computing platforms remains as much a priority as ever.

Notebooks and laptops have maintained their position at the top of the mobile computing pyramid primarily due to their storage capacity and processing power. They are true desktop replacements that modern workers use in their offices or anywhere they need to be present and productive. Tablets and smartphones are ubiquitous as well, but lack the power to truly bring productivity applications to the forefront.

Tablets, smart phones and other smaller mobile devices are better for consuming data, says Steve Taylor, solution architect for

Intel. Laptops and notebooks have the storage and capacity for creating data. They're far better suited than smaller mobile devices for productivity applications that generate data, such as spreadsheets, presentations and documents. "No one wants to run a presentation from their phone," says Taylor.

That has led to the ubiquitous presence of laptops and notebooks in any organization's infrastructure, and the host of challenges when it comes to managing and securing those systems. "There's a whole set of unique problems," says Taylor. "The number one challenge is data loss. Any laptops that are outside the organization are susceptible to theft or loss. You also have the issue of laptops being misused, whether accidentally or deliberately."

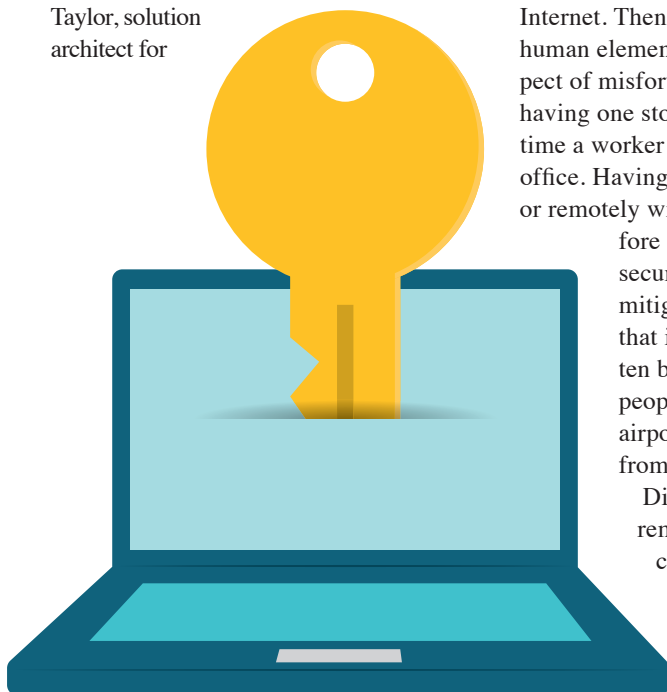
Viruses, malware and malicious attacks are always a possibility, as with any device that connects to the Internet. Then, of course, there is the human element and the simple prospect of misfortune. Losing a laptop or having one stolen is a possibility any time a worker brings one out of the office. Having the ability to lock down or remotely wipe a hard drive is therefore an essential aspect of a security plan. "The ability to mitigate the risk of an asset that is lost or stolen has gotten better," says Taylor. "But people still lose devices at airports or have them stolen from cars."

Disk encryption and remote disk wipe are critical functions, especially in instances where organizational policy allows workers to

maintain potentially sensitive data on their laptops and notebooks. It's also important to have appropriate policies in place to ensure laptops and notebooks are able to remain updated. "The management console needs to provide secure communications whether [the laptop] is connected to the VPN or not," says Taylor.

When considering a management solution, look for one that provides role-based access control. "Not everyone requires the same level of access," says Taylor. He points to the different roles in an organization like the administrators who establish and enforce policies, help desk operators who configure and deploy those policies and standard business users. All those users require differing levels of access and privileges.

To ensure notebook and laptop computers are as secure as possible, it ultimately depends on having the combination of the latest hardware with a fast processor, enhanced security features and the latest most secure operating systems and security software, says Taylor. It's not one or the other; you do need both.



SPONSORED BY



Making FITARA matter: Tools for implementation

ACT-IAC has unveiled its first resource to help agency IT leaders implement FITARA and reap the benefits of the ambitious law

BY DARREN ASH AND RICHARD A. SPIRES

The objective of the Federal IT Acquisition Reform Act is to improve the management of IT within an agency and, hence, improve the ability of that agency to achieve its mission and conduct its business.

Those improvements, however, can happen only if FITARA is effectively implemented. So the American Council for Technology-Industry Advisory Council, in consultation with the Office of Management and Budget, launched a FITARA Implementation Project, which has more than 50 volunteers from the public and private sectors.

Those experts in IT, finance, human resources and acquisition are backed by a steering committee composed of current and former public- and private-sector CIOs, chief acquisition officers, chief financial officers and chief human

capital officers. That team is working to help agencies clear the hurdles of FITARA implementation.

ACT-IAC's three-phase project aims to provide:

- An IT Management Maturity Model to help agencies not only conduct self-assessments but also establish a roadmap to achieve demonstrated maturity in IT management.
- Policies, processes, tools and other artifacts that represent proven IT management practices garnered from the public and private sectors. We hope such artifacts from proven management practices can help agencies more rapidly mature their IT management capabilities.
- Development of metrics to help OMB and the agencies measure the impact of FITARA over time.

The IT Management Maturity Model

We have recently completed Version 1 of the IT Management Maturity Model. Our desire is to continue to evolve and improve the model through use and feedback. So in addition to reviewing the model, you can provide feedback on how we can improve it.

The model can help agencies assess their maturity in five critical functions of IT management:

- **Governance.** The collaboration and

decision-making glue by which IT management works.

- **Budget.** The process to formulate, obtain approval and execute the use of funds to support IT.

- **Acquisition.** The buying processes used to obtain IT products and services.

- **Organization and workforce.** The process to determine needed competencies and develop and sustain a workforce that has those competencies through recruitment and professional development.

- **Program management.** The set of disciplines used to deliver IT capabilities to meet an agency mission or business need, or the operations and maintenance of an existing system.

OMB's guidance for FITARA includes a Common Baseline for IT Management that has sections for budget formulation, budget execution, acquisition, and organization and workforce. We have reorganized and reoriented those sections slightly to support the development of the IT Management Maturity Model. We started by combining budget formulation and execution to highlight the degree of integration typical in most agency budget processes.

As the teams developed the traits and characteristics of the IT Management Maturity Model, governance and

Darren Ash, CIO of a federal agency, is writing here in his capacity as co-chair of the ACT-IAC FITARA Implementation Project. Fellow co-chair 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 Learning Tree.

The five critical functions of IT management

Version 1 of the IT Management Maturity Model has been completed.

Here are the functions it seeks to improve:



Governance

The decision-making glue by which IT management works.



Budget

The process to obtain and execute funds to support IT.



Acquisition

The buying processes used to obtain IT products and services.



Organization / workforce

The process to develop and sustain a workforce that has the right competencies.



Program management

The set of disciplines used to deliver IT capabilities to meet a business need.

program management topics became recurring themes that cut across the three primary pillars of budget, acquisition, and organization and workforce. As a result, we chose to illustrate the integrative power of both governance and program management to effective IT management. To make the maturity model easier for agencies to use, it includes explicit linkages to elements of OMB's common baseline requirements.

We present the model at three levels of detail. For each of the five functions, we provide over-arching themes that are illustrative of what demonstrated maturity looks like for that function. We also have a one-page table for each of the five functions that highlights key aspects of the model. Finally, the detailed model provides a description of the function and defines a number of attributes and traits for each attribute that can be used to assess the maturity of an organization in that function.

The model specifies characteristics of three levels of maturity: Level 1 — Basic Capabilities, Level 2 — Evolving Maturity and Level 3 — Demonstrated Maturity.

Each agency is unique, and in recognition of that, the model focuses on the behaviors and outcomes expected

at each level of maturity, not on the organizational structures and processes required to achieve those behaviors and outcomes. Hence, the maturity model can be applied to small, centralized agencies and to the largest, most diversified Cabinet-level departments.

For agencies that are federated (with bureaus, components, or equivalent and multiple IT organizations), the agency CIO can use the model to assess the agency as a whole while including the appropriate interaction, authorities and delegations from the agency to the bureaus/components or programs. A bureau/component or program-level CIO can also apply the model to IT management within a bureau/component or program.

In applying the model, all attributes and traits across all functions are important. But an agency can conduct a self-assessment against the model and should look at sequencing its improvement initiatives. Within a function, the priority should be placed on moving from Level 1 to Level 2 to have evolving maturity across a management function, then focus on moving to Level 3. Agencies should use pilot tests to improve a project or part of the agency but recognize that

achieving a level of maturity requires that attribute to be exhibited across all IT management at the agency.

Finally, the objective should be to institutionalize practices at Level 2 and eventually Level 3 through the use of policy directives, procedural guidance and tools because demonstrated maturity must survive changes in leadership.

Next steps

Our team is now focusing on Phase 2, which involves identifying proven practices and related artifacts that can help agencies rapidly evolve their IT management capabilities. The key is that they are proven and used on a regular basis to help an organization manage that function or attribute with demonstrated maturity.

We know that pockets of excellence exist throughout the government and the private sector, and we know that organizations have made the effort to refine and document processes to support their management needs. We expect to identify such practices, package them and make them available for agencies to assess and adopt, if they are helpful.

We will keep you apprised of our progress. ■

GUEST COLUMN

SYSTEMS DEVELOPMENT

DHS Moving on to CDM Phases 2 and 3

Agencies Incorporate Physical Access Metrics into Comprehensive Risk Management



Mark Steffler

Vice President Federal Practice
Quantum Secure

“The Continuous Diagnostics and Mitigation (CDM) program is a dynamic approach to fortifying the cybersecurity of government networks and systems.” This scope statement, taken directly from the DHS CDM Web site, is a heavy lift for government enterprise. DHS has wisely taken a crawl, walk, then run approach to rolling out its Continuous Monitoring and Mitigation (CDM) program, so as not to overwhelm US government departments and agencies. This three-phase strategy provides incremental, tangible real-world progress toward a safer and more secure government enterprise.

Phase 1 of the CDM program focused solely on securing cyber infrastructure and information systems. Phase 2 expands the scope of CDM to include fine-grained privilege management for both logical and physical resources and drives government departments and agencies (D/As) to align with the Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance.

In Phase 3, CDM will limit physical access risk by focusing on centralized management for numerous disparate and proprietary physical access control systems (PACS) deployed across D/As. This acknowledgement by DHS that both cyber and physical

resources must be more holistically controlled to reduce and manage risk, embraces and mirrors similar guidance expressed four years earlier by the Federal CIO Council in the FICAM Roadmap and strongly reinforced in OMB Memorandum 11-11.

PHASE 2 REQUIREMENTS

Despite an increasing focus on protecting personal information and national secrets in the digital world, it is critical to also treat physical access controls with the same care as logical controls. There are still vulnerable and critical assets secured by locked doors that should only be available to privileged users. While government IT managers and CIOs are familiar with identity and access management (IAM) and logical access controls, implementing Phase 2 and Phase 3 will require much greater cooperation between CISOs in the CIO offices and the CSOs tasked with facility (physical) security.

DHS defines four functional tool areas in Phase 2:

■ **TRUST**—Access Control Management (trust in people granted access)

■ **BEHV**—Security-Related Behavior Management (such as training qualifications)

■ **CRED**—Credentials and Authentication Management

■ **PRIV**—Privileges (individually managing the lifecycle of access privileges for each person)

Phase 2 focuses on least privilege management, using Attribute-Based Access Control (ABAC) in order to more appropriately limit access to only those resources necessary to accomplish one's job. Achieving this goal requires integration with authoritative identity data sources, such as databases that support PIV card issuance, training, Active Directory, Attribute Exchanges and so on. This data is used to make policy based decisions regarding privileged access.

The myriad proprietary physical access control systems (PACS) currently installed in government enterprises do not function this way. Ripping and replacing these PACS across the government enterprise to work like a cyber-system would cost billions of dollars, take at least five or more years and be incredibly disruptive to security operations and user experience.

SHORT PRIMER ON PACS AND AS-IS PROCESSES

Legacy PACS are based on a pre-determined access list (white list). This defines who has access to which door/portal in order to support their expected throughput. PACS are pre-programmed through a collection of electro-mechanical end points.

These end points must be provisioned in advance with the PIV card or other credentials and specific access authorizations for each credential. When a person presents a PIV card, the transaction to authenticate the PIV card at time of use and to see if that PIV card is authorized

to unlock a given door should happen within a few seconds. This requires PACS provisioning for the PIV card and any specific access authorizations (add/change/deletes) for certain doors be done in advance—not on the fly.

The As-Is state of physical access privilege management today is often to manually enroll credentials and manually assign ever-changing access privileges to each person. This comes at high cost associated with such manual processes, coupled with high risk of human error.

Current coping mechanisms include creating a more manageable number of “door groups” or “access levels.” There may be ten, twenty or more doors grouped together in a door group. If a person needs access to only one of those doors, the administrator will just assign the whole door group. This may give an individual greater access than he needs, which obviously increases risk.

With millions of combinations of people and their ever-changing access requirements, security personnel can only achieve the fine-grained least privilege target state through automation. In order to successfully manage each person’s minimum privilege (PRIV), the three other DHS-specified factors TRUST, CRED and BEHAV provide the needed input to qualify what access a given individual has earned.

TARGET STATE TO ACHIEVE PHASE 2

The PACS Privilege Management System must align with the FICAM segment architecture. It is important to connect the authoritative identity data sources to a policy-based decision and enforcement system. This must constantly update the numerous disparate PACS on a continuous basis, via one or both of these automation paradigms:

Policy Automation: Access policy will include a combination of user attributes, which come from TRUST, CRED and BEHAVE functions. These can be automatically enforced. If someone achieves a certain certifica-

tion or security clearance level, for example, they may automatically gain additional access authorizations to specific doors or facilities. In Phase 2 if someone currently has access authorization for a specific door, but loses their required training credential or has been reported as showing questionable behavior, this will be reported as a defect. In Phase 3, the result could automatically terminate that specific access authorization without human intervention and provide appropriate notifications to stakeholders.

Process Automation: One or more human approvals are often required to gain physical access to an area. It is important to convert this largely manual process into an electronically automated process that is auditable and enforces policy with proof of compliance. The government defined model for achieving this target state is more fully fleshed out in the FICAM Roadmap, Chapter 4, which the CDM program fully embraces and leverages in its requirements.

MOVING TO PHASE 3

DHS defines three new areas in Phase 3, focusing on event management and boundary protection, employing technologies for forensic analysis and data loss prevention, among other goals:

- **BOUND-N** – Network (not endpoint) focused protection
- **BOUND-E** – Encryption for data in transit and at rest
- **BOUND-P** – Enterprise PACS Centralized Management and Control

DHS is still developing its Phase 3 requirements. There is a strong indication that BOUND -P will explicitly require integration of all disparate PACS into a centralized PACS Management System at the D/A level. This PACS Management System will perform the following critical functions:

- Centralize PIV card provisioning and associated fine-grained access privileges into hundreds of disparate PACS simultaneously as indicated in Phase 2. This will also require connections to authoritative identity data sources, such as a PIV card database (CRED) or training database (BEHAVE) and any additional data (TRUST) to assure policy-based decisions.

- Collect and analyze all current software and/or firmware versions for controller panels, card readers and other components. Compare the “as is” state to current GSA approved and/or other current secure versions for each component. Then provide a report of any defects to both the local and Federal Dashboard for mitigation.

- Collect and analyze the behavior of each person’s physical access activity for anomalous behavior. Such behavior can include badge fishing, tailgating, odd comings and goings, and badging in at more than one site at the same time. Then integrate this data with logical systems to detect a login from a site where the PACS was not accessed, or logical access and physical access patterns that don’t make sense. All this data can be aggregated into Indicators of Compromise (IOCs), which help identify and score risk at a fine grained level for mitigation.

SUMMARY

The CDM program demonstrates the importance of managing risk holistically in both the physical and logical domains to achieve high security. This is going to require greater cooperation between the IT (CISOs) and facilities security (CSO) practices within government organizations. The DHS CDM program provides robust support to D/As to help accomplish this goal.



For more information, please visit:
www.quantumsecure.com/safe-government

FCW Index

People

Ash, Darren..... 28-29	Hollister, Hudson.... 8	Slick, Stephen..... 16-17
Boehner, John 8	Hugler, Edward..... 9	Snowden, Edward..... 17
Branch, Ted..... 3	Johnson, Troy 3	Spaulding, Suzanne 7
Brennan, John 15-17	Labovitz, George ... 11	Spires, Richard 9, 28-29
Cantor, Eric..... 8	Levy, Dawn 22, 24	Sweet, Larry..... 9
Cohen, John 7	Lux, Rob 24	Switzler, Al 11
Currie, Chris..... 7	McMillan, Ron 11	Taylor, John 10
Danet, Theon..... 9	Missal, Michael..... 9	Tseronis, Peter..... 9
Dorris, Martha..... 9	Moskovitz, David 9	van Riper, Kris 10
Fiorina, Carly 17	Olson, Kelly..... 20-21	von Halle, Barbara 24
Goldberg, Larry 24	Patterson, Kerry..... 11	Waldron, Roger 21
Gordon, Susan 17	Ratcliffe, John..... 7	Wennergren, David 11
Grenny, Joseph 11	Roche, Sean 16-17	Wince, Kevin..... 9
Griffin, Richard 9	Rosansky, Victor 11	Wolfe, Doug..... 16-17
Hallman, Andrew... 16	Ross, Ron..... 9	Wynn, Renee..... 9
Harris, Shane 17	Rumsey, Matt..... 8	
Hayden, Michael..... 16-17	Schwartz, Ari..... 9	

Agencies/Organizations

Accenture..... 9	Navy..... 3, 11
ACT-IAC..... 28-29	NGA 17
CEB 10	NIST 9
CIA 14-17	NSA..... 17
Coalition for Government Procurement 21	Object Management Group..... 24
Congress 7, 8	OMB..... 22, 28-29
Data Transparency Coalition..... 8	Partnership for Public Service..... 9
DCMA 9	Professional Services Council..... 11
DHS..... 7, 9	Rutgers University 7
DOE..... 9	Sunlight Foundation 8
Freddie Mac 24	University of Texas 17
GAO 7, 22	VA..... 9
GSA..... 9, 20-21	Venable..... 9
HP..... 17	White House 9
Labor..... 9	Zachman International..... 9
Learning Tree..... 9, 28	
NASA..... 9	



FCW WEBCAST SERIES

CLOUD COMES OF AGE

SESSION 3:
Cloud Computing: Deeper into the Enterprise

NOV 17th, 2015 @ 2PM EDT

FEATURING: Greg Capella,
Acting Executive Director
of the Enterprise Systems
Development Office at DHS

SPONSORED BY: VMware, Carahsoft and Carpathia, A QTS Company

REGISTER NOW AT: fcw.com/2015CloudComputingSession3

Statement of Ownership, Management and Circulation

1. Publication Title: FCW
 2. Publication Number: 0893-052X
 3. Filing Date: 09/30/15
 4. Frequency of Issue: Two issues monthly Mar. through Sep. and one issue in Jan., Feb., Oct. and Dec.
 5. Number of Issues Published Annually: 18
 6. Annual Subscription Price: US \$125, International \$165
 7. Complete Mailing Address of Known Office of Publication:
9201 Oakdale Ave., Ste. 101, Chatsworth, CA 91311
 8. Complete Mailing Address of the Headquarters of General Business Offices of the Publisher: Same as above.
 9. Full Name and Complete Mailing Address of Publisher, Editor, and Managing Editor:
Henry Allain, COO and Public Sector Grp. President, 4 Venture, Suite 150, Irvine, CA 92618
Troy K. Schneider, Editor-in-Chief, 8609 Westwood Center Dr., Ste. 500, Vienna, VA 22182-2215
Terri J. Huck, Managing Editor, 8609 Westwood Center Dr., Ste. 500, Vienna, VA 22182-2215
 10. Owner(s): 1105 Media, Inc, dba: 101communications LLC
9201 Oakdale Ave., Ste. 101, Chatsworth, CA 91311. Listing of shareholders in 1105 Media, Inc.
 11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or more of the Total Amount of Bonds, Mortgages or Other Securities:
Nautic Partners V, L.P., 50 Kennedy Plaza, 12th Flr., Providence, RI 02903
Kennedy Plaza Partners III, LLC, 50 Kennedy Plaza, 12th Flr., Providence, RI 02903
Alta Communications IX, L.P., 1000 Winter Street, South Entrance, Suite 3500, Waltham, MA 02451
Alta Communications IX, B-L.P., 1000 Winter Street, South Entrance, Suite 3500, Waltham, MA 02451
Alta Communications IX, Associates LLC, 1000 Winter Street, South Entrance, Suite 3500, Waltham, MA 02451
 12. The tax status has not changed during the preceding 12 months.
 13. Publication Title: FCW
 14. Issue date for Circulation Data Below: September 30, 2015
 15. Extent & Nature of Circulation:
- | | Average No.
Copies Each Month
During Preceding
12 Months | No. Copies of Single Issue
Published Nearest
to Filing Date |
|--|---|---|
| a. Total Number of Copies (Net Press Run) | 52,254 | 52,400 |
| b. Legitimate Paid/and/or Requested Distribution | | |
| 1. Outside County Paid/Requested Mail Subscriptions Stated on PS Form 3541 | 29,291 | 31,894 |
| 2. In-County Paid/Requested Mail Subscriptions Stated on PS Form 3541 | 0 | 0 |
| 3. Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid or Requested Distribution Outside USPS* | 10,423 | 9,898 |
| 4. Requested Copies Distributed by Other Mail Classes Through the USPS | 0 | 0 |
| c. Total Paid and/or Requested Circulation | 39,714 | 41,792 |
| d. Nonrequested Distribution | | |
| 1. Outside County Nonrequested Copies Stated on PS Form 3541 | 11,759 | 9,668 |
| 2. In-County Nonrequested Copies Distribution Stated on PS Form 3541 | 0 | 0 |
| 3. Nonrequested Copies Distribution Through the USPS by Other Classes of Mail | 0 | 0 |
| 4. Nonrequested Copies Distributed Outside the Mail | 356 | 577 |
| e. Total Nonrequested Distribution | 12,115 | 10,245 |
| f. Total Distribution | 51,829 | 52,037 |
| g. Copies not Distributed | 425 | 363 |
| h. Total | 52,254 | 52,400 |
| i. Percent paid and/or Requested Circulation | 76.63% | 80.31% |

Ad Index

Advertisers

Acquire Show

www.ACQUIREshow.com **23**

CDWG

www.CDWG.com/admc2 **10a-10d**

www.CDWG.com/cloud **12-13**

www.CDWG.com **25-27**

FCW Webcast Series

www.fcw.com/2015CloudComputingSession3 **32**

Hewlett Packard

www.hp.com/go/pubsecsecurity **2**

InterSystems Corp.

www.InterSystems.com/Federal1CC **35**

Northrop Grumman

www.northropgrumman.com/cyber **1a-1b**

Quantum Secure, Inc.

www.quantumsecure.com/safe-government **30-31**

The Boeing Company

www.boeing.com **18-19**

United Healthcare

www.uhcfeds.com **5**

Vision Technologies Inc

www.visiontech.biz **36**

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

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

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

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

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

The big worries about big data

Federal agencies are moving warily when it comes to big-data projects. Four in 10 have no big-data plans at present, and just a handful have fully implemented programs.

AMONG THOSE AT LEAST CONSIDERING BIG DATA...

- 28% Investigating
- 18% Will have in next 12 months
- 38% Pilot project(s) underway
- 16% Fully implemented

73%

find the lack of qualified staff to be a major concern.

THOSE WITH PROJECTS UNDERWAY HAVE ALREADY SEEN STRAINS:

Very concerned about...

- 77% Overall costs
- 73% Security risks
- 73% Strains on existing IT infrastructure
- 70% Difficulty architecting analytics systems

28%

say, "It is difficult to demonstrate the value of big-data analytics to my agency's management."

INFRASTRUCTURE IS A BIG CONCERN, AND THOSE CONSIDERING BIG-DATA EFFORTS ARE TAKING STEPS TO SCALE UP:

In the next 12 months, plan to...

- 63% Increase network bandwidth
- 55% Improve data security
- 54% Add cloud-based analytic services
- 48% Add cloud-based storage services
- 46% Add server hardware

THOSE WHO'VE PUT BIG DATA TO WORK DO SEE BENEFITS:

Big-data programs have...

- 93% Improved decision-making speed and quality
- 87% Improved ability to predict trends
- 87% Allowed for better risk quantification
- 74% Streamlined internal processes
- 70% Improved planning and forecasting

Source: Beacon Technology Partners survey for FCW and GCN.
This research was underwritten by Unisys Federal Systems.



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

HealthShare transforms care by sharing health information.

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

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

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

Learn more at: InterSystems.com/Federal1CC

INTERSYSTEMS®

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

Are You Suffering From Bad WiFi?



That unreliable connection. The slowly spinning indicator. It happens to everyone.

If poor wireless performance is what ails you, **Vision Technologies** has the remedy. From simple signal enhancement to comprehensive infrastructure design, implementation and support, our solutions enable business mobility.

With a well-established history in wireless communications and converged voice and data networking, Vision partners with Cisco, Ruckus, and Meraki to engineer wireless Local Area Networks (wLANs) solutions suited to every environment. We bring secure, authenticated wireless networking to high traffic public areas such as airport terminals, convention centers, hotels, offices, manufacturing facilities, warehouses, auditoriums and classrooms – while bringing our clients simple network management and peace of mind.

So stop suffering from bad WiFi, and see how Vision can help you.



VISION

SOLUTIONS:

- ▶ Enterprise WiFi and Hotspots Guest access
- ▶ WiFi For business services
- ▶ Multi-service mesh networks
- ▶ Outdoor broadband wireless/WiFi Point-to-point wireless
- ▶ Point-to-multi-point wireless
- ▶ Wireless video surveillance
- ▶ In-building cellular solutions
- ▶ WiFi cellular signal enhancement
- ▶ Public safety solutions

(866)746-1122

info@visiontech.biz
www.visiontech.biz