



THE BUSINESS OF FEDERAL TECHNOLOGY

# CAN TONY SCOTT GET IT ALL DONE?

The U.S. CIO has made a mantra of 'land the planes' and pushed notable improvements in his first nine months. But the to-do list for 2016 is long indeed.

PAGE 16

**2015 RISING STARS**

**YOUNG  
LEADERS  
TO WATCH**

PAGE 20



## 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](http://uhcfeds.com).**

**Open Season runs from November 9 through December 14.**



Not all health plans are available in all areas. Visit [uhcfeds.com](http://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.

## Pentagon purges HTML from .mil emails

As part of its campaign to improve email security, the Defense Department is instituting a policy to render web links unclickable in email messages to .mil addresses, Richard Hale, DOD's deputy CIO for cybersecurity, told FCW.

The new policy, which was coordinated between Hale's office and U.S. Cyber Command, is already in place for much of the .mil domain, Hale said. For at least some users, outside email messages are being flagged in the subject line as coming from a "non-DOD source."

Hale told FCW that after reviewing a series of anti-phishing measures already in place, officials decided that a more stringent approach was needed. "For years we have had an email policy that says we will not render HTML email," he said, but some email clients still include active links in their messages.

He said the solution was to "deactivate the links more actively in the mail system before it gets to an end user by adding a little extra into the link that says, 'Caution.'" Email users can still paste the link into a Web browser, "but we don't want that link to be active in

[an] email and have someone click on it before they've thought through" the security implications.

The extra measure is part of a series of initiatives begun in September by Joint Force Headquarters DOD Information Networks.

"We need to arm ourselves and our families with the defensive skills and knowledge to protect them from being victimized by a phishing email, computer or phone scam."

— TERRY HALVORSEN, DEFENSE DEPARTMENT

"JFHQ DODIN provided direction to all DOD components to implement initiatives to further harden the DOD information environment, which included improving endpoint security system standards," a Cyber Command spokesperson said in a statement. "Along with these initiatives, efforts to harden the DODIN's defenses are always ongoing."

Deputy Defense Secretary Robert Work and other officials have said that a great majority of intrusions into Pentagon networks are the result of the kind of human error that is exploited

in phishing attacks, in which seemingly trustworthy email links are used as attack vectors to hijack computers, install malware or steal credentials.

Therefore, DOD CIO Terry Halvorsen has made clamping down on phishing a priority during his tenure. In March, he issued a memo warning about potential phishing attacks on defense personnel through social media accounts.

"Phishing continues to be successful because attackers do more research, evolve their tactics and seek out easy prey," Halvorsen's memo states. "We need to arm ourselves and our families with the defensive skills and knowledge to protect them from being victimized by a phishing email, computer or phone scam."

The new anti-phishing policy will have consequences for marketers and media (including FCW) trying to reach audiences behind the .mil screen. FCW and its sister publications already offer plain-text versions of their email newsletters and have taken additional steps to make those messages user-friendly for newly restricted DOD recipients.

— Sean Lyngaas

### FCW CALENDAR

#### 12/2 Big data

Commerce Chief Data Officer Ian Kalin and CFPB CDO Linda Powell are among the speakers at this FCW event on integrating big data into agency operations. Washington, D.C.  
[FCW.com/bigdata](http://FCW.com/bigdata)

#### 12/10 Agile

ACT-IAC's Emerging Technology Community of Interest will host a panel discussion on overcoming the challenges of acquiring agile digital services in government. Washington, D.C.  
[is.gd/agile\\_gov](http://is.gd/agile_gov)

#### 12/15 Cybersecurity

DHS Cybersecurity Strategist Darryl Peek will speak at Washington Technology's Cybersecurity Industry Day, which will explore agencies' near-term cyber initiatives. Falls Church, Va.  
[is.gd/wt\\_cyber](http://is.gd/wt_cyber)



# Contents



## **16 PEOPLE** **Can Tony Scott get it all done?**

The U.S. CIO has made a mantra of 'land the planes' and pushed notable improvements in his first nine months. But the to-do list for 2016 is long indeed.

**BY ADAM MAZMANIAN**

## **20 RISING STARS** **Young leaders to watch in 2016 and beyond**

Here are 14 young women and men — in agencies and the private sector alike — who are overachieving in their current roles and distinguishing themselves as the likely leaders of tomorrow. *(Pictured above: Lindsay Burack)*

**BY FCW STAFF**

## TRENDING

### **3 CYBERSECURITY**

Pentagon purges HTML from .mil emails

### **FCW CALENDAR**

Where you need to be next

### **10 PROCUREMENT**

GSA mulls new cloud acquisition vehicle. Plus, 18F hacked procurement and got code for \$1.

### **11 EDITOR'S NOTE**

Federal 100 nominations are due by Dec. 23

## DEPARTMENTS

### **12 COMMENTARY**

Wish they all could be...

**BY ALAN BALUTIS AND STUART ROBBINS**

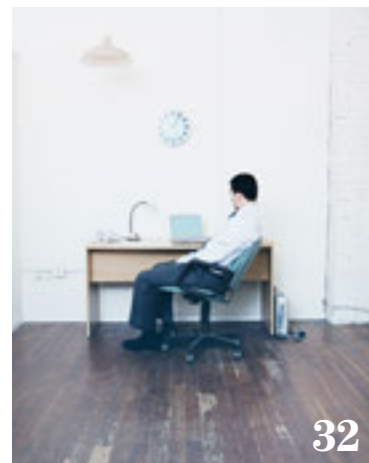
A breach is coming — is your agency ready?

**BY KRIS VAN RIPER AND SCOTT SHERMAN**

### **32 DRILL DOWN**

Telework and the loneliness left behind

**BY ZACH NOBLE**



COVER PHOTOGRAPH BY ROBERT SEVERI



# MANAGED SERVICES.

A POWERFUL IT SOLUTION FOR GOVERNMENT AGENCIES.

Secure your network. Protect your data. And rest assured your IT infrastructure is cared for by a leader in the business. We'll work with your IT team to handle the day to day network tasks, so they can focus on the big picture. From reliable bandwidth to accountability and cost efficiencies, nobody knows networks, and your network needs, like we do.

**1-877-900-0246**  
[brighthouse.com/enterprise](http://brighthouse.com/enterprise)

BRIGHT HOUSE NETWORKS  
**enterprise solutions** 

WE'RE WIRED DIFFERENTLY



**MANAGED SECURITY | MANAGED NETWORK | MANAGED WIFI**

©2015 Bright House Networks. Some restrictions apply. Serviceable areas only.  
Service provided at the discretion of Bright House Networks.



**Editor-in-Chief** Troy K. Schneider  
**Executive Editor** Adam Mazmanian  
**Managing Editor** Terri J. Huck  
**Staff Writers** Aisha Chowdhry, 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, Bianca Spinoso  
**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

**Chief Technology Officer**  
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

# The Federated Cloud

**M**ost federal IT managers and their staff are familiar with the different types of cloud technology available—private, public, community and hybrid. However, there's another important concept when it comes to understanding cloud technology—the federated cloud.

Federation is the process of combining multiple smaller parts that perform a common action. When applying the term to cloud technology, it means combining several clouds—private, public, hybrid or community. Each cloud may meet one specific requirement or accomplish one specific goal.

In the case of federal government, this could mean creating a federated cloud to share data for a research project that spans multiple agencies. In other cases, a federated cloud might serve an entire agency or workgroup that needs to consistently share resources and data.

Simplified management is one of the greatest benefits of cloud federation. Federation lets agencies assign applications to the cloud platforms that make the most sense for that application, instead of simply relying on the agency's default cloud. It



also simplifies load balancing. Security also becomes easier, because agencies can focus on adding more security features to the cloud stack that hosts the most sensitive data and applications.

Federation also means agencies have more freedom of choice. Instead of buying cloud services from one provider, agencies can pick and choose the cloud services that make the most sense for each specific workload, regardless of vendor.

The federal government is enthusiastic about the potential of cloud federation. NIST's Cloud Computing Technology Roadmap, for example, requires frameworks to support seamless implementation of federated community cloud environments. It has assigned a working group to determine the best way to integrate across diverse provider environments, as well as public and private cloud environments.

# The Cloud Security Challenge

**W**hen it comes to the technology supporting federal government operations, security will always be a primary concern. That's certainly true of the cloud. Despite significant progress, agencies are still legitimately concerned about hackers accessing sensitive data stored in the cloud. Recent surveys show security is still the top issue holding agencies back from greater adoption of cloud technology.

While security will always be the most important factor governing any government IT decision, there has been significant progress with respect to cloud storage. In fact, the cloud is far more

secure than it was even just a few years ago. A recent survey published by The Economist, for example, found cloud providers have vastly improved data security and compliance with security and regulatory requirements.

Microsoft, for example, has bolstered security by increasing transparency, visibility and user control. It has added HP's ArcSight as its security information and event management (SIEM) platform. Google also has made great strides, not only by improving transparency, but through Project Zero—its effort to quickly find and fix zero-day exploits.

Other providers are making similar

progress. For example, many have added SIEM, which provides real-time security alert analysis and DDoS (Distributed Denial of Service) protection. This prevents attacks that can completely shut down services. Many also use application container technology and have improved authentication processes.

As cloud security improves and FedRAMP approves more vendors, agencies have begun increasing their levels of cloud adoption. The Defense Department, for example, is moving much of its non-sensitive data to the cloud, such as e-mail and milCloud, DISA's cloud services product portfolio.



# Five Steps to Cloud Readiness

Despite a slow start, cloud adoption throughout the federal government is on the rise. It's expected to increase even more over the next few years. There are several reasons why, according to a report by Forbes Insights. Agencies that have moved some workloads to the cloud are experiencing

significant cost savings and improved data security. Here are some ways to ensure your agency is ready to gain those advantages with cloud computing:

**1. Assess your needs and define expected benefits:** Before diving into a cloud deployment, set clear goals and ensure you know what you want

to achieve. If cost savings is your top priority, for example, that might dictate a different environment than one where increased collaboration or faster response to business needs is the primary driver.

**2. Prepare:** Moving to the cloud isn't just a matter of moving an on-premises workload to a cloud environment. Getting the most value out of a cloud deployment requires starting with clean and organized data. It also requires determining how your applications and data will connect. Determine what type of interfaces they will require. An experienced provider can help with these steps.

**3. Tackle security challenges head-on:** While cloud security has improved considerably, it's important to ask the major security questions upfront. In addition to confirming FedRAMP certification, find out whether all candidates have the type and level of security features you require. Rule out any solutions that don't meet all your security requirements.

**4. Identify the right provider and mix of cloud types:** Evaluate service providers on federal compliance, performance, user support and security. Pinpointing the right type of cloud for specific workloads can be tricky. In most cases, it is extremely helpful to engage a cloud expert with specific experience with federal cloud deployments to help determine what makes sense.

**5. Prepare the organization:** Moving to the cloud brings many benefits, but it changes the workflows, processes, and the roles of IT staff. Start explaining what will change well before you begin the cloud implementation. Explain why the agency is adopting the cloud model; how it will work; and how processes, workflows and IT policies will change. Explain how the roles of IT staff will change from less hands-on to more strategic, and ensure them that they will be retrained to handle these changes.

## BY THE NUMBERS

8%	Percentage of federal CIOs satisfied with their level of cloud adoption
18%	Percentage of federal agencies just getting started with the cloud
30%	Percentage of agency respondents with the right in-house expertise to effectively buy a cloud service
33%	Over the next 12 months, roughly one-third of agencies plan to implement hybrid clouds
35	The number of approved secure Cloud Service Provider offerings
67	The percentage of federal cloud users who believe data is safer in the cloud than in legacy systems
\$7.34 billion	The amount of money the federal government will spend on provisioned services such as cloud in the FY 2016 budget request
\$18.9 billion	The number of dollars the federal government could save by migrating services and applications to the cloud

## CLOUD COMPARISON CHART

TYPE OF CLOUD	PRIVATE	HYBRID	PUBLIC
Cost	Highest	Medium	Lowest
Security	Very high	Very high	High if certified
Scalability	Depends on implementation	Very high	Very high
Performance	Very high	Very high due to ability to cloudburst	Medium
Reliability	Very high	High	Medium to high
Fast deployment	Medium	Depends on mix of technologies	Very fast



# Agencies Move Toward Cloud Interoperability and Integration

As more federal agencies successfully move workloads to the cloud, they are beginning to realize the true benefits of cloud technology—scalability, cost savings, security and efficiency.

Despite the Cloud First initiative and more choices of FedRAMP-approved secure clouds, full-scale adoption of cloud technology is still elusive. Besides security, some agency CIOs worry about whether their legacy applications and data sets can fully migrate fully to the cloud. They're also concerned with whether multiple cloud instances within an agency will work together without compatibility issues.

Vendors and standards organizations are taking those concerns to heart. And they are making progress in eliminating those barriers. In the meantime, agencies can get these benefits by ensuring the cloud technologies they're using work together well.

One example is the close relationship between EMC, Dell, VMware and Virtustream. These companies recently came together in a series of mergers that ensure their combined technology stack will integrate seamlessly.

EMC's strength in traditional storage infrastructure and Dell's strength in computing technology, combined with VMware and Virtustream—a FedRAMP-approved public cloud provider—are a solid combination. Together, these solutions provide agencies with a full spectrum of options across public, private and hybrid cloud—as well as traditional IT infrastructure.

Adding Virtustream to the stack holds particular appeal for federal agencies. In addition to FedRAMP certification, Virtustream offers a secure way to move even mission-critical applications to the cloud. This is now part of EMC's Federation Enterprise Cloud solution.



## FIND THE RIGHT FIT

While the Dell/EMC/VMware/Virtustream stack is an excellent way to ensure integration and interoperability aren't deal-killing issues, it's not the only option. In fact, as FedRAMP certifies more public cloud solutions, there are more possibilities all the time.

More choices are always better, but too many choices can complicate the decision-making process. That's when it becomes particularly important to work with a partner that understands not only the technology options, but an agency's specific requirements and approach.

The hardest part of a federal CIO's job is making the business case for IT while considering the Cloud First initiative and the Federal IT Acquisition Reform Act (FITARA). Part of making the business case is determining the most cost-effective and efficient use of cloud. That means not only the best IT delivery model for each given IT service, but also which vendors can deliver the best solution. CDW-G works with every major manufacturer and offers federal agencies as much support as necessary to find the best solution.

Broad knowledge of technology and federal requirements are particularly important when it comes to security. "The underlying infrastructure has to be able to accommodate whatever security

parameters the CIO and CISO require, whether that's a FedRAMP baseline or something much higher," says Jack Nichols, Manager of Cloud Services for federal/state/local/education and healthcare at CDW-G. "Wherever they set the bar, we have to come up with a solution that meets those requirements."

## LOOKING AHEAD

The industry is making real progress in removing integration and interoperability barriers between cloud providers through open source software and standards. As vendors continue to work on ways for organizations to move seamlessly between cloud providers, agencies can look forward to a day when vendor lock-in will be a thing of the past.

"We're getting there. When it happens, agencies won't have to worry about locking themselves into long-term contracts," says Nichols. "Instead, when cost and other advantages present themselves, agencies will be able to switch cloud providers without worrying about portability, interoperability or security."



## GSA mulls new cloud acquisition vehicle

The General Services Administration is considering establishing a broad cloud-specific contracting vehicle that would help agencies handle their growing cloud service needs.

GSA's existing cloud blanket purchase agreements are expiring, and federal customers are evolving past the cloud services designations under GSA's Schedule 70 and other contracting vehicles that include cloud services. Therefore, the agency is thinking about creating a next-generation cloud-specific contract, said Stan Kaczmarczyk, director of GSA's Cloud Computing Services Program Management Office.

"We're working on a business case now" for what could be either a governmentwide acquisition contract or an indefinite-delivery, indefinite-quantity contract for cloud, he said at Washington Technology's Cloud and Mobility Industry Day event earlier this month.

Federal business volume for cloud services will reach \$2.254 billion in fiscal 2017, Kaczmarczyk said, adding that GSA's cloud infrastructure-as-a-service BPA has already expired and its email-as-a-service BPA will expire in two years, paving the way for a new contracting vehicle.

If everything goes smoothly, Kaczmarczyk said a request for information could be issued by September 2016. "We can't rush," he said. "We need to get it right."

The goal is to give GSA's customers a more streamlined way to acquire cloud services. The agency has already moved in that direction by dedicating a Special Item Number for cloud services on the IT Schedule 70 contract, Kaczmarczyk added.

— Mark Rockwell

## 18F hacked procurement and got code for \$1

Last month the General Services Administration's 18F set out to use micro-purchase authority to buy code by holding a reverse auction that started just under the \$3,500 threshold — at \$3,499.

The project involved loading Schedule 70 data into GSA's Contract-Awarded Labor Category tool, and winning bidder Brendan Sudol successfully finished a few days ahead of schedule, and he did it for \$1.

"I love reading about the innovation and impact that 18F, [U.S. Digital Service] and company are having in the government, and it's made me want to help contribute to the cause," Sudol told FCW. "Plus, I use open-source technology on a daily basis and saw this as a great opportunity to give back."

However, some bidders raised con-

cerns when they saw bids plummet from \$1,250 to \$1 in a single day. They said one bidder could log a \$3,499 bid, a colluding vendor could bid \$1 and then fail to deliver within the 10-day time limit so the higher bidder would get the project at the maximum rate.

In a Nov. 6 blog post, Acquisition Management Director V. David Zvenyach said 18F

was considering tweaks to its system. "In some respects, this result was the best possible outcome for the experiment," he

wrote. "It proved that some of our core assumptions about how it would work were wrong. But the experiment also validated the core concept that open-source micro-purchasing can work, and it's a thing we should try to do again."

— Zach Noble



**18F's V. David Zvenyach** said a recent micro-purchase experiment "validated the core concept that open-source micro-purchasing can work, and it's a thing we should try to do again."

### INK TANK



# Web Threats Target Industry

Industrial systems across the globe face increasing risks from cyber-threats.

**U**ntil recently, the Industrial Control Systems (ICS) industry saw itself as somewhat of an island. It was secure in its isolation from the Wild West of the Internet and the growing threat of cyber-attacks unleashed on networks and IT systems. As the formerly proprietary world of ICS has become increasingly dependent on commercial off-the-shelf (COTS) IT, that complacency has disappeared.

The security of most ICS environments is now described by many people in the industry as a “train wreck.” It’s all but non-existent. Using COTS technology and TCP/IP networks for connecting systems has opened ICS environments to the host of cyber threats now assaulting traditional IT systems.

The term ICS generally encompasses supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), programmable logic controllers (PLC), remote terminal units (RTU), intelligent electrical devices (IED), basic process controllers (BPCS), safety instrumented system (SIS), and operator panels and ancillary systems. The security trend in the industry, which is fortunately gathering speed, is to integrate ICS systems with IT networks and connect them through the Internet in order to improve the overall ICS capabilities.

“Advanced persistent threats (APTs) are a major headache



targeted at COTS products,” says Leo Medina, systems engineer at Juniper Networks. It’s a matter of simple crossover. “If you are using an off-the-shelf product that’s vulnerable to an APT, then [ICS COTS users] are going to take that vulnerability along with it.”

## WAKE UP CALL

While the ICS security problem has been developing for years, it wasn’t until the Stuxnet worm was discovered in 2010 that governments around the world became fully aware the extent of the problem. They realized their critical infrastructures, which were wholly dependent on ICS running smoothly, could be threatened by cyber thieves and hostile states.

Stuxnet was the first example of an APT found to have affected an ICS/SCADA environment. It was used to attack equipment at Iran’s Natanz nuclear facility, including the centrifuges used to

enrich uranium. It was apparently introduced into the computers that controlled and monitored the centrifuge speed. A similar approach might have been adopted for other systems to get them to override safety interlocks.

The ICS at Natanz were apparently air-gapped from the regular Internet and therefore presumed safe from the kind of remote attacks that had besieged traditional IT environments. However, Stuxnet was designed to be spread using USB flash drives. It was suspected to have been introduced via a contractor’s computer connected in some way with the Natanz computers.

It reportedly first penetrated Natanz systems at least a year before it was discovered, giving it a lot of time to find vulnerabilities and compromise the ICS. When analysts examined the Stuxnet code, they were astounded by its sophistication and complexity. It was well beyond

what had been seen in worms and viruses up to then.

Stuxnet was a wake-up call for organizations to the potential vulnerability of increasingly COTS and Internet connected ICS/SCADA systems. It was also a revelation to many hackers, who suddenly became aware of the potential of worms and viruses for specifically targeting ICS.

Over the past few years, there have been a number of different variations of Stuxnet found in many ICS environments. Hackers have developed other types of threats as well using easily obtainable hacker tools. In 2014, for example, security researchers noticed that Havex, a remote access tool (RAT) used in targeted attacks, had been aimed at ICS environments with “trojanized” variations of the ICS/SCADA manufacturers’ own control software.

Late in 2014, the Department of Homeland Security’s ICS-CERT organization issued an alert about malware called BlackEnergy. This was said to be spreading through ICS environments via Internet-connected human-machine interfaces. It was initially designed to steal information, but was considered readily adaptable to a more malicious industrial sabotage application. ICS-CERT said BlackEnergy could have been burrowing into U.S. ICS environments since 2011.

In its 2015 Annual Threat Report, Dell described a massive two-year increase in worldwide ICS/SCADA attacks, from slightly less than 92,000 in January 2012 to more than 675,000 in January 2014. Buffer overflow attacks—something common in traditional IT environments—were the primary method for a quarter of these. However, it warned, this might not paint the whole picture.

“Because companies are only

required to report data breaches that involve personal or payment information, SCADA attacks often go unreported,” the report states. “As a result, other industrial companies within the space might not even know a SCADA threat exists until they are targeted themselves.”

This lack of information sharing, combined with the vulnerability of industrial machinery due to its advanced age “means that we can likely expect more SCADA attacks

on how to achieve cybersecurity for energy delivery systems. Since then, it has been funding development of security tools aimed at specific elements of the delivery infrastructure.

“Cybersecurity is one of the most serious challenges facing grid modernization,” says Patricia Hoffman, assistant secretary for DOE’s Office of Electricity Delivery and Energy Reliability, “which is why a robust, ever-growing pipeline

## “CYBERSECURITY IS ONE OF THE MOST SERIOUS CHALLENGES FACING GRID MODERNIZATION”

—Patricia Hoffman, assistant secretary for DOE’s Office of Electricity Delivery and Energy Reliability

to occur in the coming months and years,” according to the report.

### POWER GRID AT RISK

Most of the ICS environment in the U.S. is in the hands of the private sector, but with energy infrastructure such as electricity grids, power plants and oil refineries seen as one of the biggest targets of cyber-attacks, the federal government is taking an active role in trying to boost security. The potential for disruption and chaos following a successful attack is potentially wide-ranging. This is due to what the Department of Energy (DOE) calls the “increasingly interdependent” nature of virtually all sectors of the nation’s energy system.

“Further,” states the DOE in its recent 2015 Quadrennial Technology Review, “the power grid, buildings, manufacturing, fuels, and transportation sectors of the energy system are necessarily coupled to water systems, material flow, waste products, and energy financial markets.”

In 2011, it published a roadmap

of cutting-edge technologies is essential to helping the energy sector continue adapting to the evolving landscape.”

The Department of Defense (DOD) is itself a large owner and operator of ICS, with around 2.5 million unique systems spread across 500 installations worldwide. Once it develops the appropriate policies, it intends to accurately inventory all its ICS systems, and then develop automated measures to detect, patch and manage cyber vulnerabilities across the DOD’s ICS infrastructure.

In 2014, the DOD also decided to drop its DoD Information Assurance Certification and Accreditation Process (DIACAP) and adopt the National Institute of Standards and Technology (NIST) risk framework as the basis for certifying and accrediting cybersecurity processes. As far as ICS is concerned, that means the DOD is now using NIST’s special publication 800-53. This defines the security safeguards to use with industrial control systems.



The Obama Administration published an overarching policy document in 2011 that federal agencies are supposed to follow as a guideline. The President's executive order—Improving Critical Infrastructure Cybersecurity—called the cyber threat to critical infrastructure “one of the most serious challenges we must confront.” And that challenge only continues to grow.

## ADVERSE EVOLUTION

Many of the security weaknesses in current ICS environments stem from the evolution and automation of the industrial control sector over the years. There has been movement toward ensuring those environments could run for a long time without requiring much human intervention. Reliability and stability were the overarching industry standards.

That led to such things as default passwords being hard coded into Ethernet cards and other parts of the environment. This allowed for fast remote login by administrators. Also, given the stable nature of many of the systems, there was very little patching for operating systems and applications required over time.

That's fine for a closed legacy environment, but it becomes a glaring vulnerability once COTS enters the picture and communications open to the Internet. Also, many ICS systems and control devices have been installed using factory settings, or with preset standard configurations. Those factors make legacy ICS an easy mark for hackers and thieves. They introduce malware into the environment via COTS vulnerabilities.

“Having such things as embedded passwords just can't be tolerated anymore, it's only a matter of time before they are exposed,” says Prem Jadhvani, chief technology officer at Government Acquisitions, Inc.

(GAI). “We have to take this very seriously and use the same best practices that are deployed in the non-ICS world, everything from file integrity monitoring to end-to-end encryption, dynamic white listing, memory protection and so on.”

The sooner these kinds of controls are adopted, he says, the better off the ICS/SCADA environments will be.

Sufficient security controls are not the only problem. COTS and Internet-related threats are a new phenomenon ICS organizations know they must tackle. However, there is major cultural resistance from workforces that haven't faced these issues before.

They push back against disruptions to the kinds of business flows they've been using to get their work done. Training employees to understand the problems posed by concepts such as spear phishing, zero day attacks and APTs—now common practices in many on-ICS environments—is still foreign to them.

That lack of awareness is exacerbated by the fact that there is still a lack of trained manpower and skilled people within the ICS industry who understand the problems. Therefore, various tools are often thrown at the problem as point solutions in an attempt to plug security holes. They often don't work together, and the skills needed to know how to select the right ones and make them effective don't exist.

Many ICS/SCADA facilities in the U.S. are also run by local authorities. Faced with persistent budget constraints, many of these also don't have the money to hire the extra personnel needed to deal with these advanced security issues.

None of this is conducive to building the kind of infrastructure—an integrated end-to-end platform, processes that allow for automated systems, all overseen by skilled and motivated employees—required for an ICS environ-

ment that can react to security threats proactively and in real time.

The origins of threats now faced by ICS environments will be familiar to non-ICS IT organizations. They include:

- Contractors
- Corporate intelligence
- Criminals/organized crime
- Disgruntled staff
- Foreign intelligence services
- Hackers
- Internal attackers/bystanders
- Protestors and activists
- Staff undertaking unauthorized actions
- Terrorists

Potential attackers also have relatively easy ways to find ICS targets. SHODAN, for example, is a Google-like search engine designed to find Internet-connected devices. It indexes Web message header information. This easily locates devices such as routers, servers, traffic lights—and industrial control equipment.

It contains a wealth of information that can be useful to potential attackers, including IP addresses, geographic location, service port header information, firmware details and so on. It's also freely available on the Web for use by anyone.

As of January 2014, a 20-month academic research program called Project SHINE (SHodan Intelligence Extraction) identified more than 2 million ICS/SCADA devices connected to the Internet. Many of these devices are thought to be completely unprotected.

## ASSESS AND EXECUTE

The first thing all ICS environments should do to improve security, says Jadhvani, is conduct a full risk assessment. The goal is to identify the level of actual risk to the organization and establish the “risk appetite.” Some may be willing to expose themselves to a higher risk if the return is justified.

In order for the controls to be effective, he says, we have to get away from the stove-piped nature of security products and take an integrated platform approach such that the cybersecurity and physical security solutions become an integral part of the industrial systems lifecycle. For the ICS cyber security program to be effective, it is necessary to apply the “defense-in-depth” and “continuous monitoring” solution strategy, layering security solutions such that the impact of a failure in any one mechanism is minimized and the new advanced targeted and zero day attacks can be effectively mitigated.

This process has the added benefit of making those organizations do a full inventory of their ICS/SCADA devices. A big problem now is many organizations, particularly larger

tailored to the ICS environment.

“Many of these differences stem from the fact that logic executing in ICS has a direct effect on the physical world,” the guide states. “Some of these characteristics include significant risk to the health and safety of human lives and serious damage to the environment, as well as serious financial issues such as production losses, negative impact to a nation’s economy, and compromise of proprietary information.”

The NIST SP 800-82 ICS security guide advises on how to reduce the vulnerability of computer-controlled industrial systems to malicious attacks, equipment failures, errors, inadequate malware protection and other threats. SP 800-53 contains a catalog of security controls that can be tailored for specific needs

security guidelines verses SP 800-53, and how to tailor the controls for low, moderate and high impact ICS.

The European Union Agency for Network and Information Security (ENISA) also has its own set of ICS security standards, guidelines and policies. These can augment those put out by NIST.

In a June 2015 survey, the SANS Institute looked at the current state of ICS security and confirmed the lack of trained and skilled ICS security practitioners. It also found a lack of visibility into ICS equipment and network activity. This situation limits the confidence organizations can have in truly knowing their levels of vulnerability and just how many breaches they are experiencing.

On the positive side, the survey says, collaboration between IT and control systems personnel is on the rise. The number of products and services that provide the necessary insight into ICS threats and vulnerabilities is increasing.

The SANS Institute survey says it hopes organizations with the most to lose, particularly those built on dependency and reliability of their control systems, “will recognize the rising level of risk and focus their resources on addressing the serious threats to their continued operations.”

## “THE FIRST THING ALL ICS ENVIRONMENTS SHOULD DO TO IMPROVE SECURITY IS CONDUCT A FULL RISK ASSESSMENT.”

— Prem Jadhvani, chief technology officer, Government Acquisitions, Inc.

ones, don’t know how many devices they have and where they are located. Even if they secure those devices of which they are aware, any other devices left unsecured give attackers a way into the interconnected ICS environment.

NIST’s approach to securing ICS, the primary resource in this area for both government and the private sector, is detailed in its special publication 800-82—Guide to Industrial Control Systems (ICS) Security. The most recent version of this was released in June 2015. In that guide, NIST stresses that ICS environments more frequently resemble regular IT systems, but there are differences and some cases require new solutions

according to an organization’s mission, operational environment, and specific technologies. ICS also have unique performance and reliability requirements, as well as other factors. They can use operating systems and applications unfamiliar to regular IT personnel, says NIST. Plus the goals of safety and efficiency occasionally conflict with security in control system design and operation.

Recommendations for IT security controls are included in NIST’s SP 800-53, Revision 4, published in April 2013. It includes a reference to NIST’s own Risk Management Framework, and how to apply that to ICS security. SP 800-82 also includes overlays of the NIST ICS

**JUNIPER**  
NETWORKS®

For information on Juniper Networks federal solutions, please visit [www.juniper.net/federal](http://www.juniper.net/federal)



Please contact Government Acquisitions, Inc. (GAI) at 513.721.8700 to learn more about taking the first step in securing your agency with a full risk assessment.

For information on GAI’s cyber security solutions please visit <http://gov-acq.com/solutions-capabilities/cyber-security/>

# 35 percent

is the average shortfall in agency pay compared to non-federal workers doing similar jobs, the Federal Salary Council found

## EDITOR'S NOTE

### Federal 100 nominations are due by Dec. 23

The deadline for the 2016 Federal 100 awards is fast approaching. So please help the most exceptional members of 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 is the most prestigious award in federal IT — and for good reason — and it all starts with a great pool of nominees.



If you know individuals 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 award is for individual accomplishments in 2015.

3. Winners go above and beyond — whatever their level or rank. A fancy job title is not required, and doing one's job well is not enough.

4. You are allowed to 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](http://FCW.com/2016fed100) for details, and submit your nominations today.

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

## SPECIAL REPORT: VIRTUALIZATION

ONLINE REPORT  
SPONSORED BY:



# DELIVERING ON THE PROMISE OF VIRTUALIZATION

## TOPICS INCLUDE:

VIRTUALIZATION  
HELPS AGENCIES  
REACH IT GOALS

SOFTWARE-DEFINED  
PLATFORMS  
DEFINE FUTURE OF  
VIRTUALIZATION

THE PROMISE OF  
CONTAINERS

SERVICE  
VIRTUALIZATION  
COULD BE BIG FOR  
DEVOPS

VIRTUALIZATION  
SECURITY: THE GOOD  
AND THE BAD

TO LEARN MORE, VISIT: [FCW.COM/2015SNAPSHOTVIRTUALIZATION](http://FCW.COM/2015SNAPSHOTVIRTUALIZATION)



## Wish they all could be...

The administration is right to be building bridges with the tech community.  
But there's talent to be found outside California.

With sincere apologies to the Beach Boys circa 1965, federal IT leaders continue to be enamored with the California girls and boys of Silicon Valley. In the past several months, smitten suitors have made the trip to California to press their thirsty lips to the fountains of agile and innovation knowledge.

Examples abound, including:

- Last month, ACT-IAC held meetings in San Jose with a number of enterprise companies, venture capital firms and select startups.
- The Professional Services Council will hold a similar session this month with the California Technology Council.
- The departments of Defense and Homeland Security are both opening offices in Silicon Valley. Deputy CIO Margie Graves said DHS is looking into new ways to collaborate with tech start-ups, including inviting them to work on pilot projects and other approaches that side-step the official contracting process.
- Programs like 18F, the Presidential Innovation Fellows and the U.S. Digital Service have targeted Silicon Valley technologists for term appointments in government.

All those efforts are well-intentioned, but perhaps some perspective is in order.

We first met in the early 2000s, when Mark Forman was named the first U.S. CIO, IT spending was growing at close to a double-digit rate and the White House's e-government initiatives were being launched. Alan Balutis had just left

public service to lead the Industry Advisory Council, while Stuart Robbins, who founded the CIO Collective, was working with a number of Silicon Valley firms that wanted to get into the federal market. We both agreed to work with Forman and his staff to build better bridges between the tech community and the public sector.

Although much has changed since the early 2000s, especially with the actual technology, some fundamental issues remain.

Although much has changed, especially with the actual technology, some fundamental issues remain. We offer the following thoughts and suggestions because of our long history as advocates for public/private collaboration:

- The new generation of General Services Administration and Office of Management and Budget employees are bright, energetic and committed to building bridges between D.C. and the tech community, especially in Silicon Valley.
- The young leaders from the venture capital community are equally bright and energetic, but they are somewhat naïve about business

complexity inside the Beltway. They are similarly uninformed about legacy systems, legislative complications and the Washington bureaucracy (of which at least some knowledge is necessary).

- Relatively few companies or people outside the Beltway know about initiatives like 18F and the Presidential Innovation Fellows. A broader marketing and outreach campaign could be more useful than creating additional pathways for business.
- Getting rid of regulatory complexity is a nice idea, but there is a reason for and value in programs like FedRAMP, which vets candidates and eliminates those that do not have the discipline or rigor to provide business at scale. If a company can't meet those requirements, maybe it should recognize that it won't be able to "hit big league pitching" when it comes to federal IT.
- There seems to be little or no appreciation for state and local governments as proving grounds for new technologies. And we see scant interest at the federal level in intergovernmental partnerships as an expanded marketplace for pilot projects that could solve citizen problems while simultaneously serving as a test bed for solutions that could scale to the federal level.

If we aren't pilloried for these initial observations, we might have more to offer on this subject in the future. In the interim, we welcome your feedback. ■





# A breach is coming — is your agency ready?

The key to successfully navigating a security breach is to develop a three-pronged, comprehensive incident response process ahead of time

Advanced threats are spreading at an alarming rate, putting agency data at risk and making attacks almost inevitable. In July, the Government Accountability Office reported that information security incidents involving federal agencies skyrocketed from 5,503 in fiscal 2006 to 67,168 in fiscal 2014.

If recent high-profile incidents are any indication, those numbers will only further increase in the years to come. Agencies should assume that they are at risk for a breach and implement processes for post-incident recovery.

A well-designed incident response plan gives agencies the tools necessary to respond to an attack, investigate the causes of a breach and manage internal and external communications. Such plans should involve a three-pronged approach:

**1. Define the conditions required for a response.** Agencies must differentiate between security “events” and security “incidents.” CEB defines a security event as any observable occurrence in a system or network — for example, a user connecting to file sharing or a firewall blocking a connection attempt. By contrast, a security incident is an event that results in or presents an imminent threat of a violation of computer security policies, acceptable-use policies or standard security practices.

All security incidents are security events, but not all events are incidents. Security incidents include denial-of-service attacks, infiltration

by malicious code or unauthorized access to sensitive information. Those incidents should trigger the agency’s response process, but if agencies were to automatically respond to every security event, they would waste time and resources chasing endless false alarms.

**2. Create an incident taxonomy.** The second step involves the creation of a standard set of labels known as an incident taxonomy. It allows agencies to categorize incidents within well-defined

If recent high-profile incidents are any indication, the number of attacks will only increase in the years to come.

parameters to more quickly identify patterns, which enables a faster response to common types of incidents and streamlines trend analysis.

Although 83 percent of organizations use a taxonomy system, there is no overwhelming preference for a specific type, according to CEB’s research. However, the taxonomy an agency selects is not as critical as the fact that it chooses and maintains one for consistency.

**3. Follow the protocol for recovery.** Once agencies have categorized their triggers and taxonomies, they

should focus on recovery protocols, which are the most valuable accelerators to a rapid recovery. In order to adopt effective response protocols, agencies should create processes that span four distinct phases:

• **Preparation** — Select a specialized incident response team, a single point of contact and a system for evaluating and tracking the external threat environment. In our research, 89 percent of organizations have designated a single point of contact for incident response coordination and leadership.

• **Detection and analysis** — Develop a strategy for monitoring a variety of channels that are responsible for detecting incidents. And create consistent severity categories that align with levels of resource allocation and response timelines.

• **Containment, eradication and recovery** — Establish workflows for responding to various incidents, including formal action plans that empower incident response teams to react quickly. Also, ensure that officials are communicating clearly with all stakeholders and maintaining processes that enable the collection of evidence for analysis.

• **Post-incident response** — Require postmortem assessments that facilitate organizational change and reinforce the importance of operational improvement.

By assuming that system attacks are imminent and planning accordingly, federal agencies can limit the actual attack and manage the resulting impact. ■



# Hyperconvergence Simplifies the Data Center

## Virtualizing servers, applications and the network reduces equipment and management costs

**I**T resources—equipment, software, real estate and man hours—continue to sprawl in an attempt to keep pace with demand. For federal agencies, this never-ending data center creep has crowded innovative development out of budgets. Agencies struggle with increasing operations and maintenance costs as the demand for storage and processing power expands.

Over the years, going back to the Reagan administration, the government has made repeated attempts to consolidate its data centers to reduce footprint, curb redundancy, trim excess capacity and untangle complexity. Despite sustained efforts over the last few years, the current Federal Data Center Consolidation Initiative has barely made a dent, as agencies have been struggling to get an accurate count of the centers they have and determine which should be closed.

Agencies have recently shifted their emphasis to data center optimization, using virtualization and smaller form factor servers to improve efficiency. Such efforts have reduced costs, but haven't yielded substantially more available budget for innovation.

The problem is that we keep trying to address the sprawl with the same technologies that got us here in the first place. The anxiety each fiscal year is around how we are going to purchase more of the same stuff? We have more data, therefore

we must need more storage. We need more processing power, therefore we must need more servers and networks. But why try to solve the problem with more of the same? What if federal CIOs and IT shops radically changed the way they address their needs for storage, networking, and compute capacity? Such a solution does in fact exist. In fact, some 170 federal programs are already supported by it. It is already radically reducing data center costs while improving mission support, security and manageability.

### Come Together

This solution is hyperconverged infrastructure – the combination of servers, storage, and storage networks into a single appliance. The virtualization revolution dramatically optimized industry-standard servers, enabling similarly dramatic server and data center consolidation. However, in order for virtualization to effectively perform its magic, it required massive amounts of redundant storage and networking capacity. That traditional 3-tier architecture is as inefficient and unsustainable as pre-virtualization data centers were. Yet storage and compute requirements keep multiplying, driven by mobility, big data and the Internet of things. Enter hyperconverged infrastructure. Allow us to deconstruct. Traditional storage architecture

leverages a three (or more) tier hierarchical subsystem, accessed by servers via a network—itsself composed of an array of switching devices. By moving the storage intelligence into software and running that software directly on the servers in a hyperconverged infrastructure, the once-inefficient and proprietary storage area network (SAN) is eliminated. Instead, standard top-of-rack switches are used to connect the environment as a cluster of resources. This model appears as a standard 3-tier environment to a hypervisor, but the underlying architecture is radically simpler, with exponentially fewer areas to troubleshoot and monitor, and significantly smaller in overall rack space. This eliminates the need to perpetuate legacy 3-tier architectures for virtualized environments. Instead, this brings software-defined storage to virtualized environments.

“Physically it's much simpler,” says Jason Langone, director of OCONUS and Tactical Programs for Nutanix. “What hyperconvergence has done is moved the logic of the shared storage array—the deduplication, data compression, replication—everything you expect in enterprise storage, and put that in software that runs directly on the servers.”

Nutanix hyperconverged infrastructure uses the company's own hypervisor for storage and evolves virtualization by an order of magnitude. Therefore,

hyperconvergence produces two seemingly opposed benefits. It gives the IT shop a step function reduction in the cost and complexity of the data center by collapsing storage into a virtual, software-defined subsystem. Yet it preserves investments agencies have made in Microsoft, RedHat or VMware hypervisor technologies—all of which can run on the Nutanix platform.

Virtualizing storage reduces complexity by incorporating storage management and control into the same appliance as the storage and compute hardware. The resulting turnkey form factor represents up to a 90 percent reduction in rack space. Equally important, hyperconvergence is massively scalable, enabling agencies to add capacity without adding complexity.

## A New Kind of Architecture

The emergence of large organizations built on a virtual presence, most notably Google, Facebook, and Amazon, is possible because of a new approach to data centers. This approach—known as web-scale architecture—represents a new use of standard hardware components, open APIs, and deep virtualization—including storage.

Web-scale architecture is built around distributed system design. An instance of a given service could fail and the distributed system immediately heals around the failure, without user intervention. Web scale architecture does all the intelligence in software, without proprietary hardware. These are the lessons that organizations like Google have learned over the last decade.

“There’s a lot of desire to have AWS-like capabilities, to have resources on line and available,” says Langone. “[Federal agencies] are looking for more consumer

grade user experiences, and much quicker access to resources. They’re looking for something like Amazon within the confines of their own IA and their own datacenter.”

Federal agencies can also realize the benefits from web scale architecture used to transform traditional data centers to sleek, high performing private clouds.

■ **Radically smaller space requirements:** Agencies save on the air conditioning, power and real estate costs that go along with floor space. For its IT support, one program required 60 racks of traditional gear. By moving to a hyperconverged infrastructure, that requirement shrunk to merely six racks. Infrastructure itself is dramatically smaller with hyperconvergence.

■ **Logistically easier field operations:** The smaller physical footprint and fewer moving parts are boon to the military services supporting field operations.

■ **Simple, inexpensive scalability:** No more buying double the storage capacity every year or the long procurement approval cycles and costly “rip and replace” operations required by bulky new infrastructure. You can grow capacity much faster by simply adding hyperconverged appliances incrementally, each about the size of a PC. This all means that an agency can at last have, in its own facilities, true cloud benefits while retaining critical data within government walls.

■ **Greater cybersecurity:** An Army general in the cyber command recently commented the consolidation of IT resources reduces the attack surface for malicious hackers. Hyperconvergence radically reduces the data center attack surface. Plus, the appliance’s software bundle includes two-factor authentication—a requirement for privileged users coming from recent Office

of Management and Budget policy.

■ **Stronger data protection and mission assurance:** The Nutanix backup and virtual machine restore capabilities are baked in, resulting in optimal recovery point and time objectives, among other features.

■ **Lower costs:** The space and power savings, mass storage reductions and ease of administration via a user-friendly management Web interface trim expenses. In addition, procuring one solution and related service and support, versus three different elements in a traditional storage approach, is inherently less expensive in hard and soft costs.

In the long term, the hyperconverged infrastructure allows agencies to reset their priorities. The data center, instead of being a cumbersome cost, becomes an agile, quickly scalable resource that supports existing enterprise applications at a high level of performance, while also helping to realize the promise of emerging solutions, such as big data, digital services and mobility.

This is the point of the data center consolidation initiative, the Federal Information Technology Acquisition Reform Act, and the overarching federal digital strategy: To start tipping expenditures away from the operation and maintenance of legacy systems and toward innovations in online services and operations that support an agency’s mission.

To learn more about how Nutanix is a force for innovation in the Federal government, see our use-cases at: <http://www.nutanix.com/solutions/federal-government/federal-use-cases/>

**NUTANIX**





# CAN TONY SCOTT GET IT ALL DONE?

The U.S. CIO has made a mantra of 'land the planes' and pushed notable improvements in his first nine months. But the to-do list for 2016 is long indeed.

BY ADAM MAZMANIAN

When U.S. CIO Tony Scott started making the rounds at Washington-area events in March, about six weeks after his appointment, he projected a calm, unruffled demeanor and showed a knack for staying on message with his metaphors.

He told audiences he had come to town from Silicon Valley to "help land the planes." As an experienced pilot, Scott said he knew that getting into the air was the easy part. And under President Barack Obama, whose administration formally created the U.S. CIO position, there was plenty of air traffic when it came to federal IT.

The 25-point IT management reform plan of the first CIO, Vivek Kundra, promised to have agencies moving IT operations to commercial cloud providers, put acquisition of commodity IT on an enterprise-wide basis and monitor risky projects using a data-driven oversight process.

Steven VanRoekel, the second U.S. CIO,

pushed PortfolioStat and launched the U.S. Digital Service, an effort to embed forward-thinking design, acquisition and usability specialists inside agencies' IT organizations to transform and modernize how the government imagined IT. Congress had passed the Federal IT Acquisition Reform Act, and implementing the new law was going to be a big job, requiring a technology rethink across all levels of the federal government.

Scott — a corporate CIO with experience leading IT organizations at VMware, Microsoft, Disney and General Motors — did not come armed with a lengthy agenda like Kundra or speak management-guru like VanRoekel. He showed up at events without the protective screen of a confidential assistant or Office of Management and Budget press handlers. He was entirely believable in the role he cast for himself: a dedicated IT manager who came to Washington, despite the terrible weather and worse traffic, to help land the planes.

But not long after Scott started, the planes crashed.

PHOTOGRAPH BY ROBERT SEVERI

## People

The theft of personal information on 21.5 million federal employees and their families from the Office of Personnel Management, including the breach of the database of forms on employees seeking security clearances, was the most devastating cybersecurity event to strike the U.S. government to date. The infiltration, discovered in mid-April, upended Scott's plans for an orderly execution on existing policies and spurred a governmentwide "sprint" to tighten up cybersecurity, with a focus on two-factor authentication and the use of personal identity verification (PIV) cards.

Scott didn't exactly see the OPM hack coming, but he wasn't totally surprised either. In a recent interview with FCW at his office in the Eisenhower Executive Office Building, Scott said he knew going in that the vulnerability of federal systems needed to be addressed.

"When I first came on board, one of the things I had a strong sense of is cyber is one of the areas that we're going to have to double down and really pay a lot of attention to," he said. "You could look around you and see in the retail sector, in the banking sector, in the media and entertainment sector, to name a few, that there had already been a series of pretty eventful occurrences. To believe that the government was somehow immune from that was probably not credible."

He added that the OPM hack "put an exclamation mark on the work that I already thought we were probably going to need to do. At the end of the day, I don't think it changed things all that much, although there were a few weeks in there where obviously we got some extra work to do."

As part of a longer-term initiative to protect networks, Scott released the Cybersecurity Strategy and Implementation Plan for federal civilian agencies on Oct. 30. That document offers definitions for what constitutes a "major breach" and gives agencies a blueprint for responding. It is complemented by the 2016 Federal

Information Security Modernization Act guidance and a long-awaited update to OMB's Circular A-130. Agencies are now required to identify "high-value assets" that need special protection, and CIOs are tasked with identifying systems that rely on older infrastructure and are due for modernization.

"Coming out of this sprint we asked people to look at your high-value assets," Scott said. "Then we asked [CIOs and chief information security officers] to make a risk-based assessment about whether things are adequately protected or not."

There is more antiquated technology in government than Scott would like to see, but he takes a realistic view about where modernization activity should be focused.

"I would love to see all Windows Server 2003 systems upgraded or replaced," he said. "But if they're not in a place where it's the highest priority threat or there's any threat at all, then I care a lot less about it."

Scott is also realistic in accepting that — despite the best efforts of his team at OMB and IT shops across government — federal systems will continue to be targeted.

"I don't care if you're the local 7-11 store or the U.S. federal government," he said. "The number of attacks is going up."

At the same time, Scott stressed that feds are improving their batting average when it comes to deflecting attacks.

Agency IT leaders have generally given Scott high marks in return. "I think he's done a very good job — especially when it comes to keeping important work moving in the face of so many potential distractions," Federal Communications Commission CIO David Bray said.

Scott has also put much-needed emphasis on cultivating leadership in the IT ranks by not just recruiting from the private sector but also developing talent internally, Bray said.

"We need to think about how we can

work with the folks we already have," he added.

Indeed, while the hiring and deployment of the digital services teams — which were pioneered in the wake of the HealthCare.gov launch debacle — continue, Scott stressed that there is still a lot of work to be done.

"I think the digital services are a great example of the surgical use of a very special kind of talent to act as a catalyst for certain things," Scott said. "Where the digital services teams have done work, they've really made some important contributions in the most critical of the consumer- or citizen-facing services."

However, he said, those teams "are not designed today to do the heavy lifting of taking these old, siloed systems and moving them to a modern platform.... Mostly we've focused them on citizen-facing kinds of services, where frankly there was a lot of work to do as well."

### From Silicon Valley to the Oval Office

Scott said he was happy as CIO at VMware and didn't give much thought to government work. Even though he worked at a leading cloud vendor when "cloud first" was the declared goal of the Obama administration, Scott focused on technology and not the marketing of VMware's services to government.

"Coming here, I had to get up to speed as quickly as one can on the ways that government buys stuff," Scott said.

He was first approached at a technology conference in September 2014 and asked to help with White House efforts on diversity and nontraditional hiring in technology. He invited some friends and CIOs to a conference, after which, Scott said, "I naively thought I was done."

Instead, he was recruited by U.S. CTO Megan Smith, a former Google executive; Todd Park; Beth Cobert, who was OMB's deputy director for management at the time; OMB Director Shaun Donovan; and others in the West Wing.

"Over time it became apparent that it was a challenging opportunity and one where I felt that I could make a unique contribution," Scott said. He came on board in February.

In his second day on the job, Scott found himself in the Oval Office briefing Obama. Although Scott declined to share details on his interactions with the president, he said he has offered advice on a range of issues related to IT in government. Scott's was among the voices that prevailed in the long-running conversation about how to handle high-grade commercial encryption.

"At the end of the day, I think the better policy is probably not to require these backdoors" for law enforcement to access encrypted communications from commercial providers, Scott said. The problem is as much practical as it is technological, he added: Smart programmers who aren't subject to U.S. law will put functionally unbreakable encryption on the market.

"All the really bad people who are highly motivated to keep their stuff secret are going to use the encryption method that doesn't have a backdoor," he said. At the same time, by giving law enforcement a window into encrypted communications, the government would create an "easy button" that could end up thwarting other investigative work.

"It actually makes you a little less effective than if you used all of the tools and resources that are available to you," Scott said.

### **Political cover for a final push?**

Scott has been pleased with his relationship with Congress. He has appeared before committees to talk about the OPM hack, FITARA implementation and other IT issues. At the same time, he noted, the bipartisan agreement about IT is centered on the perception that federal agencies are moving too slowly to modernize, spending too much money, and relying

on creaky and vulnerable technology.


"Most people agree that there's a lot of work to do [and] that we're way behind the point where we should be and way behind private industry in terms of modernizing," Scott said.

He said he is seeking to advance the IT procurement cause now that FITARA is law by talking more seriously about funding mechanisms that can be used to "accelerate the move to some more modern platforms."

stay around until the lights go out on the Obama administration.

"It's been both the opportunity and the challenge of a lifetime," he said. "I'm going to stick it out as long as they'll have me."

By the end of the term, Scott said he wants to get to 100 percent use of PIV cards for privileged users of federal systems. He would also like to see more significant progress on replacing outdated systems, an overall reduction in the number of privileged users and more attention



**"Where the digital services teams have done work, they've really made some important contributions in the most critical of the consumer- or citizen-facing services."**

And so far, Scott appears to be well-liked on the Hill.

"Tony's got a very difficult job, but he has a great background and experience on how to do it," Rep. Will Hurd (R-Texas) said. "It seems like he's getting the right kind of support that he needs in order to be successful at his job. I think he's a smart guy, he's a thoughtful guy, and he knows how to work with people."

Hurd, a former CIA officer and cybersecurity specialist who leads the IT Subcommittee of the House Oversight and Government Reform Committee, added, "This is an issue that transcends political affiliation. This is about protecting the federal government, this is about protecting the citizens of the United States of America, and this is something that... shouldn't be tainted by partisanship."

Scott, for his part, said he hopes to

paid to patching existing vulnerabilities.

"One thing I know from my private-sector experience — and I think it holds true in the public sector — is if you're slow, you're dead," he said. "So you'd better figure out how to be faster and faster and faster, or I don't like the outcome. Certainly, federal IT has to become that way."

Scott knows it is impossible to leave a clean in-box for his successor, whether he or she serves in a Democratic or Republican administration. But he'd like to leave a playbook behind for the next U.S. CIO — something that would serve as "a homework list for my successor that outlines, at least from my perspective, the opportunities and challenges" of the role.

He also plans to attach a note that reads, "Congratulations. It's the best job you'll ever have." ■

# YOUNG LEADERS TO WATCH [ IN 2016 AND BEYOND ]

---

There are 14 months remaining in President Barack Obama's administration, but the exodus has already begun. Political appointees are starting to leave, while retirements from the career federal workforce hint at demographics that have worried IT leaders for years.

Those fearing a hollowed-out IT community, however, should take a look at the talent coming up through the ranks. Young women and men — in agencies and the private sector alike — are overachieving in their current roles and distinguishing themselves as the likely leaders of tomorrow.

Each year, FCW honors such individuals with the Rising Star awards. Nominations come from all corners of federal IT as peers and managers point out early-career colleagues who are going above and beyond to make government perform better. And as this year's 14 winners make clear, there's plenty of leadership potential waiting in the wings.





## Lindsay Burack

Lindsay Burack got interested in web design while working on Capitol Hill for a firm that specialized in market research and political polling and outsourced its design work. Intrigued, she took some courses in graphic and web design and subsequently landed a job at Living Social in 2010, during that startup's early days. She worked out of a small office in D.C.'s Chinatown neighborhood, where she shared desks with other employees.

"I got to see the inner workings of a new-age startup," Burack said. "It was a really small group at the time. It was all hands on deck."

She loved focusing on the user experience, but missed government. So in early 2013, Burack joined Sapient Government Services as an information architect, and ultimately got to work on the National Cancer Institute's Cancer.gov website. She helped streamline the site to make it work better on mobile devices, and

she rewrote content and removed old and duplicated information. In the end, she pared the site's 24,000 pages down to 6,800 and built in support for social sharing.

The revamped site that launched in May is much more accessible to the approximately 40 percent of users who visit it via mobile devices.

"It was gratifying on many levels," Burack said. "I'm so proud to know that we've made it easier for cancer patients, researchers and advocates to find information."

Like many people, she has loved ones who have battled cancer, including a young cousin with breast cancer.

Managers at Sapient said Burack and her team transformed the customer experience because they understood the importance of getting cancer-related information to people in a way that is empowering. She continues to make improvements to

Cancer.gov based on analytics and user feedback.

As for companies that might try to lure her away from government, Burack said she intends to continue working in the public sector.

"I love that here I get to do tech work and user experience and all that stuff that's really interesting to me, but I still get to do something good for the world in the public sector," she said. "That's really the best part... about this job."

Burack's advice for others — and particularly for women eyeing careers in tech — is to be passionate, know your strengths, and learn as much as you can from the mentors and core senior people around you.

"Not holding back, putting in the extra work and really caring about your work — I think that can definitely propel any woman forward," she said.

— Bianca Spinosa

## 2015 Rising Stars

### Michael H. Brody

As director for policy, architecture and governance at the Department of Homeland Security's Information Sharing Environment Office, Michael Brody is expected to be an expert on rules.

According to his managers, how-

ever, it's Brody's deft communication skills, management acumen, cross-boundary view and sense of humor that make him so effective. He was promoted to his current position after just one year at DHS, and his ability to reconcile mission needs with privacy protections has elevated his work.

He has a knack for bringing together officials with wildly disparate and often opposing views to make progress on common goals despite those differences. He led the effort to improve the processes and strategy for the Information Sharing and Safeguarding Governance Board — no easy feat because it required close consultations with DHS' many independent-minded components.

He also rallied support for the Homeland Security Information Network, a collaborative platform for more than 40,000 state, local, territorial, and tribal law enforcement and emergency responders — even though he was only supposed to provide policy expertise for HSIN's day-to-day operations and for managing security events and incidents.

Brody said that at its heart, his work has a much deeper purpose.

"Our work ensures the [Office of the CIO] delivers what mission operators need to save lives, protect property and secure the homeland," Brody said. "The DHS OCIO's Information Sharing Environment Office is the bridge between the information-sharing mission and information technology."

— Mark  
Rockwell

— Mark Rockwell

### Akosua Ali

Akosua Ali is unusually good at making sense of complicated, sometimes disjointed environments. As a management program analyst and contracting officer's representative at the Department of Homeland Security, she ironed out complex acquisition issues and found millions in unused funds.

She led multiple IT contract reconciliation projects that involved analyzing complex financial reports, researching contract actions in DHS' PRISM financial system and meeting weekly with all stakeholders. She meticulously analyzed funds left over from previous years for the CIO office's largest IT services and support contracts and worked with vendors to find unused money that could be made available for other procurements or turned over to the Treasury Department. Her efforts uncovered more than \$15 million that might otherwise have been lost.

Her superiors said Ali has improved the process for administering IT services and support funds at DHS. Beyond tracking down unused money, she developed training on

invoice processing, and established best practices and standard operating procedures to help contracting officer's representatives in the IT Services Office manage a wide range of operations — including invoice payments, reports on how quickly contract dollars are being spent and the funding execution of more than 180 contracts totaling more than \$700 million.

Ali's training, best practices and programmatic support have resulted in a 70 percent increase in the accuracy of ITSO's fiscal 2015 IT services contract funding and enhanced the monitoring and analysis of contract spending rates.



### Regina Kassar

Regina Kassar grew up in a military family, so it was only natural that when the opportunity arose, she would help service-disabled veterans grow their companies.

As a business development manager at Red Team Consulting in 2014, Kassar volunteered for the

“ GEICO really takes care of its customers. We saved a lot of money, and the customer service has kept us here. ”

**Kevin Le**

*Government Employee for 19 years  
GEICO Policyholder for 14 years*

KEVIN LE got his

# FEDERAL DISCOUNT.

GET YOURS.

## GEICO®

Insuring Federal Employees for over 75 years

**1-800-947-AUTO**

Some discounts, coverages, payment plans and features are not available in all states or all GEICO companies. Discount amount varies in some states. One group discount applicable per policy. Coverage is individual. In New York a premium reduction may be available.  
GEICO is a registered service mark of Government Employees Insurance Company, Washington, D.C. 20076; a Berkshire Hathaway Inc. subsidiary. © 2015 GEICO

## 2015 Rising Stars

Service-Disabled Veteran-Owned Small Business Council and organized its monthly dinner events and educational boot camps.

Within a year, she became Red Team's vice president of education, helping small and midtier companies of all stripes find opportunities in the federal marketplace.

"I worked with industry as well as government to speak with those members to tell them if you're looking to go after this

contract, let's dig in deeper," Kassar said. "Overall, it wasn't really the value of the project. It was the impact you had on that company to win the award to provide jobs as well as those capabilities to our government and our military men and women, which is what it always goes back to for me."

"Regina was an absolute superstar for our company," said Jeff Shen, vice president and general manager of Red Team Consulting.

"She certainly went above and beyond for both Red Team and the federal IT community."

Her passion for helping veterans goes back to her roots. Her brother and grandfather served in the Navy, and her father, Merton Miller, served in the Air Force for 26 years and is now associate director of investigations at the Office of Personnel Management's Federal Investigative Services.

Kassar also took on volunteer roles at AFCEA and within a year became president of the NOVA Chapter's Young AFCEANs, where she leads networking and mentorship programs for members younger than 40.

Despite her family background, Kassar started out far from federal service, working in real estate sales and marketing. Then she earned a master's degree in teaching and taught second grade in Fairfax County, Va., for more than three years. After the birth of her twins, she decided to go back into business.

Her various jobs have taught her the value of technology, said Kassar, who recently left Red Team Consulting to work in federal software sales at IBM.

"It's neat to see how technology as a teacher at the time supported us to be so much more successful to make an impact," Kassar said. "Now I'm here on the solutions side learning all the IT I sell. It's incredible to see it in use."

— Bianca Spinosa

## Evan Chan

Evan Chan's love affair with NASA's Jet Propulsion Laboratory started when he was a student at the university the lab calls home: the California Institute of Technology in Pasadena. He interned at the lab, and that internship turned into a post-graduation job. Nine years later, he's still going strong.

Trained in both business and computer science, Chan has been in management roles for the past three years and has helped lead paperless procurement and augmented-reality initiatives.

Deploying a hybrid of Microsoft's OneNote and SharePoint, Chan and his team helped transform the "encyclopedias' worth of paper" that used to accompany procurement into a streamlined digital process, he said.

On the augmented-reality front, he was involved in craft-

ing an immersive mobile app that projects 3D images of spacecraft such as Curiosity, Cassini and Voyager.

And although his business education has helped Chan offer well-rounded leadership to his JPL team, he said part of what has kept him attached to NASA all these years is the distinct lack of typical business concerns.

At JPL, he said, "it's not so much about reducing costs for a product or shipping a new device." Instead, he can focus on quantifiable progress toward a much bigger goal: advancing humanity's trek through the stars.

It's a compelling reason to stay with the agency, Chan said: "We're doing things very few organizations can do."

— Zach Noble



---

## Christina Prat

Christina Prat's job is getting Border Patrol agents the data they need to quickly identify the people crossing the country's borders to ensure the safety of everyone involved.

She manages the day-to-day operations associated with developing, implementing and supporting the Biometrics and Federated Person Query modules of the e3 application. E3 is a web-based system that collects and transmits the

biographic, encounter and biometric data used by Customs and Border Protection to identify and verify individuals' identities at the border.

As an IT specialist, Prat works with the Border Patrol to understand its requirements and works

---

## Alexander Lin

When TCG Vice President David Cassidy met Alex Lin five years ago, he knew he wanted to make the hire.

"Alex has a certain set of skills and characteristics that are not always easy to find," Cassidy said. "Sometimes you don't know what you're looking for until you have it, and meeting Alex was like that."

Unfortunately, the company "didn't have the ideal position for Alex, but we knew his skills would be helpful on a project we had ongoing," Cassidy said. "So we hired him for that role, in which he excelled, and when a perfect position arose, we transitioned him to that."

Lin had planned to get a Ph.D. in English literature, but he abandoned that academic track after the master's degree stage to pursue technology consulting. The type of big-picture thinking he had learned in his studies, however, stuck with him and has helped him succeed with tough projects.

That broad perspective was especially helpful in 2013 when Lin was assigned to the Office

of Government Ethics' Integrity.gov project. The website was part of an effort to fulfill requirements of the Stop Trading on Congressional Knowledge Act of 2012, which addresses insider trading by members of Congress and federal employees. The website was a high-risk initiative with difficult demands and strict deadlines, but as project manager, Lin could visualize the outcome of the project without stressing over the

ambiguities that popped up throughout the process.

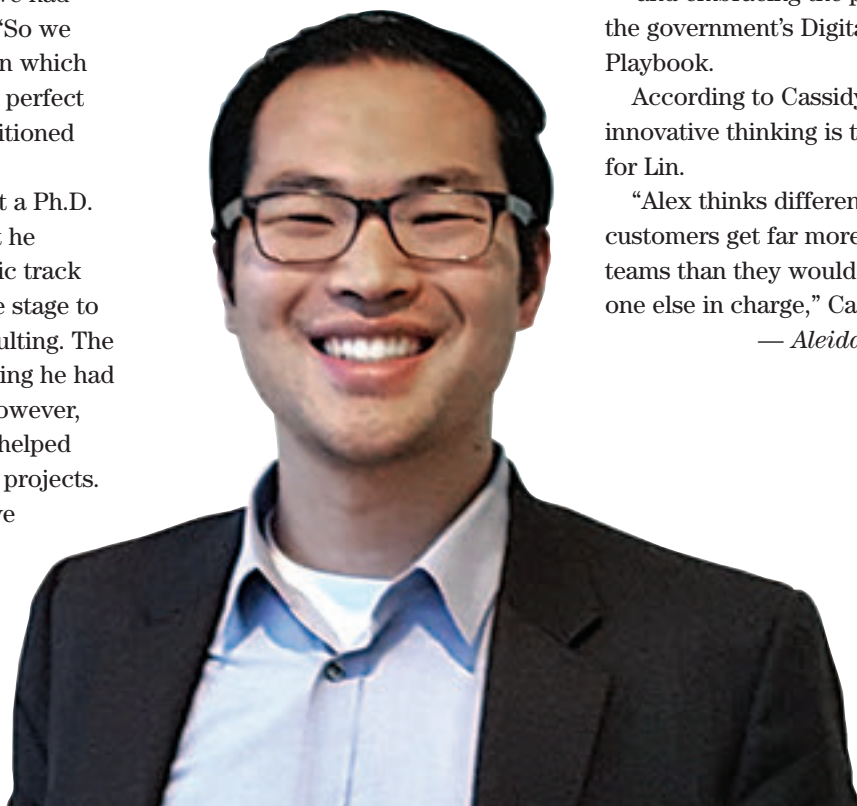
He took a particularly big risk when he convinced officials to build the site using the government-developed MAX.gov platform as a service, instead of going with a popular commercial solution.

Lin's leadership and risk-taking paid off. He and his team generated exponential savings while managing the expectations and requirements of senior executives — and embracing the principles in the government's Digital Services Playbook.

According to Cassidy, such innovative thinking is the norm for Lin.

"Alex thinks differently, [and] customers get far more from his teams than they would were someone else in charge," Cassidy said.

— Aleida Fernandez



## 2015 Rising Stars

with the contractor team to develop solutions. She is the data traffic cop for e3, and her efforts have improved the system's ability to capture and share biometric data on detained suspects and match data from other government entities.

Prat has gotten to know her Border Patrol data customers through numerous visits to the rugged lands they work. She understands that officers must be able to identify the people they encounter quickly to ensure everyone's safety. She also works closely with information partners at CBP's Office of Information and Technology and the departments of Homeland Security, Defense and Justice.

"I feel that each day I come into the office, the team and I have the ability to help U.S. Border Patrol agents on the frontlines of our nation's borders," she said. "I truly believe the work we do supporting their systems technically helps the agents work fast and stay safe."

— Mark Rockwell

## Teresa Rodriguez

Teresa Rodriguez might have gotten into government IT as the result of a bit of a misunderstanding, but now she's tackling challenges with a vengeance.

She earned a degree in criminal justice from the University of New Mexico, then worked in human resources in the private sector. Soon, however, she found herself drawn to tech.

# Nicholas Keshavarz-Nia

Nicholas Keshavarz-Nia's career is young, even for a Rising Star.

He was an intern at nonprofit Noblis while in college and joined the organization as a full-time information systems security engineer/analyst in 2014 when he graduated from the University of South Carolina's computer information systems program.

As both an intern and a full-time analyst, Keshavarz-Nia led development and deployment of the automated continuous monitoring solution called ScanCenter. He now uses the tool to support the Federal Risk and Authorization Management Program as leader of FedRAMP's Continuous Monitoring Team.

By automating processes that were once manual, ScanCenter has slashed monthly continuous monitoring analysis for nearly two dozen cloud systems from an average of eight hours to just one hour, FedRAMP's government managers said.

"I'm all for saving money and time,"

Keshavarz-Nia said, "and this program seems like it's doing both."

FedRAMP's streamlining of cloud authorization processes has proven critical for government, he said, adding, "This is something we've really needed for a really long time."

Monitoring ever-multiplying cybersecurity vulnerabilities is a "grueling task," Keshavarz-Nia admitted, but he is pursuing a master's degree in systems engineering at George Washington University as part of his plan to delve even deeper into the cybersecurity space.

— Zach Noble



# IT protects U.S. borders and citizens

BMC helps prevent border breaches and terrorist activity by ensuring availability for critical screening systems.



 **bmc** *for* Border Protection

Bring IT to Life at [bmc.com/federal](https://bmc.com/federal)

## 2015 Rising Stars

"I knew the front end of HR," she recalled. "I wanted to know the back end."

So Rodriguez dove into the Lawson HR software her firm used. At the time, she thought she was implementing the system, though she later realized she was actually doing end-user testing. That misunderstanding helped her land her next job: Because she put "implemented" on her résumé, she was brought in as a consultant to help the Albuquerque, N.M., public school system deploy Lawson.

She quickly realized her mistake,

but she powered through the steep learning curve. "It was a huge growth spurt for me, but I loved it," Rodriguez said.

That same spirit has characterized her latest job leading a U.S. Forest Service team.

In the past year, Rodriguez has spearheaded 10 initiatives, including a system for onboarding new employees, a performance management system and the first integrated safety and workers' compensation system implemented in the federal government.

Called eSafety, it was so impor-

tant that President Barack Obama was briefed on the project.

Rodriguez, however, is quick to credit colleagues for her successes.

"I feel that I'm only as good as my team," she said. Learning to trust one's partners, she added, can be the hardest part of any project, but she has come to value her small, six-person team inestimably.

And she's happy to have joined the feds after starting her career in the private sector. "I'll finish my career in federal service," Rodriguez pledged.

— Zach Noble

## Erica McCann

Erica McCann fell in love with procurement policy during a college internship. She was studying political science and already knew she was interested in government relations. Although she'd had other internships, this one sealed the deal.

That passion for procurement policy separates her from the rest of the pack, said Kitty Klaus, a senior program manager at HP Enterprise Services. McCann is "very enthusiastic about federal acquisition policy, which is not an area that a lot of people get enthusiastic about," Klaus said. "She really understands our issues in the industry, and she's very proactive in representing those interests."

As director of federal procurement at the Information Technology Industry Council's IT Alliance for the Public Sector, McCann is

responsible for representing a wide range of companies on Capitol Hill, where she makes recommendations about legislative and regulatory actions that affect the contracting environment.

More than 60 of those recommendations were incorporated into the fiscal 2016 National Defense Authorization Act and should ultimately help the Defense Department continue its efforts to sustain an edge in technology acquisition and attract new, innovative companies into the federal marketplace.

McCann

said maintaining the country's technological edge is what motivates her.

"I work in procurement policy because there's so much innovation in the private sector," she

added. "We're in an IT era; we need to be more flexible."

— Aleida Fernandez





## Michael Wheelless

The Navy is wrestling with the challenge of securely outfitting its ships with modern IT, and the service has found an ally in Michael Wheelless. The principal systems engineer at mobile communications firm Oceus Networks has managed to engineer a low-latency, high-bandwidth 4G LTE communications system for a Navy ship.

The project, which Wheelless said combined different technologies that “ride a single backbone,” demonstrated that commercial smartphones and tablets could work securely at sea. That is no small thing, considering that Navy officials are concerned about the vulnerabilities inherent in having sailors connect to devices while at sea.

But security and ease of access were compatible in this case, and the network connected to a satellite, which “allowed the ship’s crew to access whatever sites they needed to,” Wheelless said.

He added that many of the project’s challenges involved linking with networks ashore. “Some of the hiccups that we ran into were just coordinating with the dry side,” he said. That included connecting with the networks of the Defense Information Systems Agency, which is in charge of the Pentagon’s IT infrastructure.

The project complied with all the Navy’s security specifications and also took advantage of the National Security Agency’s Commercial Solutions for Classified Program, Wheelless said.

His work earned him special recognition by the Navy’s 7th Fleet

commander. Given the service’s demand for secure mobile technology, Wheelless might just be getting started.

— Sean Lyngaas

## Andrew Yuen

Andrew Yuen got his start in government in 2007 while still an undergraduate, and he has applied his

## Katherine Mullins

Without Katherine Mullins, the Department of Homeland Security’s network for sharing sensitive but unclassified information would not run nearly as smoothly.

The Homeland Security Information Network is the communications backbone for 40,000 current and prospective users, including employees of federal, state, local and private-sector entities. The network allows users to communicate securely during an emergency, make security plans for big public events and tap geospatial tools to track resources and intelligence.

Colleagues say Mullins is changing the way HSIN users are trained, and she has ushered in a new learning management system to track the effort.

Mullins, director of HSIN mission integration and outreach, started as a contractor and now manages engagement with all the network’s users. That work involved migrating terabytes of data and tens of thousands of users to a new platform. She has

also gone to bat for the network, pitching it to state agencies by drawing on her experience at the Mississippi Department of Public Safety’s Office of Homeland Security.

“I grew up with law enforcement and first worked as an analyst with a fusion center,” Mullins said, “which is where I was introduced to this ever-evolving world of information sharing in the post-9/11 environment.”

She built a communications strategy for HSIN from scratch and has brought together disparate user groups into integrated teams. She has also transformed the way network users’ stories are collected and displayed.

The importance of her job means Mullins keeps high-level company. She has briefed top leaders at DHS, including the undersecretary for intelligence and analysis.

The network itself might be composed of machines, but Mullins is proof that managing HSIN takes a human touch.

— Sean Lyngaas



## 2015 Rising Stars

background in environmental science, policy and web design at the Environmental Protection Agency ever since.

In 2013, he joined the web division of EPA's Office of Environmental Information as an IT specialist, with the main task of migrating EPA's web pages to a Drupal web content management system so that all the

agency's content could be better organized and easily searchable.

Yuen designed a mobile-friendly template that has searching and browsing options, created an archive for older EPA material and developed an email notification system to remind employees to update web content. Now the entire agency is

using the new system.

"We wanted to make sure that folks could find information faster," Yuen said, adding that "we redeveloped our websites to address specific key audiences."

His most recent project is the redesign of the Developer Central website, a one-stop shop for external developers to find information on the EPA's resources, application programming interfaces and datasets. Yuen facilitated cross-agency collaboration to incorporate additional developer toolkits, and he continues to provide extensive outreach to research communities by attending hackathons; partnering with universities and local and state environmental groups and agencies; and promoting outside APIs and datasets.

Before his current role, Yuen was the project manager for the Office of Pesticide Programs' Chemical Search Web Utility, an application that opened the EPA's pesticide data to the public.

One of his latest challenges is serving as leader of the EPA's Mobile Access Review Committee, where he spearheads efforts to revamp mobile application development strategies for the entire agency. He is also involved in the redesign of the EPA's Envirofacts data warehouse, where his goals include creating an advanced query builder interface, a data explorer tool and an API management platform so that developers and scientists can more easily access and download the warehouse's APIs.

"I enjoy the intersection between technology and environmental science," Yuen said, "and I think that's really necessary to understand why we're doing some of the IT projects we're doing."

— Amanda Ziadeh

## Mark Naggar

In the world of federal IT acquisition, Mark Naggar is a revolutionary firebrand on a search-and-destroy mission.

"The federal government spends around \$50 billion on IT services each year, and we're plagued by ineffective and inefficient acquisition of IT services," he said. "The acquisition approach and subsequent implementation and maintenance of IT systems [are] outdated and long overdue for improvements."

At the Department of Health and Human Services, Naggar has used his Buyers Club initiative to touch off a reform movement that is spreading to other government agencies.

He began by setting up a two-stage online system that skips the rigid, cumbersome acquisition process in favor of eight-page concept papers and statements of objectives. The Buyers Club approach streamlines activities for government and industry alike and allows vendors to show off what they can

do. It also minimizes the risk to federal agencies by freeing them from long, expensive, multilevel contracting processes, which have all too often wound up failing.

"There's a high failure rate associated with the acquisition of IT services, at HHS and throughout the federal government," Naggar said. "Given previous failures — of all sizes — associated with the acquisition and implementation of IT services at HHS, there's a tremendous need to mitigate risk of failure and ensure success."

Like most common-sense, innovative ideas, Naggar's Buyers Club is generating wider interest, with acquisition officers at other agencies eager to learn how to use it. The Inaugural Conference for Innovative Acquisitions in February drew more than 500 employees from 20 agencies, despite a snowstorm that slowed Washington to a crawl the day of the event.

— Mark Rockwell



# CALL FOR NOMINATIONS!

**Nominate a government or industry leader** for The Federal 100 who has gone above and beyond their daily responsibilities and have made a difference in the way technology was bought, managed or used in the past year.

**Deadline for nominations is December 23, 2015.**

The winners will be featured in the April 15th issue of *FCW* and at the Federal 100 celebration April 7, 2016.

**Submit your nominations today!**



**[FCW.com/2016Fed100](http://FCW.com/2016Fed100)**

# Telework and the loneliness left behind

A new study reveals that the morale of on-site workers can suffer as telework programs expand — and spark an office exodus rooted in loneliness

BY ZACH NOBLE

For the 100-mile commuter, the harried single parent and others, flexible telework is the best thing ever. But what about the people who still go into the office? According to a recent paper, they get lonely.

“Contagious Off-Site Work and the Lonely Office: The Unintended Consequences of Distributed Work,” by Michael Pratt of Boston College and Kevin Rockmann of George Mason University, delves into the plight of the teleworker’s abandoned colleagues.

“People still appear to desire something like a traditional office,” the report states. “In our study, even people who worked largely off-site still missed the social and work benefits of the old office.”

In fact, many people who are currently teleworking might be doing so only because their offices have been deserted.

The authors asked more than 600 employees at a Fortune 100 company why they chose to telework and how often they did it. Given the company’s wide-open telework policy, employees could essentially choose where they wanted to work every day.

Although many employees cited work/life balance and efficiency, the employees who felt disconnected because of the prevalence of tele-



**“You used to have...established friendships and stuff at work that were a lot more close,” one employee said. “And now it’s just come to work, do your work and leave.... It’s not as friendly to come to work now.”**



work wound up spending the most time off-site. Specifically, employees who agreed with the statement, “Few people, if any, from my team work in the office much, so I do not benefit from coming in,” averaged 72 percent of their work time out of the office. For employees who did not feel that description applied to them, the average was 27 percent.

The authors concluded that some employees are fleeing their offices not because of telework’s benefits but just because the offices have emptied.

A smaller, in-depth survey of 29 employees at the company uncovered some morale issues.

“[Being] remote makes it hard to have the spontaneous dynamic interactive discussions in the hallway,” one manager said. “Because people are spread out and working from home, we don’t have a sense of team.”

“You used to have...established friendships and stuff at work that were a lot more close,” another employee said. “And now it’s just come to work, do your work and leave.... It’s not as friendly to come to work now.”

### **The flip side: Management and Skype**

Despite the potential risks, there are both financial and personal upsides to telework — and govies are bullish on the practice, as long as it’s effectively managed.

Cheryl Cook, former CIO at the Agriculture Department and now chief innovation officer at the Pennsylvania Department of Agriculture, recalled the financial boon for the Forest Service when it went from three D.C.-area office buildings down to one thanks to telework.

When Cook served as Pennsylvania director of the USDA’s Rural Development Mission Area, that organization was able to shrink from 42 offices to

## **The same principles that should guide a traditional organization can hold a teleworking office together: accountability, engagement and a shared sense of purpose.**

12, a process that saved money even as it ensured that USDA officers were spread more evenly across the state by staying in their local zones.

She also noted the personal benefits. When she worked at USDA headquarters, she faced a 220-mile roundtrip commute between D.C. and southeastern Pennsylvania. Teleworking one day every two weeks was a godsend for a woman who barely had time to sleep.

“It’s tempting to say nothing can replace in-person collaboration,” Cook said, “but the truth is the additional sleep on days that I teleworked made me a clearer thinker and a better collaborator with my staff, who were spread out all over the country and for the most part only knew me from the end of an email string anyway.”

So how can telework be effectively managed?

The General Services Administration’s 18F recently dedicated a blog post to the subject. The prescription included over-communicating on tools such as GitHub, Slack and old-fashioned email; having face-to-face video chat meetings at least once a week; and collaborating as often and as extensively as possible.

NASA Chief Human Capital Officer Lauren Leo, meanwhile, said clear performance expectations and managerial trust are the keys to effective telework. However, she noted that NASA is nowhere near the ghost-town scenario

of Pratt and Rockmann’s study because only 2 percent of NASA employees telecommute more than three days a week.

Cook said the same principles that should guide a traditional organization can hold a teleworking office together: accountability, engagement and a shared sense of purpose.

But according to the study, telework puts a strain on morale — something managers must watch. It can also fog an organization’s institutional memory.

“Formal training often is sacrificed when budgets get tight, leaving newer employees more dependent than ever on more experienced co-workers for advice and informal training as issues arise,” Cook said. “If those more seasoned employees are regularly not in the office several days per week, that window of opportunity closes a little.”

“Telecommuting in a vacuum does have this life drain on people,” Leo said. Video chat sessions can help, but “in our experience, they won’t ever replace the face-to-face connection.”

The study’s authors said their findings are an invitation for further consideration. “At the very least, off-site work is not the win-win situation it’s widely considered to be,” Pratt said.

“If the office is going to become a collection of employees not working together, it essentially becomes no different than a coffee shop (though perhaps with better Internet and worse coffee),” the authors wrote. ■

# FCW Index

## Advertisers

<b>BMC Software, Inc.</b> www.bmc.com/federal .....	<b>27</b>	<b>IBM Corporation</b> www.ibm.com/outthink .....	<b>36</b>
<b>Bright House Networks, LLC</b> www.brighthouse.com/enterprise .....	<b>5</b>	<b>InterSystems Corp.</b> www.InterSystems.com/Federal1CC .....	<b>35</b>
<b>CDWG</b> www.CDWG.com www.FCW.com/2015SnapshotVirtualization .....	<b>7-9, 11</b>	<b>Nutanix Inc.</b> www.nutanix.com/solutions/federal-government/ federal-use-cases .....	<b>14-15</b>
<b>GEICO</b> www.geico.com .....	<b>23</b>	<b>United Healthcare</b> www.uhcfeds.com .....	<b>2</b>
<b>GOVERNMENT ACQUISITION, INC.</b> http://gov-acq.com/solutions-capabilities/ cyber-security .....	<b>10a-10d</b>	These indexes are provided as an additional service. The publisher does not assume any liability for errors or omissions.	
<b>FCW Webcast Series</b> www.fcw.com/2015EnterpriseEvolution1 .....	<b>34</b>	To advertise in FCW, please contact Dan LaBianca at dlabianca@1105media.com. FCW's media kit is available at 1105publicsector.com.	
<b>Fed 100 Nominations</b> www.FCW.com/2016Fed100 .....	<b>31</b>		

**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

REGISTER  
NOW

## FCW WEBCAST SERIES

# THE EVOLUTION OF THE ENTERPRISE

### SESSION 1

## VIRTUALIZATION: THE PATH TO A MORE SCALABLE ENTERPRISE

FEATURING: DR. MICHAEL VALIVULLAH

Chief Technology Officer, National Agricultural Statistics Service, United States Department of Agriculture

### VIEW ON-DEMAND AT: [fcw.com/2015EnterpriseEvolution1](http://fcw.com/2015EnterpriseEvolution1)

SPONSORED BY

A young Black man with short dark hair is lying in a hospital bed, propped up by white pillows. He is wearing a white hospital gown with a blue collar and a small blue pattern. He is smiling warmly at the camera.

**“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](https://www.intersystems.com/Federal1CC)

**INTERSYSTEMS®**

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



**Cognitive security is here.**

When everything is connected, everything is vulnerable. IBM uses cognitive technology to help protect the critical assets of your agency. It senses and helps detect millions of hidden threats from millions of sources, and continuously learns how to defeat them. When your agency thinks, you can outthink.

**outthink**  
threats

IBM and its logo and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. See current list at ibm.com/trademark. Other product and service names might be trademarks of IBM or other companies. ©International Business Machines Corp. 2015.

[ibm.com/outthink](http://ibm.com/outthink)

