GCN

TECHNOLOGY, TOOLS AND TACTICS FOR PUBLIC SECTOR IT

OCTOBER 2015 • VOLUME 34, ISSUE 10

THE OFFICE OF THE FUTURE

It's already here, if you know where to look

PAGE 9

THE 2015 GCN AWARDS

Profiles of all the winners inside!

PAGE 14

DDS 5900 Digital Discussion System

WHAT GREAT SOUND LOOKS LIKE.

DC 5900 F FLUSH MOUNTED CONFERENCING UNIT delivers the exceptional sound quality, flexibility, and styling that are hallmarks of the DDS 5900 Digital Discussion System. Innovative design and new automatic configuration technology makes set up and installation quick and easy for conference rooms where style and performance are critical.

- **Compact** form factor and sleek appearance
- **Modular** design suits many applications
- **Multiple** configurations: Delegate or Chairman button overlays
- **Easy** setup: Overlays automatically activate distinct configurations
- **Compatible** with Shure Microflex® gooseneck microphones

www.shure.com/conferencing

SHURE®

LEGENDARY PERFORMANCE™

© 2015 Shure Incorporated

INSIDE

FEATURES

GCN (ISSN 0738-4300) is published 11 times a year, monthly except 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. **Subscription inquiries, back issue requests, and address changes:** Mail to: *GCN*, P.O. Box 2166, Skokie, IL 60076-7866, call (866) 293-3194, outside U.S. (847) 763-9560; fax (847) 763-9564 or email GCNmag@1105service.com. **POSTMASTER**: Send address changes to *GCN*, 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.

GCN

Technology,
Tools and Tactics
for Public Sector IT

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: GCNmag@1105service.com
Mail: GCN
PO Box 2166
Skokie, IL 60076
Phone: (866) 293-3194 or (847) 763-9560

REACHING THE STAFF

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

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

Contributing Writers Kathleen Hickey, Stephanie Kanowitz, Will Kelly, Suzette Lohmeyer, Carolyn Duffy Marsan, Patrick Marshall, Brian Robinson, William E. Welsh

Editorial Fellow Mark Pomerleau

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

PUBLIC SECTOR MEDIA GROUP

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 **Michele Long**
Project Coordinator, Client Services **Olivia Urizar**
Manager, Lead Generation Marketing **Andrew Spangler**
Coordinators, Lead Generation Marketing **Naija Bryant, Jason Pickup, Amber Stephens**

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

FederalSoup and Washington Technology
General Manager **Kristi Dougherty**

OTHER PSMG BRANDS

FCW
Editor-in-Chief **Troy K. Schneider**
Executive Editor **Adam Mazmanian**
Managing Editor **Terri J. Huck**
Staff Writers **Sean Lyngaas, Zach Noble, Mark Rockwell**
Editorial Fellows **Aleida Fernandez, Jonathan Lutton, Bianca Spinosa**

Defense Systems
Editor-in-Chief **Kevin McCaney**

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**

1105 MEDIA

Chief Executive Officer
Rajeev Kapur

Chief Operating Officer
Henry Allain

Senior Vice President & Chief Financial Officer
Richard Vitale

Executive Vice President
Michael J. Valenti

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

Chairman of the Board
Jeffrey S. Klein

Foster telework through secure remote access

Federal and state agencies have worked hard to implement telework, and it's paying off. According to official reports at both levels of government, it has resulted in lower costs, higher employee satisfaction, improved productivity and better preparation for continuity of operations plans.

Agencies understand that teleworking conveys many advantages, but also introduces increased security concerns. Remote PCs or mobile devices—whether owned by the agency or the employees themselves—can't be consistently protected.

To mitigate these threats, almost all agencies have implemented secure remote access in the form of a virtual private network (VPN). This includes identification, authentication and authorization at the firewall level, as well as encryption technology. Government agencies have learned the hard way though that not all VPNs are created equally. VPNs don't all provide the same level of security. Some only require a username and password for access, despite the OMB's requirement for two-factor authentication in all cases of remote access. Two-factor authentication requires any two of the following:

- something you know (like a password)
- something you are (biometrics, like a fingerprint)
- something you have (a smartcard or Common Access Card)

Besides ensuring a VPN uses two-factor authentication, agencies can improve their remote access security by implementing network monitoring, Security Information and Event Management (SIEM), network access control, advanced malware protection and data loss prevention (DLP).

Then there's always the human element. All the technology in the world isn't worth much if employees don't know what's acceptable and what's risky. At the very least, any remote access security policy should include:

- List of specific equipment, operating systems and software acceptable for use outside the agency's offices
- Requirements to keep the operating system, anti-virus and anti-malware software up to date by applying patches as soon as they become available
- Rules for how to connect to the VPN
- A "whitelist" of acceptable apps and/or "blacklist" of unacceptable apps
- Teleworkers responsibilities when it comes to protecting the security and integrity of agency data
- Applications and data workers can't access remotely
- Teleworker accountability and responsibility for data integrity and confidentiality
- Specific repercussions if guidelines are not followed

PROTECT THE MOBILE ENDPOINT

PROTECTING mobile endpoints like smartphones and tablets has never been easy. The sheer explosion in the number of mobile devices in use at all levels of government agencies, many of them owned by employees themselves, is part of the issue. The way employees use those devices is another issue.

According to a recent report from the Ponemon Institute, employees who don't comply with security policies are the greatest source of endpoint risk. All this means traditional methods of protecting mobile endpoints—anti-virus software, host-based firewalls and so on—aren't enough anymore. These solutions and strategies can complement and integrate with existing enterprise mobility management solutions:

- Identify the threats your users face today, and rewrite your endpoint security governance and control processes to reflect those realities. Without this, you won't have the right information to choose the right tools.
- Upgrade to more advanced anti-malware detection that can analyze multiple file types, detect different forms of evasions and block bad files.
- Invest in a solution that enforces continuous endpoint monitoring. These solutions offer real-time visibility and monitoring of all endpoints, policy enforcement, threat remediation and other security capabilities.
- Include a threat intelligence component that analyzes real-time user and network data for potential threats.
- Implement a real-time endpoint forensics data capture and analysis tool that can monitor all processes running on endpoints at all times, along with processes that aren't considered normal behavior.

What is Virtual Mobile Infrastructure and why do we need it?

When it comes to protecting mobile data and securely accessing mobile apps, government agencies have increasingly turned to solutions like Mobile Device Management (MDM) and Mobile Application Management (MAM). These solutions are effective to a point, but with the increasing adoption of Bring-Your-Own-Device (BYOD) throughout government, the stakes are higher—and protection more elusive. Enter Virtual Mobile Infrastructure (VMI).

WHAT IS VMI?

Think of this as Virtual Desktop Infrastructure (VDI) for mobile devices. The purpose of VMI is to provide secure access to mobile applications, data and secure networks from mobile devices. Like VDI, users are assigned a profile. This profile is centrally managed and stored on agency servers. Applications and data are delivered to the device via a secure remote protocol. To access applications, users must log in securely on the device. No agency data is stored on the device. Because nothing sensitive is stored on the device, there is no risk of data loss due to device theft. It's more efficient because installation, upgrading and patching are automated.

HOW DOES VMI HELP WITH SECURITY WHEN MANY EMPLOYEES USE THEIR OWN DEVICES?

Agencies can be confident there's no cross-over between agency data and apps, and personal data and apps. This means the chance of confidential data getting into the wrong hands is slim to none.

WHY DO WE NEED VMI IF WE ALREADY USE ENTERPRISE MOBILITY MANAGEMENT SOLUTIONS LIKE MDM AND MAM?

MDM focuses on distributing data, applications and security configuration settings to mobile devices. MAM provides more controls specific to applications and often manages an organization's app store. MAM solutions can also store fully encrypted data without fully encrypting the device and remotely enforce policies. However, both have limitations. MDM doesn't do much to secure applications and isn't ironclad when it comes to protecting against attacks or data leaks. Also, both MDM and MAM solutions require multiple protocols, which means more potentially weak links. And enforcing policies on these solutions is time-consuming.

DOES THIS MEAN OUR INVESTMENT IN MDM AND/OR MAM WAS A WASTE OF TIME AND MONEY?

Not at all—these solutions are an important step in managing mobile devices. Layering a VMI solution over your existing infrastructure will strengthen security. Existing solutions are still useful in securely delivering some mobile apps, while VMI can take care of more sensitive, complex apps and provide access to more sensitive data.

BY THE NUMBERS: THE MOBILE SECURITY THREAT

29%	The percentage of mobile devices connected to the network of a major U.S federal agency that has encountered a mobile threat during the past year.
33%	The percentage of organizations that never test their apps.
40%	The percentage of organizations that aren't scanning the code in their apps for security vulnerabilities.
75%	The percentage mobile malware in the U.S. has grown over past year.
85%	The percentage of commercial mobile apps that track when WiFi and data networks are used, if the device is turned on, or the device's current and last location.
188%	The percentage by which Android vulnerabilities have increased compared to 2011.
262%	The percentage by which iOS vulnerabilities have increased compared to 2011.
More than 20,000	The number of mobile applications that fail to properly validate SSL certificates.
16 million	The number of mobile devices worldwide that have been infected with malware.
1,432,660,467	The number of attacks launched from online resources located throughout the world.

Secure Mobility Across the Board

There's a lot riding on mobility at all levels of government. It can improve productivity, increase employee satisfaction and even play a key role in agencies' disaster recovery plans. Yet despite significant progress in providing at least some degree of mobility to government employees, security concerns have hampered progress.

To manage security concerns, government has largely turned to solutions like Mobile Device Management (MDM) and Mobile Application Management (MAM), which help secure data on devices through encryption and containerization. While these measures are helpful, they're far from foolproof. For example, if a device is lost or stolen, there's a risk of sensitive data falling into the wrong hands.

There's a better way—by not storing data on mobile devices in the first place. That way, first responders, field workers and office workers who need mobile devices can access sensitive or classified data securely without the risk. The data is never stored on the devices. Instead, users see the data redisplayed on their screens.

Government agencies have been using virtual desktop infrastructure (VDI) technology for years on laptops. VDI runs a user's applications and desktop, storing their data on a server and displaying that information on the endpoint. For example, a federal law enforcement agency uses Raytheon|Websense's Trusted Thin Client® solution for employee laptops. That way, agents in the field can access multiple sensitive networks without having to bring multiple laptops and encryption devices. And if they need to leave the unit behind during an unexpected evacuation, there's no risk of data loss.

Today, agencies can use the same type of technology for smartphones and

tablets. "We knew this was something government needed to solve security concerns, especially in the case of sensitive and classified information on mobile devices," says George Kamis, CTO of Raytheon|Websense, Federal Sector. "Trusted Access Mobile uses an encrypted network connection, a secure mobile gateway and virtual mobile infrastructure to ensure that when users need to access sensitive information on mobile devices, what they are really seeing is only a display of the information on a screen."

The Trusted Access Mobile solution runs on both Android and iOS devices. It uses Defense-grade security with Suite B encryption algorithms and nested TLS encrypted tunnels. Its hardened mobile gateway uses an SE Linux® foundation, and the mobile gateway blocks all other traffic between the device and the agency.

With this technology, mobility becomes more secure across the board. Agencies allowing BYOD no longer have to worry about sensitive information falling into the wrong hands. Employees appreciate the flexibility it gives them to use the device for their personal needs as well as work.

There are other benefits as well. In situations when the office is inaccessible, such as a weather or threat event, employees can remain productive. And when traveling abroad, employees can securely access email, calendar and data on mobile devices. The data isn't stored on the device, which greatly reduces data loss or exposure.

At the other end of the spectrum, agencies that require solutions with top-level security can equip their employees with mobile devices for use in the office without raising undue concern if a device mistakenly leaves the building. "For a long time, thin clients have been considered more secure than PCs," says Kamis. "Now mobile devices can be just as secure."

Raytheon | websense

http://www.raytheoncyber.com/capabilities/products/trusted-thinclient/
http://www.raytheoncyber.com/capabilities/products/trusted-mobile/
http://www.raytheoncyber.com/resources/

[BRIEFING]

California shares its criminal justice data

BY DEREK MAJOR

The California Department of Justice and the Office of the Attorney General have launched OpenJustice, a data-sharing effort that the state described as a first-of-its-kind initiative.

OpenJustice consists of two key elements: a dashboard of criminal justice indicators and an open-data portal that encourages users to download and reuse the data.

The dashboard draws from three datasets: law enforcement officers killed or assaulted in the line of duty; deaths in custody, including arrest-related deaths; and arrests and bookings. Each set has interactive tools to allow the public to visualize and explore different indicators over specific timelines and across jurisdictions.

California Attorney General Kamala Harris said the OpenJustice initiative is a way to "hold ourselves accountable and improve public safety."

The portal publishes raw data from criminal justice datasets that can be downloaded by software developers, researchers and journalists to identify trends and problems in the criminal justice system.

"Being 'smart on crime' means measuring our effectiveness in the criminal justice system with data and metrics," California Attorney General Kamala Harris said. "This initiative puts forward a common set of facts, data and goals so that we can hold ourselves accountable and improve public safety." •

USPTO opens the door to 4 decades of data

BY DEREK MAJOR

The U.S. Patent and Trademark Office has teamed up with the Center for the Science of Science and Innovation Policy to launch a prototype web tool called PatentsView that allows individuals to explore data on patent activity in the United States as far back as 1976.

Users can search patent titles, types, inventors, assignees, patent classes, locations and dates. The resulting information can be displayed as graphs or charts to show trends in patent activity. Researchers, inventors and startups can also search the patents of specific companies and see what technology is on the rise or starting to drop in popularity.

PatentsView is part of a broader open-data initiative by USPTO, which is seeking to improve the accessibility and usability of valuable patent and trademark data. •

READ ME

What: "Leveraging Data Through Partnerships," a report by the CIO Council's Innovation Committee about open-data efforts at the U.S. Agency for International Development.

Why: Establishing an open-data policy has helped USAID build better relationships with its partners and use data to help people in different countries tackle significant issues. This CIO Council study looks at the concrete steps USAID has taken to ensure that open data is built into its operations rather than treated as an afterthought.

Key elements include creating data stewards in every operating unit, defining a standard data clearance process and establishing a web-based repository for datasets for public release.

USAID has used open data to help disaster response teams find open roads to reach victims after an earthquake in Nepal, bring water management to North Africa and the Middle East, and improve farming trends and crop growth to produce more food for people in Kenya.

Takeaway: If it didn't share data with its partners, USAID would struggle to achieve its mission. The agency has altered its basic operations to better gather and share data about its aid efforts, while at the same time ensuring privacy and security.

Full report: is.gd/GCN_USAID

DAG.CA.GOV

THE OFFICE OF THE FUTURE

It's already here, if you know where to look

By 2015, we were supposed to have hoverboards. So is it too much to ask for a workplace where government employees have the tools to deliver on digital government's promise?

That question (minus the hoverboard lament) was the gist of a Justice Department request for information this summer on best-of-breed technologies for a future virtual office. And although other agencies might not be detailing their questions in RFIs, there is active exploration of new approaches to office IT at all levels of government.

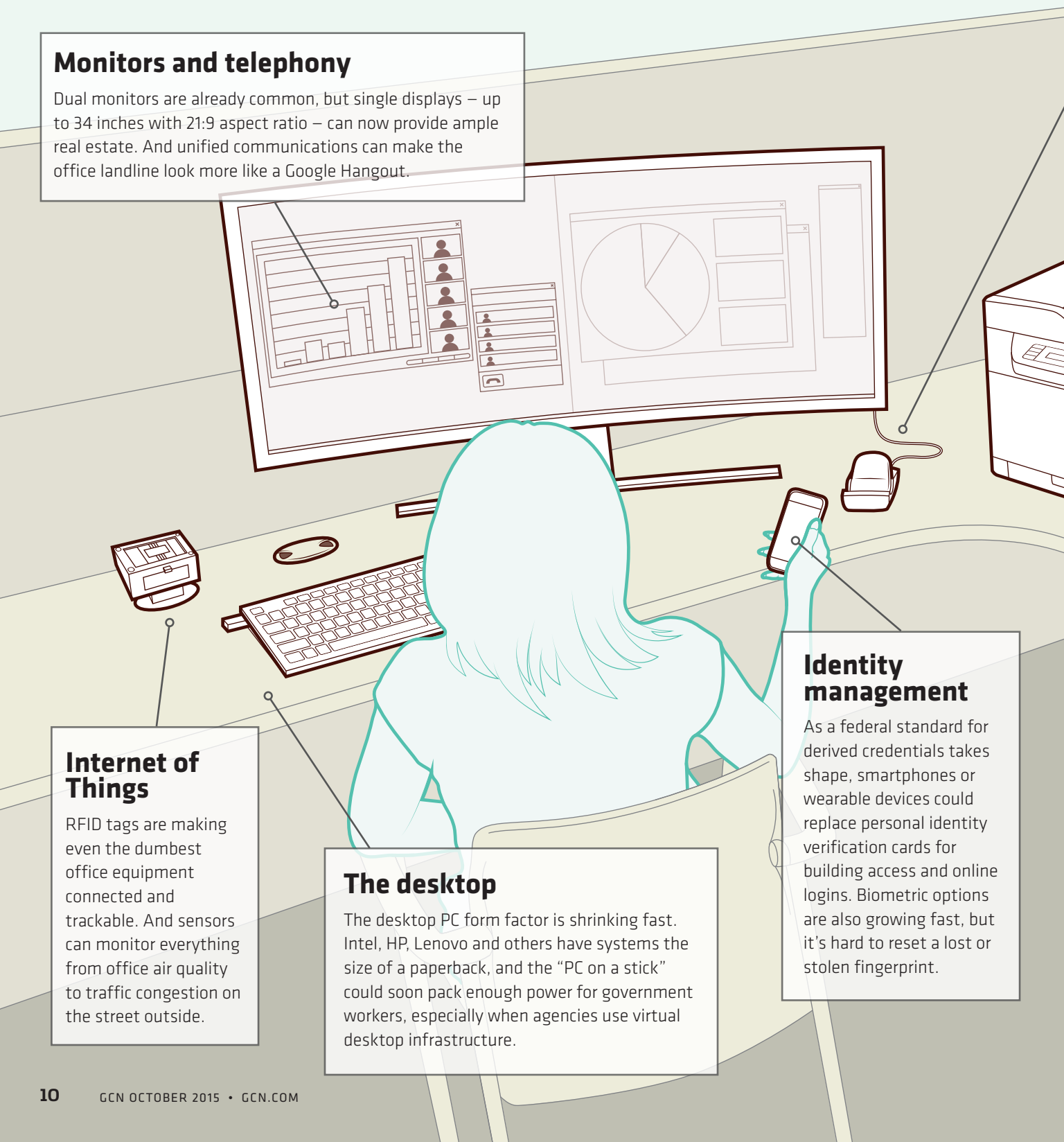
So GCN did some exploring to see just what a bleeding-edge office might look like. No sci-fi speculation here; all the technology in question exists in production form. And as the pages that follow make clear, government cubicles might be about to get significantly more interesting.

– GCN staff

Illustrations by Dragutin Cvijanovic

"The future is already here – it's just not evenly distributed yet."

– William Gibson



Monitors and telephony

Dual monitors are already common, but single displays – up to 34 inches with 21:9 aspect ratio – can now provide ample real estate. And unified communications can make the office landline look more like a Google Hangout.

Internet of Things

RFID tags are making even the dumbest office equipment connected and trackable. And sensors can monitor everything from office air quality to traffic congestion on the street outside.

The desktop

The desktop PC form factor is shrinking fast. Intel, HP, Lenovo and others have systems the size of a paperback, and the "PC on a stick" could soon pack enough power for government workers, especially when agencies use virtual desktop infrastructure.

Identity management

As a federal standard for derived credentials takes shape, smartphones or wearable devices could replace personal identity verification cards for building access and online logins. Biometric options are also growing fast, but it's hard to reset a lost or stolen fingerprint.

Mobile device docking

That device we insist on calling a smartphone is really a computer with the power to handle most daily tasks. Although today's docks focus on syncing and secondary display, efforts like Andromium's could make mobile devices the primary machine – and change the calculus of bring-your-own vs. agency-issued devices in the process.

Workspaces without cables

Wireless gigabit and near-field communication are advancing quickly and can allow for completely wireless desk spaces. Those technologies make "hoteling" and flexible seating much simpler for users and IT support staff alike.

Wi-Fi everywhere

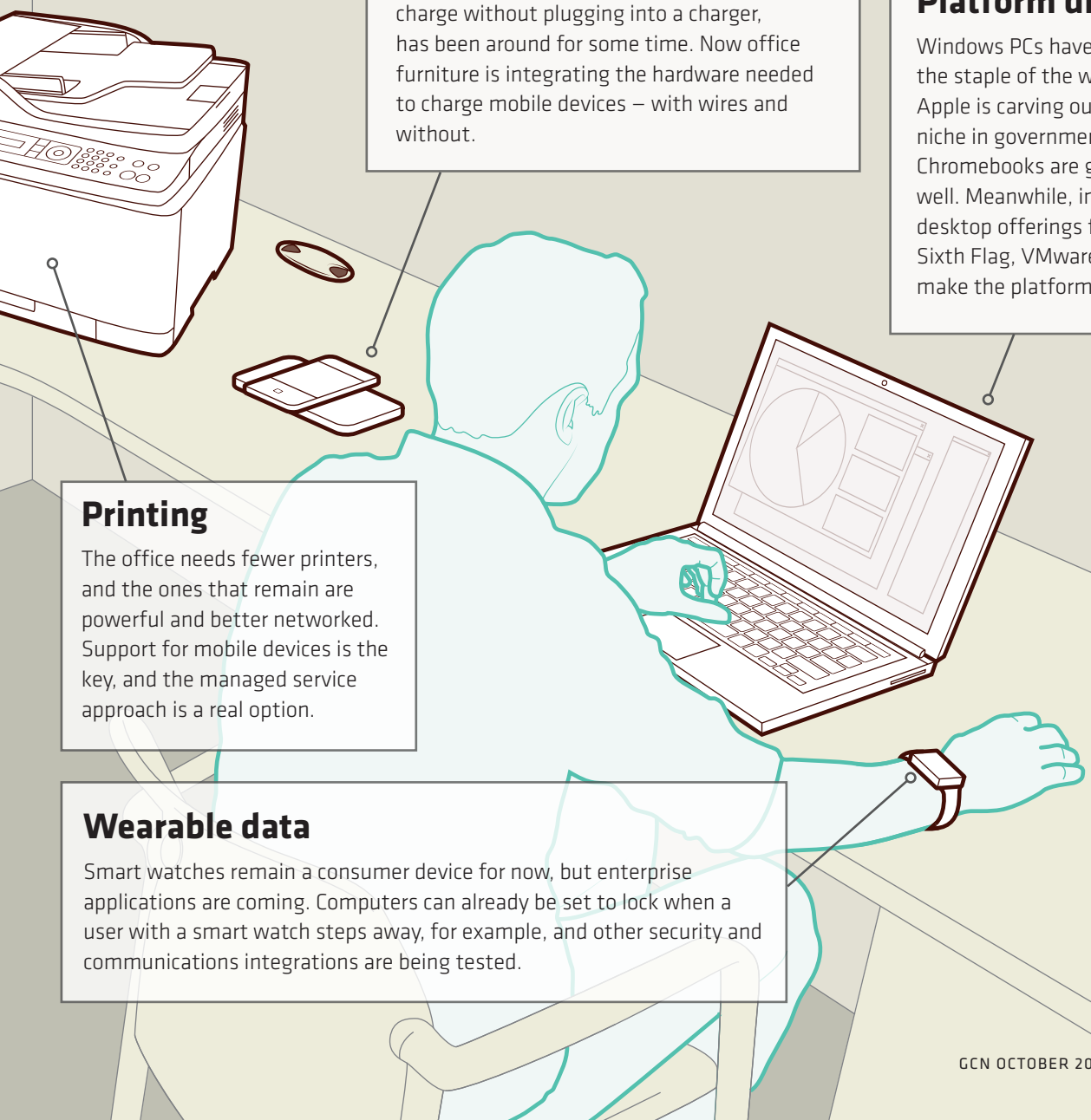
Wi-Fi is no longer optional, and offices need connectivity that is both robust and secure. Enterprise-grade solutions offer better coverage with fewer access points, requiring fewer ports and translating into less network infrastructure overall.

Device charging

The Qi standard, which allows devices to charge without plugging into a charger, has been around for some time. Now office furniture is integrating the hardware needed to charge mobile devices – with wires and without.

Platform diversity

Windows PCs have long been the staple of the workplace, but Apple is carving out a broader niche in government, and Google Chromebooks are getting a look as well. Meanwhile, improved virtual desktop offerings from Citrix, The Sixth Flag, VMware and others could make the platform all but irrelevant.



Printing

The office needs fewer printers, and the ones that remain are powerful and better networked. Support for mobile devices is the key, and the managed service approach is a real option.

Wearable data

Smart watches remain a consumer device for now, but enterprise applications are coming. Computers can already be set to lock when a user with a smart watch steps away, for example, and other security and communications integrations are being tested.

SNAPSHOT

VIRTUALIZATION

Virtualization security: The good and the bad

The promise of virtualization to improve the use of IT resources is now well established. Unfortunately, understanding the attending security issues has not kept pace. In the age of advanced cyber threats, sophisticated malware and regular high-profile breaches of both private and public organizations' security, virtualized environments could prove particularly vulnerable.

A recent survey by Kaspersky Labs found it costs organizations more than twice as much to recover from a cyber-attack on a virtualized infrastructure than an attack on a physical environment—regardless of the size of the enterprise. That's because a majority of them use virtual infrastructure for their most important operations. Also, some 42 percent of the survey respondents believe security risks in virtual environments are significantly lower than in physical environments.

Organizations do expect that going virtual will decrease their IT spend and streamline their infrastructure, says Matey Voytov, Kaspersky's corporate products group manager. "If there is not enough attention paid to security matters in the virtual environment," he says, " expenses may exceed the benefit."

Several years ago, the National Institute of Standards and Technology (NIST) tried to bring attention to virtualization security needs with SP 800-125, a comprehensive "Guide to Security for Full Virtualization Technologies."

The guide noted virtualization has some negative security implications. "Virtualization adds layers of technology, which can increase the security management burden by necessitating additional security controls," the guide states. "Also, combining many systems onto a single physical computer can cause a larger impact if a security compromise occurs."

Virtual systems also make it easy to share information between systems. That's a convenience in regular IT operations, but can also be a way into a system for cyber threats. In some cases, according to NIST, virtualized environments are quite dynamic. That can also make creating and maintaining the necessary security boundaries more complex.

NIST followed up on that report in 2014 with draft guidance on how to secure hypervisors, the software that lets you build virtual machines on physical host systems. Specific hypervisor threats include such things as configuration errors, snooping on virtual network traffic, or denial of service attacks.

Virtualization itself is still seen as an enabler of better security, however. That's the case for network virtualization, for example, which some feel can ease security concerns because it allows for easier distribution of such things as virtual firewalls. Organizations can also more quickly mitigate malware by tearing down an infected virtual network and replacing it with another clean network.

It's an argument that Maj. Gen. Sarah Zabel, the new vice director of the Defense Information Systems Agency, gave to a recent industry meeting for adopting network virtualization. It will help the DISA banish persistent threats from its networks, she says.

Organizations should be careful in getting too caught up in the potential of virtualization to improve their overall use of IT, Kaspersky warned, even though that potential is indeed real.

"Virtual environments are trusted more than physical servers," says the Kaspersky report, "and nothing can be trusted in a grim security environment."

Other Virtualization Report Articles:

- Virtualization Helps Agencies Reach IT goals
- Software-defined platforms define future of virtualization
- The promise of containers
- Service virtualization could be big for DevOps

GCN.COM/2015SNAPSHOTVIRTUALIZATION

THE CLOUD and CDW-G

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

CLOUD ADOPTION ON THE RISE

$3 BILLION
Amount spent by the federal government on cloud computing in 2014.

5X
SaaS adoption has more than quintupled in the past four years.

35%
of IT services are currently delivered via the cloud.

721
The number of cloud-based services the average public-sector organization uses.

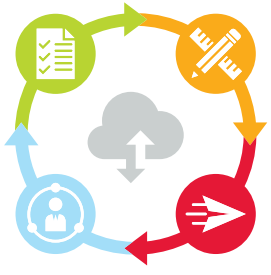
SOURCE: [1]IDC Government Insights, Perspective: Looking Up – U.S. Federal Cloud Forecast Shows Sustained Growth Through 2018, September 2014 [2]CDW, Cloud 401: Navigating Advanced Topics in Cloud Computing, February 2015 [3]Source: North Bridge and Gigaom Research, The Future of Cloud Computing, June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

THE CDW·G APPROACH

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

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

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



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

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

For more information on our cloud offerings, visit CDWG.com/cloud

Microsoft

CDW·G PEOPLE WHO GET IT™

TEAMWORK, CHANGE AGENTS AND THE BEST IN PUBLIC SECTOR IT

GCN Award Judges

The independent panel of judges that select each year's GCN Award winners have spent decades improving public-sector IT themselves and devoted countless hours to the consideration of this year's nominees. These awards would not happen without them, and GCN is grateful for their time and expertise.

David Bray
CIO, Federal Communications Commission

David Garcia
Secretary of Information Technology, State of Maryland

Deborah Diaz
CTO, NASA

Terry Halvorsen
CIO, Defense Department

Karen Evans
National Director, U.S. Cyber Challenge

Alan Shark
Executive Director and CEO, Public Technology Institute

Lt. Gen. Robert Ferrell
CIO, U.S. Army

Renee Wynn
CIO, NASA

In public-sector IT, the attention too often goes to the projects that went wrong – the lessons learned and what could be done differently. Yet there's every bit as much to be learned from the projects that went right and from the teams that made it happen.

And the 2015 GCN Awards are proof positive that great things are being accomplished at all levels of government IT. Whether it's streamlined citizen service in Philadelphia or the largest enterprise resource planning deployment in U.S. Army history, the teams and leaders featured in the pages that follow show just how much creativity, perseverance and technical prowess are being put to the task of making government work better.

It's been a privilege to learn more about this year's winners and to share their work with the broader IT community. We hope you enjoy learning from their successes as well.

ZAID HAMID

GOVERNMENT EXECUTIVE OF THE YEAR: RON ROSS

If the discussion involves information security, NIST's technology fellow is almost certainly shaping it

BY BIANCA SPINOSA

Ron Ross got his start in cybersecurity by accident. In the early 1980s, while still in the Army, he earned a master's degree and then a Ph.D. in computer science from the Naval Postgraduate School in hopes of joining a group of military officers familiar with robotic vehicles.

But the day before Ross was to start his new assignment, he found out that the person currently in the robotics position would be staying for another year. Ross talked to his buddies, and they suggested he try the National Security Agency. He joined NSA in 1990.

"I didn't know anything about computer security at that time, but I had my two advanced degrees," Ross told GCN. "So I had a good grounding in the fundamentals of the system and software."

He said he read everything he could about computers, and "I just fell in love with the field. It was such a fascinating area because back in 1990 computers were important but nowhere near as important as they are today."

Today, of course, IT is woven into everything from weapons systems and power plants to the banking system and government records. And Ross is on the cutting edge of keeping all that technology safe in his current role as a fellow at the National Institute of Standards and Technology and leader of the Federal Information Security Management Act implementation project.

He's the main architect of the Risk Management Framework, a multitiered methodology for agencies to integrate FISMA standards. He also coauthored NIST's security engineering guidelines for federal agencies and the private sector.

Ross compared building stronger computer systems to building stronger airplanes or bridges. "We have confidence because we trust that competent people designed the bridge and the airplane," he said. "That's what we're trying to achieve in this new publication — helping people get the same kind of confidence in the systems and software they deploy in their day-to-day lives."

Another major challenge for cybersecurity is protecting the Internet of Things. Ross raised eyebrows in April when he said the IoT might be indefensible, but he said there are ways to design systems to control the complexity.

"It's not a hopeless situation," he told GCN. "We may have to hang on and be trailing that technological revolution, but we're going to be close behind."

He said his most satisfying accomplishment so far is being able to give back to the military and intelligence communities. As leader of an interagency partnership among NIST, the Defense Department, the intelligence community and the Committee on National Security Systems, he helped create the Unified Information Security Framework so everyone at DOD and the intelligence agencies could focus on their jobs.

"To be able to give back…it's just very gratifying," Ross said. "NIST allows you to do the work you love to do. I've been doing it a long time, and I still love doing it." •

INDUSTRY EXECUTIVE OF THE YEAR: DAVID MOSKOVITZ

In a tight and tumultuous market, the CEO of Accenture Federal Services is building "this tremendous culture of client"

BY TROY K. SCHNEIDER

After several years of retrenchment in federal IT, the past year saw "green shoots" that hint at new opportunities for government contractors. And more often than not, it seemed, those sparks of growth and innovation have involved Accenture Federal Services and its CEO, David Moskovitz.

Accenture won a high-profile contract to put HealthCare.gov back on track and this summer scored a big win as part of the team awarded the Pentagon's much-awaited Defense Healthcare Management Systems Modernization contract. But the firm also had success in other fields, including student loan processing for the Education Department, logistics management for the State Department and suicide prevention efforts for the National Guard.

"Tackling the heart of the largest and most complex issues is really our sweet spot," Moskovitz told GCN.

He has also worked to broaden the firm's range of expertise. The purchase of Agilex Technologies in March enhanced Accenture's analytics, cloud and mobility capabilities. And the company continued to build on its earlier acquisition of ASM Research, which brought expertise in health IT as well as analytics and cloud.

Such moves are helping Accenture Federal Services deliver better solutions to agencies that are modernizing old infrastructure and systems, and Moskovitz has the added advantage of being able to draw on the larger firm as well.

"It's what we call 'powered by Accenture,'" he explained. While Accenture Federal Services has some 6,800 employees, the parent company numbers 380,000, and other divisions can bring world-class expertise in health care payment systems or clinical policies to complement the core team's deep knowledge of the federal space.

With HealthCare.gov, Moskovitz said, "my phone was ringing off the hook from people around the firm...who wanted to help. We landed about 500 people on the ground within six weeks. And about 150 of those people came from outside AFS."

He attributed much of that talent stampede to his colleagues' desire to make a difference. But his management and recruiting style plays a part as well.

"I think of myself as a player-coach," Moskovitz said. And while serving the client is always the top priority, he said he spends a tremendous amount of time thanking and recognizing staff members and making sure Accenture is "an amazing place to work."

"Our aspiration is to be the employer of choice within the federal marketplace," he said.

And although it's clear that growth for the federal market overall will remain limited, Moskovitz's strategy is to focus on key specialties, such as health IT, cloud and analytics, and invest in its employees so it can seize the opportunities that come.

"We have this tremendous culture of client," Moskovitz said. "As long as we deliver, stay close to our clients and provide innovations, we'll continue to do well." •

ZAID HAMID

Honoring the exceptional achievements of the government technology community

AT&T Government Solutions applauds the high performing project teams recognized with **2015 GCN Awards** as Winners, Honorable Mentions and Rising Stars. Thank you for your IT excellence.

att.com/gov

©2015 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.

14 years, 3 billion miles and 2 K

The New Horizons mission team has had to be agile – and very, very patient

BY TROY K. SCHNEIDER

Sprints are in vogue for public-sector IT. Yet when the technology must travel 3 billion miles and arrive at Pluto within a tiny window of opportunity, iterative development and rapid delivery don't always apply.

Such were the challenges faced by the New Horizons mission team, which this summer celebrated a successful flyby of the dwarf planet that was 14 years in the making. (Although the New Horizons launch took place in January 2006, mission preparation began in earnest in 2001.)

And that success was due, in large part, to the meticulous planning – not just for obvious elements such as navigation and telemetry, but for everything from staffing structure to basic hardware upgrades.

For the spacecraft itself, of course, the technology was locked in at launch. Entire ground systems, however, needed to be upgraded – without losing any compatibility or introducing new software glitches.

"From the beginning, before we even launched, we prepared a longevity plan… where we would actually purchase all new hardware," Gabrielle Griffith, New Horizons senior ground systems engineer, told GCN. "We knew [the original equipment] would be obsolete by 2015…. We had to make a lot of code changes to get our custom software stack to work on the new computers."

Those changes required rigorous testing as New Horizons hurtled through space – a discipline that extended to every corner of the mission's technology. Emulators, backup systems, dry runs and multiple eyes on every line of code have been standard operating procedure.

"The test phase is more emphasized in the space world" because there is so little room for a do-over, said Chris Hersman, a New Horizons mission systems engineer.

All that planning and years-out preparation couldn't translate into rigidity, however. When New Horizons reached Pluto just 72 seconds ahead of the arrival time scheduled a decade earlier, for example, it was the result of countless adjustments, not some perfectly precise launch trajectory. Hersman compared it to the zoom-and-adjust process one would use on Google maps to get from a nationwide view down to a particular street corner – done over the course of 3 billion miles.

And the IT team faced problems that would be familiar to any government agency: Off-the-shelf components were used (on the ground) wherever possible to stretch tight mission budgets. Old machines were kept around for spare parts because some systems had to remain on circa-2000 hardware. The archive server filled up faster than anticipated and was running out of disk space just as the spacecraft neared Pluto, requiring quick adjustments on the fly.

As the rendezvous neared, the number of personnel involved ballooned from a few dozen to several hundred – and all of them drew on an IT team whose members could be counted on two hands.

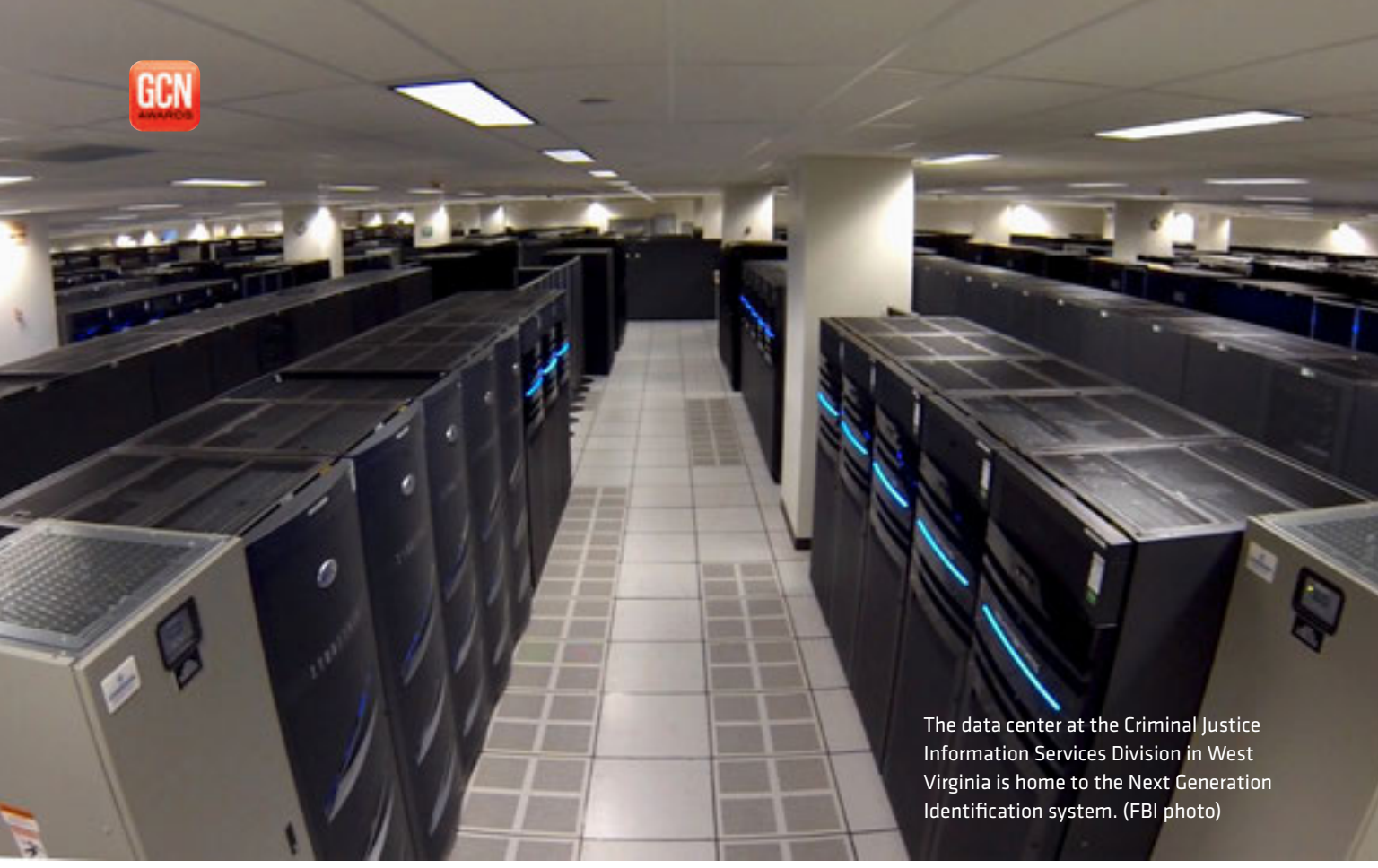
According to Julie Napp, a Unix systems administrator at Johns Hopkins University's Applied Physics Laboratory, it all boils down to a balance of discipline and creativity. Plan carefully, test relentlessly and "when you figure out that something isn't working, then you make tweaks to fix it."

Now, with New Horizons well beyond Pluto, the team's attention is on getting all that flyby data back to Earth – a

kbps data downloads

process that will take 15 months or more, given transmission speeds of just 2 kilobits/sec – and planning for the craft's next big encounter, with the Kuiper belt in 2019. Another hardware refresh is also in the plans, Hersman said, and the mission could extend as far as 2030.

Luckily, he added, "we've got sharp people who are keeping an eye on things and tweaking the knobs." •



The data center at the Criminal Justice Information Services Division in West Virginia is home to the Next Generation Identification system. (FBI photo)

NEW FBI SYSTEM CASTS WIDE BIOMETRIC NET OVER CRIMINALS

The Next Generation Identification project speeds the matching of fingerprints and facial images in criminal investigations

The FBI has a new system for identifying fingerprints and other biometric data that enhances the ability of federal, state and local law enforcement agents to catch criminals.

In unveiling the Next Generation Identification (NGI) system earlier this year, the FBI demonstrated a set of features that boosts the speed and accuracy of its matching systems by an order of magnitude over the 15-year-old Integrated Automated Fingerprint Identification System.

IAFIS, launched in 1999, was designed to handle 64,000 fingerprint-matching transactions daily with an average two-hour response time. In contrast, NGI was built to process 700,000 transactions a day, with a 15-minute turnaround.

Officials began planning for NGI in 2006 with a painstaking series of interviews of 193 agencies and 18,000 law enforcement officials that covered key requirements investigators across the country envisioned for the new system. The survey helped the FBI plan improvements to the speed and accuracy of its fingerprint-matching systems and develop a number of specialized biometric tools, including the matching of tattoos and facial images.

In doing so, the FBI was able to hit performance improvement marks, especially in 10-print matching, the heart of the FBI's investigative toolkit.

"In February of 2011, we changed the algorithm for the 10-print matching system and went from 92 percent to 99 percent accurate," NGI Program Manager James Preaskorn said.

AT A GLANCE

PROJECT: Next Generation Identification System

ORGANIZATION: FBI, Justice Department

Specialized biometric tools and a new algorithm for fingerprint matching have contributed to a faster, more robust ID system for law enforcement.

www.govtechworks.com

Introducing GovTechWorks.com by GDIT

GovTechWorks.com by GDIT is a new kind of news and information source. We cover the nexus between the people of government and the technology they put to use. Our articles and videos are designed to help leaders better grasp the trends and ideas that can make government better, deliver services more quickly and efficiently, increase public trust and confidence, and benefit the public at large.

Type **GovTechWorks** into your browser or just tear out this page for later: **www.GovTechWorks.com**.

---

www.govtechworks.com

GENERAL DYNAMICS
Information Technology

GDIT congratulates this year's GCN Award winners!

As a result, productivity surged. "We ran the system in parallel for one week and had 916 additional hits that we wouldn't have hit before," he said.

Later that year, FBI officials introduced a mobile fingerprint-matching device that gave law enforcement officers access to a data repository on criminals described as the worst of the worst, including sex offenders and suspected terrorists.

"If a cop on the street makes a traffic stop and they have this device, they take one [fingerprint] from that person, scan it, beam it back to us, and within 5 seconds, we'll give it a red light or a green light," Preaskorn said.

The tool's effectiveness has earned it a powerful reputation. Preaskorn said he has heard reports of suspects who have tried to chew or burn off their fingerprints when they saw the device in a police car.

The NGI team also launched a national Rap Back service that notifies agencies immediately when people who have already passed background checks become involved in criminal activities. The service is especially focused on people who work in fields with vulnerable populations, such as education and health care.

In addition, NGI offers facial recognition via the Interstate Photo System, which automates a process that used to involve a victim paging through a book of mugshots.

"If somebody holds up a 7-11, the police department can pull a still picture from the video of that suspect and submit it against our repository," Preaskorn said. The system does not return a one-to-one match but shows officers a range of probable matching images.

Looking ahead, FBI officials want to build a repository for criminals' iris images but are still evaluating the technology options.

NGI was designed to accommodate such updates. From the beginning, developers embarked on an incremental approach that would offer interoperability across commercial devices and build on service-oriented architectures.

"When we built IAFIS, it was designed for a certain workload…under a pretty rigid infrastructure," Preaskorn said. "NGI is designed so you can plug in new modalities as you need to. This was a $1.12 billion system, the biggest the bureau has ever done. We wanted to take it in small chunks. You don't eat the elephant in one bite. And that's why we came up with an incremental strategy."

— Paul McCloskey

NIH-BUILT TOOLSET HELPS RESEARCHERS SHARE AND COMPARE DATA

BRICS offers biomedical researchers a modular, generic and rapidly deployable system for global collaboration

On battlefields across the Middle East and football fields in the United States, traumatic brain injury (TBI) has hit near-epidemic proportions in the past several years. Officials at the Centers for Disease Control and Prevention say it leads to 52,000 deaths and 275,000 hospitalizations in the U.S. each year.

The spiraling caseload is pushing biomedical researchers to stretch their increasingly tight budgets and maximize their research to help prevent TBI and other serious health threats.

The National Institutes of Health has developed a set of software modules that researchers say are meeting both goals. The Biomedical Research Informatics Computing System (BRICS) gives scientists from different fields of research access to a common set of data management tools they can use to share results and discoveries more easily and frequently.

AT A GLANCE

PROJECT: Biomedical Research Informatics Computing System

ORGANIZATION: National Institutes of Health

Standardized data definitions and a modular toolset make it easier for researchers to combine and search data.

BRICS is a "set of tools that can be easily combined to help advance research by using informatics," said Matthew McAuliffe, chief of NIH's Biomedical Imaging Research Services Section.

In the past, researchers captured information in a variety of ways, which made it nearly impossible to compare datasets, he added. BRICS standardizes data definitions and records data consistently across all studies.

"The thing that's really exciting now is that data can have a longer life, [which] means that research is going to be shared more quickly as opposed to what often happened — data would be in somebody's lab and then be lost," McAuliffe said.

Work on BRICS began when the Army's Medical Research and Materiel Command approached NIH for help in developing a research database for TBI. "We said, 'OK, let's take a step back. Let's build a modular system that we can use for TBI,

but we'll keep it modular, generic and easily instantiated,'" he said. "Essentially, that was the motivation for everything."

BRICS forms the basis of the Defense Department-managed Federal Interagency Traumatic Brain Injury Research, but its influence has expanded beyond its original goal. BRICS supports the Parkinson's Disease Biomarkers Program from the National Institute of Neurological Disorders and Stroke and is the basis of the National Eye Institute's eyeGene, which seeks to advance the study of eye disease and its causes.

There are six components to the BRICS toolset, several of which McAuliffe considers "foundational," including a data dictionary that helps researchers accurately locate data that is most relevant to their research.

"We consider that foundational because all the data that goes into the system is collected consistently," he said. "Study A collects age data the same way Study F did. That way, you can combine the data easily and search it more easily."

In addition, the Global Unique Identifier helps collect de-identified data consistently over time to help chart disease progression, and ProForms is an electronic data capture tool that builds electronic forms and maintains data consistency.

In the future, BRICS will run on the Drupal open-source content management framework, which is often used for knowledge management and collaborative applications. McAuliffe said the biggest advantage will be the ability to update content quickly.

"We won't have to wait for the next deployment or ask the developers to add information to the site," he said. It will also be easier to incorporate public-facing features to the site, including social or video tools and widgets.

As BRICS-based platforms grow, they will need to meet greater data storage requirements, especially in genomics research. McAuliffe sees that as one of the project's bigger challenges and believes cloud might be the answer.

"With genomics, you are looking at an immense amount of data," he said. "We want to see if we can maybe store that data out in the cloud and still make it discoverable."

Meanwhile, BRICS developers are deciding whether to formalize an application programming interface for the data dictionary. "If we make it formal, then others can connect to it and convert their data in a way that's more consistent with the installation of BRICS for that community," he said.

— Paul McCloskey

UNRAVELING A WEB OF FRAUD

Los Angeles County built a platform that links data mining, social network analysis and rules management to fight child care fraud

When Los Angeles County began to explore data mining to help track fraud in its California Work Opportunity and Responsibility to Kids Child Care Program, it was daunted by the complexity of the scams it faced.

The county's Department of Public Social Services (DPSS) began to see signs of escalating collusion among providers and recipients in the program, which helps low-income families pay for child care services so parents can go to work.

"The collusion occurs between the care providers and the recipient, and then it expands like a web," said Michael Sylvester II, assistant director of the county's Bureau of Contract and Technical Services.

In a typical fraud scenario, an unlicensed provider takes care of many

children in a home setting. Kickbacks might flow from a provider to a care recipient or from provider to provider across large and small networks.

Another common scheme is for a provider to receive CalWORKs money when kids are actually in free after-school child care or at home. "That person is really not providing child care," Sylvester said. "Instead, they are taking the child care fees and divvying them up in many different ways."

More and more of the collusion is driven by fraud rings. Identifying the size and scope of those networks provided an incentive to increase the county's investment in an anti-fraud data-mining solution.

"The rings can get pretty big," Sylvester said, adding that the county's original goal was to find out how far the criminal networks extended. To do so, officials launched the Data Mining Solution (DMS) for Child Care Welfare Fraud Detection.

DPSS drew on the SAS Fraud Framework for Government to build a platform that ties together data mining, social network analysis and rules management applications. The county's data is maintained in a secure cloud hosted by the company's Advanced Analytics Lab for State and Local Government.

The social networking analytics have helped the county drill down into program data and begin to identify fraud networks. Via a dashboard, investigators can pull up data on providers, families using the providers, the work locations and the phone numbers of people tied to those locations.

"You start to see how the linkages spawn off," Sylvester said. "This lets our investigators really drill into the data, open it up and find out, my goodness, there are 10 others associated with that beneficiary."

The county also developed a triage unit to analyze alerts and funnel suspected fraud cases to investigators. The triggers are activated by business rules showing potential fraudulent activity, such as a person reporting income paid in cash or an unusually long distance between a beneficiary's home and the child care site.

So far, the system has had a positive financial impact, said Sylvester, who estimates that the project has cut time to prosecute fraud investigations by 18 months and generated millions in annual cost savings. It has also led to hundreds of fraud referrals to county caseworkers, leading to cost avoidance savings throughout the department.

Looking a few years down the road, Sylvester predicts that data mining and other tools will continue to improve investigators' ability to find new data sources that will help them stay in front of their casework. Some of those sources might eventually include external public- and private-sector data.

"Realizing you have huge data stores with information in them that can be pulled out and put together, it's incumbent on all of us to find ways to put them in the budget and enable investigators who are really working hard to catch perpetrators," Sylvester said.

— Paul McCloskey

AT A GLANCE

PROJECT: Data Mining Solution for Child Care Welfare Fraud Detection

ORGANIZATION: Department of Public Social Services, Los Angeles County

Social networking analytics and targeted business rules allow investigators to dig into program data and reveal fraud rings.

PUTTING A REFERENCE LIBRARY IN DIVISION OFFICERS' POCKETS

Two junior officers' idea for making critical information more accessible at sea sparked the eDIVO mobile application, which is now used throughout the Navy

Navy vessels are complicated places, and the learning curve for junior officers can be daunting. Division officers, or DIVOs, are responsible for critical functions that include electrical maintenance or engineering — duties that require ready access to a vast array of manuals, books and other reference documents. Too often, DIVOs on their first sea tour would discover that those materials were not accessible when and where they were most needed.

When Lt. Charlie Hymen and Lt. John Harry came off sea duty, they were convinced there was a better way than relying on paper printouts, random PDF files and word of mouth. They approached Vice Adm. Bill Moran, chief of naval personnel, with an idea for a mobile application containing all the necessary information — and out of that discussion came eDIVO.

The Sea Warrior Program — which manages IT systems to support a wide range of Navy missions — further explored and developed the lieutenants' idea into a fully operational solution in

Ken Johnson, technical director of the Sea Warrior Program, demonstrated the eDIVO app at AFCEA West in February. Photo by Krishna Jackson/Navy.

just seven months. The application was released in March in both the Android and Apple stores, and the result has been "a higher level of proficiency earlier in the tour, and subsequently a more efficient and successful mission for the DIVO and the entire ship's complement," according to Navy officials.

The application allows sailors to use their own smartphones or tablets to easily access more than 8,300 pages of publicly available information concerning division management, personnel management, bridge operations and emergency functions. The materials are searchable and stored in the app so that no network connection is required. It puts a full training library in sailors' pockets.

The app was developed through seven month-long sprints, each of which was followed by functionality tests and feedback from users to help developers make adjustments. The finished product includes a tutorial that familiarizes users with all the functions and services the application features.

The eDIVO application was downloaded more than 10,000 times in the first month after its release. One early user gushed: "Fantastic! As a brand-new DIVO, this is invaluable. A one-stop resource for some of the basics, as well as the essential publications for taking care of my people, is a great help. I'll be recommending this to all my fellow DIVOs."

Given the success of eDIVO, the Sea Warrior team is planning additional training apps — and the lessons learned during the eDIVO process are projected to cut development time to four months or less.

— Mark Pomerleau

AT A GLANCE

PROJECT: eDIVO Mobile App

ORGANIZATION: Department of the Navy

Division officers now have easy access to 8,300 pages of searchable job-related reference material, in place of paper documents and PDFs.

Utah state legislature at work in the House chamber of the state capitol

UTAH DASHBOARD SHORT CUTS LEGISLATIVE ANALYSIS

The Fiscal Note Agency Response System has improved the state's ability to assess the financial impact of proposed legislation

Passing laws can be a labyrinthine process that is often complicated by an increasingly common requirement: the need to provide an analysis of proposed legislation's estimated financial impact on government.

In Utah, the process was creating bureaucratic and workflow bottlenecks that strained the ability of the state's Office of the Legislative Fiscal Analyst (LFA) to review new legislation affecting 120 agencies.

During each of the state's six-week legislative sessions, LFA is called on to create a "fiscal note" that summarizes input from the state's tax commissioners, various agencies and financial analysts on the effect each proposed bill would have on state revenue and expenses.

LFA prepares approximately 1,100 fiscal notes during each session in a process that involves collecting spreadsheets, commentary and analysis from an average of five agencies for each proposed bill. And time is of the essence: Fiscal notes must be filed within three days of a new bill's introduction.

"We were able to meet those deadlines only about 60 percent of the time,

AT A GLANCE

PROJECT: Fiscal Note Agency Response System

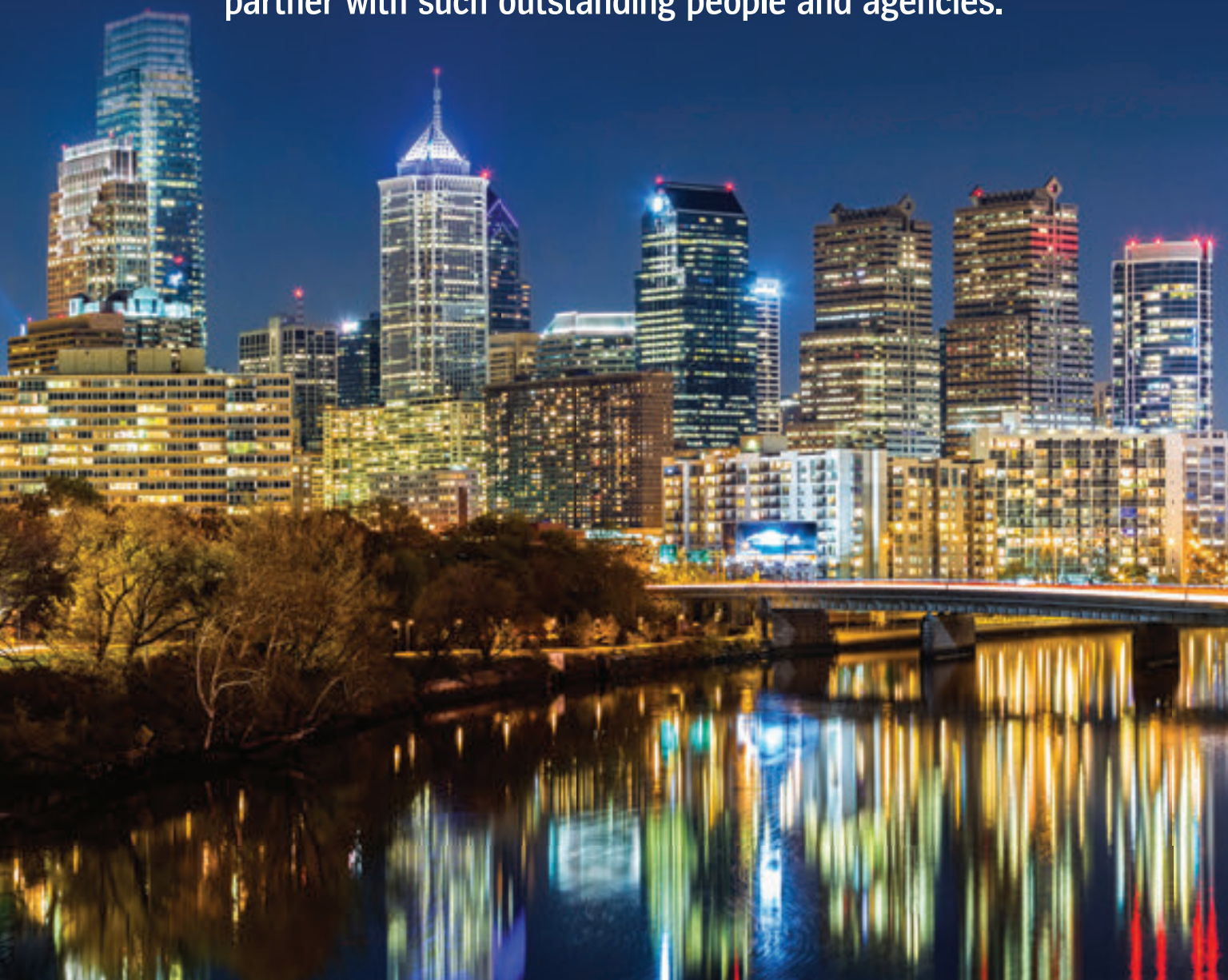
ORGANIZATION: Office of the Legislative Fiscal Analyst, Utah

An automated system for gathering projected expenses and an online collaboration engine helps fiscal analysts respond more quickly to proposed legislation.

UNISYS

Unisys Congratulates the City of Philadelphia's Philly311 project and all the 2015 GCN Award Winners.

Thank you for your significant contributions and ongoing commitment to enhance government. We are proud to serve and partner with such outstanding people and agencies.



so we were not doing well," LFA Director Jonathan Ball said.

The office looked for ways to streamline the routing and analysis of fiscal notes and sought to clear bottlenecks by opening up the office's legislative workflow to more collaboration. As a result, officials began developing the Fiscal Note Agency Response System last year. The custom system gathers projected expenses and revenue changes for each bill and stores the information online for fiscal analysts to review.

The system uses Microsoft's .NET framework to transmit new bills to a Java-based web service. LFA analysts can view pending actions via a dashboard, and a countdown clock helps them prioritize their responses to requests.

The dashboard also shows previous responses and lets analysts link bills to specific funding codes and other offices that would be affected by the proposed legislation. Fiscal analysts can communicate with other budget analysts more freely, often resulting in faster and more creative analysis.

"The basic inspiration came from looking at crowdsourcing and wikis," Ball said.

Early on, officials realized that most of the bottlenecks were simple sequencing requirements. "We had supervisors reviewing notes and assigning them to analysts — that's a bottleneck," Ball said. "Then we've got the analysts reviewing and assigning to agencies — that's another. So we started to ask: Why can't we have all these things going on at the same time?"

The first step LFA developers took was to write scripts that would automatically assign bills to analysts and agencies, which cut down on the time spent waiting for analysts to make the assignment.

Now officials are exploring the next steps for its dashboard, which include expanding the reach of its analytical features. One area of focus is forecasting agencies' ability to fund legislation and checking potential alternate sources of funding.

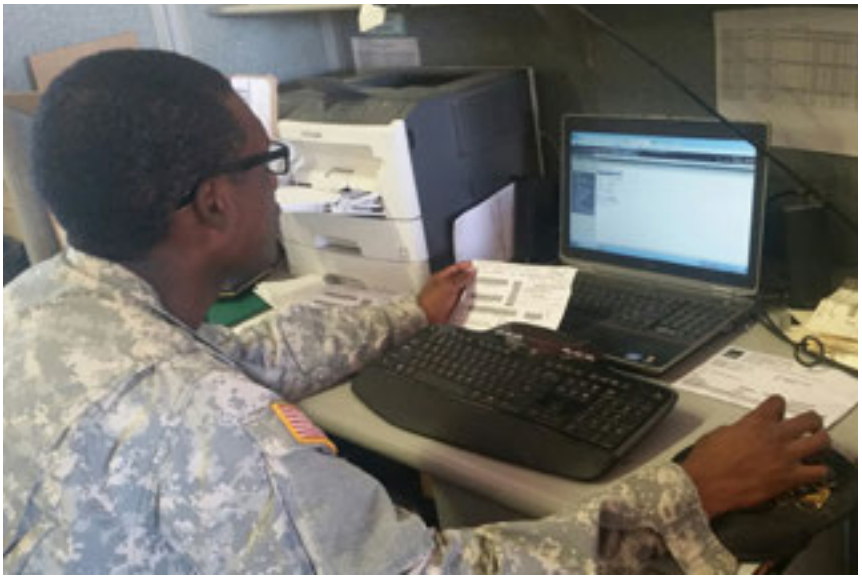
The office has also discussed ways the financial data it gathers might be made available to the public via an electronic platform. "This is the public's data after all," Ball said. "It would be interesting to have civic developers create something new we haven't thought of yet."

Overall, the project has significantly improved the state's grasp on its financial posture, Ball said.

"I think the quality of our analysis is better, and we have more time to think about it and shoot ideas back and forth," he said, adding that LFA's on-time performance has improved from 60 percent to 98 percent.

"A lot of it has to do with the fact that we're not spending time organizing paper," he said. "We were spending so much time organizing this stuff before and not enough time analyzing it."

— Paul McCloskey



TRANSFORMING 40,000 DATABASES INTO ONE CONSOLIDATED LOGISTICS SYSTEM

The Global Combat Support System-Army seeks to deliver "one version of the truth" for Army logistics data anytime, anywhere

The Army is well into a project it has called the "most significant transformation effort in history for a logistics information system."

The Global Combat Support System-Army (GCSS-Army) is designed to merge the work of 40,000 local databases that perform tactical, supply, property, maintenance and financial logistics functions. The new system will support nearly

154,000 end users in the Army, National Guard and Army Reserve.

Using enterprise resource management software from SAP, the system seeks to offer commanders a composite view of logistical data to sharpen decision-making on and off the battlefield.

"For the first time, GCSS-Army is tying in a logistics function for all associated financial transactions into a single consolidated database," said Lt. Col. Christopher Romero, product manager of GCSS-Army.

By providing near-real-time information on cost and supplies, the system will enable commanders to build "a complete logistics picture where they can make sound tactical decisions, manage budgets effectively and enhance their readiness," he added.

The goal is to have a unified view — "one version of the truth in real-time data," Romero said — of the logistics status of Army units that is available anywhere, anytime.

AT A GLANCE

PROJECT: Global Combat Support System-Army

ORGANIZATION: Department of the Army

A unified view into the contents of 40,000 logistics databases supports better tactical decisions on and off the battlefield.

Those features will also eliminate the need to reconcile costs between the older systems — a benefit the Army estimates will save two hours a day for the average soldier working at a supply office. Furthermore, the system is a key component of the Army's strategy to be financially auditable by the end of fiscal 2017.

The Army has divided the massive transition into two waves. In Wave 1, expected to occur in fiscal 2016, the Army will switch out all Standard Army Retail Supply System and associated financial management systems. In Wave 2, the Army will replace the Property Book Unit Supply Enhanced and the Standard Army Maintenance System-Enhanced.

In addition, the Army has mounted a significant program to educate users on the new system through simulations and other online exercises. The backbone of the initiative is a website that offers training materials on new applications and new terminology. Simply changing the term "requisition" to "purchase order" can affect business processes and users at all levels of the Army, Romero noted.

"Soldiers are more tech savvy today," he added, "but it's critical they get informed about the program early, take the web-based training and provide stakeholders [with] feedback."

Army officials say the GCSS project is already beginning to pay for itself, primarily by avoiding the costs related to managing legacy logistics systems. Within the first years of full system deployment, the Army expects to save at least $8 billion in avoidable costs.

— Paul McCloskey

FINDING CHILD VICTIMS IN A HAYSTACK OF FORENSIC IMAGES

A DHS program uses the latest tools to identify victims of child sexual exploitation and pursue their traffickers

According to the Homeland Security Investigations agency, one in five girls and one in 10 boys in the United States will be sexually exploited before they reach adulthood. Protecting victims and catching offenders has been the focus of thousands of federal, state and local law enforcement agents.

In 2011, the HSI Cyber Crimes Center's Child Exploitation Investigations Unit (CEIU) created the National Child Victim Identification Program to identify and rescue child victims, apprehend offenders and locate crime scenes. The program included a Victim Identification Laboratory where seized images, videos, audio and metadata are analyzed, enhanced and clarified.

Investigation of child pornography trafficking generates more data than many law enforcement agencies can process. In 2014, CEIU seized 5.2 petabytes of data, 52 percent of which involved child sexual exploitation. Unfortunately, much of it is inaccessible because investigators lack standard technologies to share data across the law enforcement community.

To meet the challenge, in 2012 CEIU joined forces with officers from across the law enforcement community, including the International Centre for Missing and Exploited Children (ICMEC), to launch Project Vic and put the latest forensic tools to work sifting through evidence of victims of child pornography.

Richard Brown, technology advancement officer at ICMEC, said the primary goal of Project Vic was to get law enforcement "on the same page when it came to standardizing the way they exchanged data with each other and the services they need to access."

Tool providers had been using pro-

prietary methods to manage forensic data, he said. In addition, the group became aware that police officers worldwide were duplicating their efforts by examining the same images over and over.

To categorize the data, Project Vic originally relied on binary hash sets — MD5 digital signatures generated by algorithms — to identify whether seized evidence matched existing library files and datasets. The hashes were maintained in a database police could check to see which images had already been identified. Early versions of the tool were effective in scoring matches, but they tended to support a focus on offenders.

"What we're not doing is finding new victims within that data," said James Cole, national program manager for victim identification at the Department of Homeland Security. "Instead, we were doing the equivalent of shoving that victim in the evidence room."

"The mantra of Project Vic is: 'That's not where you should be focusing your efforts,'" Cole said. "What you should be focusing your efforts on is the stuff that didn't hit. It's the stuff that's new to our system because that's where new victims will be."

AT A GLANCE

PROJECT: National Child Victim Identification Program

ORGANIZATION: Department of Homeland Security

Binary hash sets and an open-data exchange format help investigators match images and analyze new child exploitation cases.

TOOLS OF THE TRADE

Project Vic's leaders are working on ways to give investigators more than binary-level tools to process forensic data. Instead, they want to foster a network of collaborators who can contribute open standards-based tools to help analyze new child exploitation cases.

Recently, the project adopted an open-data exchange format called OData, which allows vendors to pass data between different forensic tools more easily "instead of being in proprietary boxes," said Cole, who calls it "one of the huge tenets of our project."

Using OData, Project Vic also developed a protocol called the Video, Image Classification System that supports querying and exchanging hashes without the need to manipulate files directly. VICS was developed to help police agencies focus on victims and other never-before-seen materials.

In December 2014, Microsoft donated its PhotoDNA Cloud Service to Project Vic and offered it as a cloud service to other organizations through the Microsoft Azure marketplace. PhotoDNA can help identify exact copies of an image or video that might have appeared on various websites. The tool is especially useful to investigators trying to identify whether a photo taken by a mobile phone is identical to a copy of the photo generated by social media sites, for example.

"When the next person uses those hashes, it's not only going to pick up on the exact match but it's going to pick up on visually duplicative matches," Brown said.

More recently, advances in imaging forensics have prompted development of tools that can perform more complex matches and help law enforcement agents pursue victim-centric strategies. That includes tools from Griffeye, formerly NetClean.

The firm said in April that its Analyze Digital Investigator would incorporate Analyze Relations, a feature that will "actively help to connect the dots between images and assist in building visual maps that abstract intelligence from visual big data."

The software identifies relationships within images by comparing multiple types of data and metadata, including what kind of camera was used to take the photos, attributes within the images, and where and when the image was taken. More than 2,500 law enforcement agencies in 30 countries use the Analyze platform, the company said.

Recently, Project Vic began exploring more complex facial recognition techniques, particularly for images that don't show a conventional snapshot view of the subject.

"Doing facial recognition from images that are all in conformity is easy because you can count the different points on the face and actually match them," Brown said. "What we're looking at is more complex facial recognition, where you get a three-quarter or tilted view of the child or suspect."

Project Vic is also evaluating technology Microsoft is working on that can gauge a person's age. "It would be useful if an investigator can say, 'Show me all females who are 18 or younger or show me any six-year-old,'" Brown said.

Another tool, dubbed F1 Video, would help investigators identify images hidden or obscured in often hard-to-reach video formats. The technology creates a hash of offending video clips that might be a short burst of a child pornographic video appearing several minutes into another piece of video or movie. F1, donated to ICMEC by Friend Media Technology Systems, allows investigators to crop the abusive material and put it into the cloud, where it can be matched against other video categories.

Collaborators say Project Vic's mission is to create an ecosystem of data-sharing partners to protect victims and find perpetrators of child exploitation.

Project Vic seems to be meeting both goals. By the end of 2014, partner organizations identified and rescued more than 1,030 child victims. And within a three-year span, the project helped increase criminal arrests by 67 percent and convictions by 55 percent.

Cole looks at the success in this way: "When we in law enforcement child exploitation cases focus on offenders, we will miss victims. But if we focus on finding victims, we will not miss the offenders."

— Paul McCloskey

INNOVATION THAT WAS WORTH THE WAIT

A funding crunch put plans for Philadelphia's 311 non-emergency system on hold for years, but the payoff was better technology and new levels of citizen service

Philadelphia's 311 non-emergency system for information and service requests got its start on New Year's Day 2008. At the time, plans for updates and expansions were scheduled for the next year and a half, but then everything stopped.

"It was supposed to take 18 months from start to finish, and it was supposed to be completed by spring 2009 and no later than the summer," Rosetta Carrington Lue, senior adviser and chief customer service officer for the city's managing director, told GCN. "We would have the centralized operations available, and phase two would be implementing more complex technology for better customer support. The third phase was for improvements based on what we were hearing."

By the summer of 2008, however, the country had plunged into a recession, and city budgets were slashed. "We had to put phase two of the project on hold, which was the installation of robust technology," Lue said. "So the original technology was supposed to be there only about four to six months, [but] six years later, we were still using this technology."

Six years is a long time for technology, and social media exploded while Philadelphia's 311 system was on hold. The system's technology grew outdated and the office became understaffed, but in 2014 Philadelphia Mayor Michael Nutter got some funding and chose Philly311 as one of eight technology projects to move forward.

Lue and her staff wanted to go beyond making simple upgrades. They wanted to change how residents made requests to the city and give them the ability to track those requests and give feedback on how the city responded.

"Our customers had a higher expectation on service delivery and response time, and they also wanted various channels to communicate with the city, meaning we had to look at what kinds of software can we use to implement that omni-channel experience," Lue said.

And the city had an opportunity to track and use data. "We needed a system to help us analyze data and turn it into information very quickly in a time of crisis or a time of ongoing need where we needed to not just look at the data but show us trends, mapping, hotspots," she added. Officials wanted a model that "would enable leaders to make a better decision based on the information they have in front of them versus waiting weeks for IT to organize all of it."

AT A GLANCE

PROJECT: Philly311

ORGANIZATION: City Manager's Office, Philadelphia

Mobile-friendly interfaces, citizen-driven design and a modernized CRM help deliver better government service.

With the help of Unisys, Lue and her team created a customer relationship management system based on Salesforce's CRM platform. The system was released in December 2014 after 11 months of development, and it immediately changed the way residents make requests.

In the past, when Philadelphians called 311 with a service request, such as a pothole they wanted fixed, they would have no idea when the city would get around to addressing it, which led to frustration for residents and repeated calls to 311.

People can now make requests via phone, web or a host of social media platforms including Twitter and Facebook, and after a request is made, the person receives a timeline for resolving the issue and a tracking number to keep up with the request without having to contact 311 again.

"We're giving our residents and customers the opportunity to report something and actually see what's going on with your request," Lue said. "That was important to the mayor.... [And] we have service agreements with the departments, so when you call in, we outline the process and set the expectations for you."

Those service agreements are part of Philly311's efforts to better partner with other city departments on requests that are complicated or require a more in-depth response.

One of the highlights of the new system is that police officers can now check on a citizen's request right from their police cruisers.

"There are about 1,000 police vehicles" out in the city, Lue said. Anytime officers are talking to community members and hear about a 311 complaint that has not yet been addressed by the city, "the police can go back to their vehicle, put the address in and the information pops up."

Lue wanted to make sure that the system would be easy for customers to use, so local citizens were involved in its design from the beginning. "We brought them in early in the process to help us, and that saved us time when it came to implementing the system and rolling it out," she added.

Lue said the unplanned six-year hiatus allowed her staff and other city departments to study trends and new technology, and to make the best decisions once funding became available.

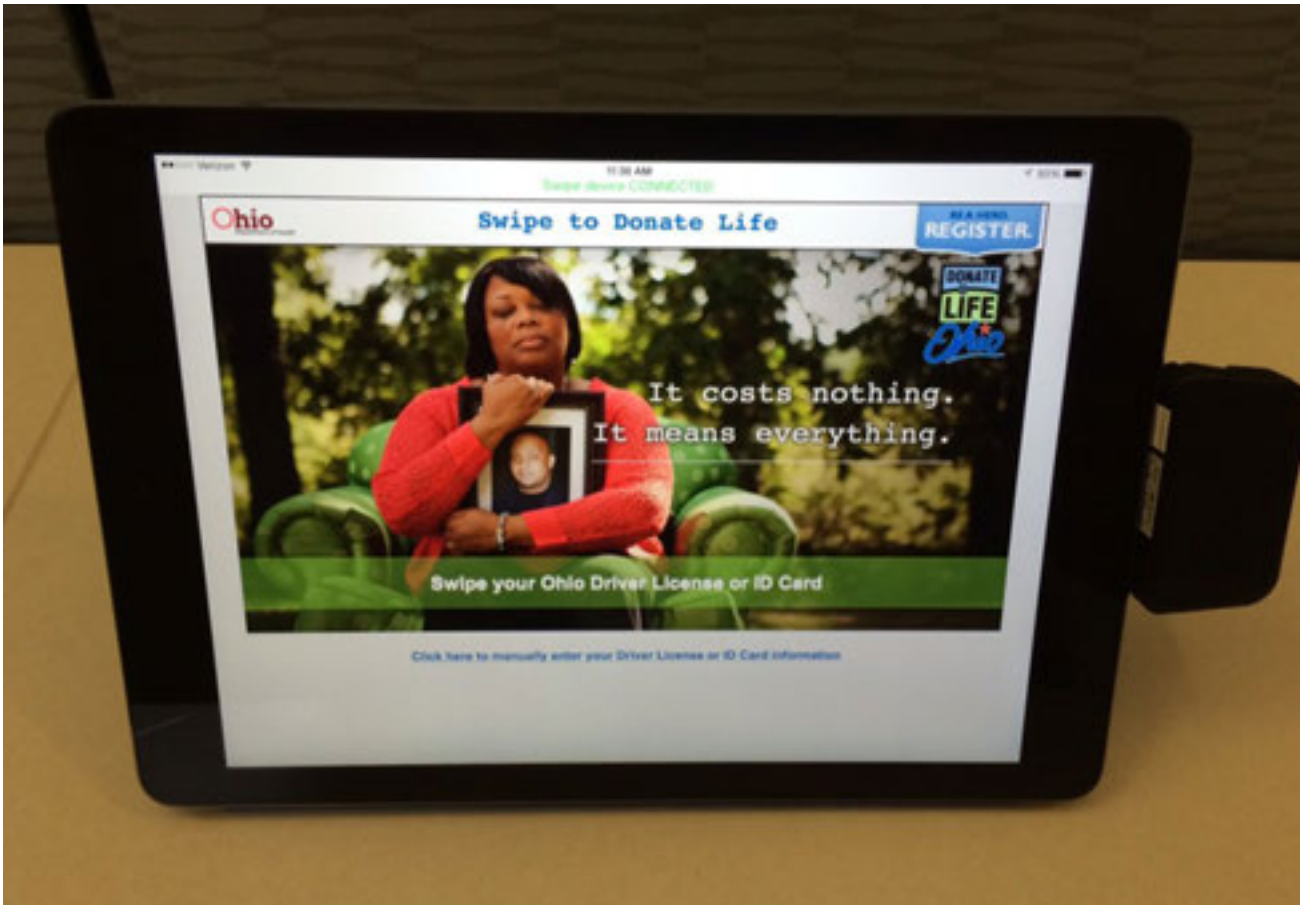
"Really it was a blessing in disguise," she added. "We were able to bring about 100 people together from different city departments and say what we like and what we don't like when it comes to the technology and getting things done. Those six years really gave us a chance to see how data was coming in and how it would be used, how we could be more efficient and effective. We were able to take all the lessons learned and say this is what we need as a city to ensure we have the right platform."

— Derek Major


COMING TOGETHER FOR THOSE WHO
KEEP US CONNECTED
Lockheed Martin is proud to support the GCN Awards Gala. We extend our heartfelt congratulations to all of this year's winners, and we honor these superior information technology professionals who make a difference each and every day.
lockheedmartin.com/cyber
LOCKHEED MARTIN
We never forget who we're working for®
© 2015 LOCKHEED MARTIN CORPORATION

HELPING OHIOANS UNDERSTAND AND EMBRACE ORGAN DONATION

The Swipe to Donate Life project used existing systems to build a much better process and reach more would-be organ donors



In October 2014, Ohio launched a project that would help the 123,000 Americans on the national waiting list for a life-saving organ transplant while also educating Ohioans about the important decision of becoming an organ donor.

The Swipe to Donate Life program was a collaboration between the Ohio Department of Public Safety (ODPS) and Donate Life Ohio, the state's coalition of four of the 58 nationwide organ procurement organizations (OPOs) in the country.

According to Marilyn Pongonis, director of communications at Columbus-based OPO Lifeline of Ohio, 99 percent of the state's registered organ donors signed up when they were getting or renewing their driver's licenses at a local Bureau of Motor Vehicles.

Four in 10 Ohioans, however, do not sign up to be organ donors. Many people are not ready to make that decision or they have questions or are unsure what it means to be an organ donor — and it's not the BMV's job to provide them with that information.

Additionally, the BMV registration process lacks the option for would-be donors to specify whether they would like to be an organ, eye and/or tissue donor, which causes most registrants to unknowingly sign up for all three.

That is where OPOs come in. Staff members and volunteers go to state functions and public events — such as college football games, state and county fairs, and health expos — to educate and register interested individuals in the organ donor program.

Previously, that meant carrying

around clipboards or laptops and asking Ohioans to provide driver's license data and personal information. The process was tedious and resulted in low registration numbers. According to Pongonis, Wi-Fi connectivity to BMV's online services was often unreliable, which made laptop-based registration impossible at some events. And when paper-based registrations were gathered, OPO staffers worried about keeping the sensitive personal information secure on site.

When an event fell on a weekend, Pongonis said she would often have to take the paperwork home with her and make sure it was safe until she could get it to BMV the following Monday.

All those concerns prompted Donate Life Ohio to search for a way to make it easier for people to sign up at events. They decided that the answer was letting drivers swipe their licenses through a card reader and update their records.

Donate Life Ohio officials looked at how colleagues in Arizona were using swipe devices and contacted some vendors, then decided to reach out to the Ohio BMV about possible system improvements. And after exploring the option of existing vendor solutions, ODPS ultimately decided to take a do-it-yourself approach to the license-swiping technology.

For one thing, many of the devices on the market stored personal information and then downloaded it to the donor registry center at a later time, which ODPS decided was an unacceptable security risk. Officials also had concerns about the development and ongoing maintenance costs and especially about the confusing interfaces when the new tools were added to the existing system.

According to Keith Albert, chief of ODPS' IT Project Management Office, the fact that BMV already maintains the organ donor database and delivers best-in-class customer service through its website convinced officials that there was no need to outsource the project.

The idea of swiping a driver's license to gather information is not a new concept to Ohio either. According to Albert, the state has been doing that for 20 years — at local BMVs and in state highway patrol vehicles. By accessing the existing framework and resources, ODPS could easily optimize BMV's website and attach a card reader to a mobile device.

The ODPS IT team first replaced the original Ohio organ donation website's ASP.NET form with Microsoft's Model View Controller in order to make it mobile-compliant and scalable to any size screen. That enhancement also allows citizens to register and edit their donor preferences themselves from any connected mobile device.

AT A GLANCE

PROJECT: Swipe to Donate Life Program

ORGANIZATION: Ohio Department of Public Safety

Mobile devices equipped with card readers and a secure connection to the Bureau of Motor Vehicles database are boosting outreach to potential organ donors.

The team then bought Apple's software development kit for $99 to create the "wrapper" application that would support the card swipe, which can only be used by OPO personnel on their iPads. The application has a SQL server backend and pulls data from an attached MagTek iDynamo 5 card reader.

No data is stored on the actual device at any time. When a card is swiped, the individual is asked to provide the last four digits of his or her Social Security number. In less than 30 seconds through a secure Verizon 4G connection to BMV's private server, the individual's registration is automatically updated and stored to the BMV database.

Nothing remains on the iPad after the transmission is completed.

Using 4G also puts connectivity concerns to rest. "In Ohio, we're very well wired here. There are only a few places where there's not 4G connectivity, and those places aren't likely to have any real events," Albert said. "We haven't had an issue since we've gone live."

On the OPO's end, the application is designed just for Ohio, is extremely easy to use and has been far better received by the public than the paper- or laptop-driven systems. And with the much-improved processing time, OPO staffers can increase their turnaround rate and register more interested citizens at a given event.

"It's just been a wonderful enhancement to our outreach in the field," Pongonis said. "We're able to look at currently registered people and…talk to them about what that decision at the BMV meant. If they want to put restrictions on it, they can."

Pongonis also stressed the importance of having more time to educate people about what it means to be a donor and how that decision is ultimately binding.

The cost of the project has been minimal. According to Albert, ODPS was able to execute the entire project for less than $6,000. Equipment was a separate cost funded by the Ohio Department of Health. Apple iPads ranged from $400 to $500 each, and the card reader was about $75. Donate Life Ohio bought about 12 iPads to start.

Signups in the field still fall far short of those done at local BMVs, but Pongonis said the new system has clearly improved on-site efforts. And she can tell citizens are more comfortable with the process.

"The number of folks signing up at these events has really gone up significantly," Albert said, sometimes by as much as 300 percent. And "the citizens of Ohio got what they needed because, ultimately, someone's life will be saved because someone signed up to be an organ donor at one of these events."

— Amanda Ziadeh

PENNSYLVANIA SPINS UP 21st-CENTURY FINANCIAL SYSTEM

After a mainframe failure, state officials took advantage of the opportunity to build a system that would automate payments and standardize data collection

Pennsylvania officials have released a set of applications that helped them catch up on nearly a decade's worth of financial service improvements in the aftermath of a mainframe failure.

The upgrades have given the state greater control in meeting its financial requirements. Features include software that gives managers the ability to audit the 21 million payments the state's Treasury Department makes annually and tools that standardize data access at 60 Pennsylvania agencies.

"Technologically speaking, we migrated from the 19th to the 21st century," said PN Narayanan, CIO of Pennsylvania's Treasury Department. "We were in a place where we didn't have any way to predict or to provide reliable systems, and now we have a technology and infrastructure that [are] much more integrated, reliable and much more secure."

When the state's aging mainframe failed in 2008, it exposed to risk some $10 million worth of payments the commonwealth made on a daily basis and triggered a massive disaster recovery effort. It also touched off the financial service transformation.

"It couldn't have happened at a more convenient time — the day before Thanksgiving, [which gave us] four days to recover," Narayanan said. Even so, it became clear that the vintage system, which was supported by a dwindling workforce of Cobol programmers, needed to be replaced.

In the aftermath of the mainframe failure, Treasury officials formulated a plan to automate payments from all branches of the state government and its three major pension systems. The plan called for Treasury to replace the mainframe and 25 internal systems, establish a common general ledger code structure across the state, build standard XML and web service interfaces for all agencies, and audit all payment records.

The plan gained momentum when officials realized the human cost of what was at stake. "The legislature realized very quickly that if payments could not be made, vulnerable citizens would be in trouble because they could not get payments at the right time, including health care benefits or unemployment checks," Narayanan said.

AT A GLANCE

PROJECT: Pennsylvania Treasury Transformation Project

ORGANIZATION: Treasury Department, Pennsylvania

The consolidation of core financial functions and adaptable algorithms have given financial managers greater insight and control.

Central to the project's success was finding software tools that could give auditors and financial managers a greater degree of control over and access to data on individual payments and audits. In particular, officials needed to meet a requirement that every payment that left the state was lawful and accurate. That meant developing the ability to conduct prepayment audits of transactions with a limited number of financial analysts on the payroll, Narayanan said.

To maintain an accurate payment stream and defend against fraud, officials had to improve financial managers' ability to target different datasets and set up audits on the fly, he added. It was a capability that would have been almost impossible under the old mainframe.

That system's constraints forced the department to make best-case approximations of the payment data stream. Auditors could only sample payments beyond a particular, often preset, threshold and had to infer whether all the other payments would be accurate or not.

For the new system, the department issued a request for proposals for tools that could produce audit algorithms for scrutinizing each tax dollar the state spent. "The idea was to replace the entire payment system, revamp all the investments and consolidate the core financial functions into an [enterprise resource planning] system," Narayanan said.

Treasury uses Oracle's PeopleSoft Financials to handle cost-payable processes and Oracle Governance, Risk and Compliance for audit analytics and forensic analysis on payment processes. The GRC module also helps managers see who made critical changes to system setups and what users have done with the authority they've been assigned.

Officials worked with the product developers to adapt it for prepayment audits, a twist that helped Treasury create rules without the IT department's involvement.

"With this set of technologies, analysts and auditors can alter their own algorithms," said Sid Sinha, Oracle's senior director of application develop-

ment. "They can create a rule that is much like an audit checklist, or they can say, 'I want to look at this agency or vendor.' Over time, they can be much more responsive to changes in their environment."

The Pennsylvania team also tackled its data networking backbone, especially the task of building common interfaces for different source systems.

"We were receiving files from multiple different sources, including SAP, PeopleSoft, mainframe systems and homegrown systems," Narayanan said. Eventually the department standardized on XML, a move that eliminated having to "deal with 30 different interfaces for moving data among 60 different offices and agencies."

The whole transformation has given financial managers a clearer overview of transactions. "Visibility across our different teams — controller, audit cash management and treasury teams — has improved a lot," Narayanan said. "We can see at any point in time our exact cash flow, cash availability and payment data. Everything is visible across the department."

— Paul McCloskey

EDITOR'S CHOICE AWARD

BUILDING A TEMPLATE FOR SUCCESSFUL HEALTH EXCHANGES

Connecticut proved that state exchanges could work from the get-go. Now it's taken enrollment mobile.

While the troubled debut of HealthCare.gov got most of the attention in 2013, many state-level health insurance exchanges got off to a rocky start as well. Access Health CT, however, was an exception.

Connecticut's exhange went live that September – ahead of the Affordable Care Act's deadline and 5 percent below budget. And while millions of uninsured Americans struggled with exchanges that were slow, error-ridden or simply down, Connecticut residents enrolled by the tens of thousands – ultimately reducing the state's uninsured rate by 50 percent.

In the two years since, Access Health CT has continued to build on that initial success – streamlining the process for consumers and steadily adding new functionality. The goal was not simply to maintain a functional government-run exchange, but to deliver a customer experience that exceeds the citizen expectations shaped by private-sector apps and online services.

Access Health CT embraced mobile early, developing a robust API and an extensible mobile platform that integrates closely with its back-end systems. Connecticut consumers can not only access plan details from their mobile devices, but also screen themselves for benefit eligibility and even upload the documents needed to verify eligibility.

And when the third open enrollment period commences on Nov. 1, Connecticut residents will be able to act on that research and actually enroll for insurance coverage through the Access Health CT mobile app. User tests suggest that "mobile enroll" can reduce the average application time to as little as 10 minutes.

Access Health CT is not the only successful state exhange, of course, and the federal government's HealthCare.gov has made great strides since its troubled debut. What truly sets the Connecticut effort apart – and what earned it the Editor's Choice Award – was the way the exchange was built with reuse and revision in mind.

The mobile platform in particular was developed from the ground up as a SaaS offering, readily reconfigurable to be deployed for other state-based exchanges or even private-sector insurance sites. It can be configured to provide a mobile platform and digital services to other state-based exchanges, private exchanges, state health and human services organizations and insurance carriers.

Such shareability doesn't mean much if the underlying system can't deliver, but Access Health CT has addressed back-end needs as well as citizen expectations. The security and privacy controls, data standards and flexible reporting functions all help to ensure the system can help Connecticut deliver on this critical mission. And other governments can do more than simply watch and learn.

– Troy K. Schneider

HONORABLE MENTIONS

These five projects were also selected by the GCN awards judges as deserving recognition for their performance and originality.

EN ROUTE AUTOMATION MODERNIZATION

Federal Aviation Administration

In March, the Federal Aviation Administration rolled out En Route Automation Modernization, a next-generation air traffic control system that uses satellite and digital technologies to pinpoint the locations of hundreds of aircraft en route to destinations across the nation's airspace.

By replacing 1960s-era, ground-based radar technologies, ERAM enables blanket coverage of air traffic and weather conditions that help make air travel more convenient and predictable while reducing fuel usage and time spent on the ground.

The centerpiece of the system is a 4-dimensional trajectory software model – 3D plus time – that helps predict the path and manage the route of every aircraft from takeoff to landing. The system also uses the data to improve controllers' situational awareness and warns pilots of aircraft unexpectedly entering their airspace.

Altogether, the FAA said the tools will "dramatically improve the nation's airspace."

MAIN COMMUNICATIONS FACILITY FOR SOUTHWEST ASIA THEATER

Department of the Army

In the early days of the Army's engagement in Southwest Asia, an aging data environment, out-of-date system maintenance and insufficient data storage threatened the U.S. military's mission. Therefore, the Army's Program Executive Office for Enterprise Information Systems opened a $50 million, state-of-the-art communications hub at Camp Arifjan in Kuwait in 2014.

An Army team and contractor LGS Innovations built the Main Communications Facility for Southwest Asia Theater from scratch. They consolidated older data centers and provided secure command, control, communications and computer network capabilities across 20 countries in the Southwest Asia theater.

The facility now connects thousands of warfighters and offers increased performance, data security and enhanced C4 services. When the program reaches capacity between 2016 and 2020, it will form the basis for establishing the Joint Information Environment, which is designed to allow all Defense Department personnel to use the network from any device, anywhere in the world.

NEXT GENERATION NETWORK AND SECURITY PROGRAM

Fairfax County, Va.

When Fairfax County, Va., officials wanted to build a new secure public network, they sought to deploy technologies that could pave the way for future plans and programs.

As a result, the county's Institutional Network is built as a 10 gigabits/sec optical Ethernet with a redundant backbone that runs on Dense Wavelength Division Multiplexing technology. The cutting-edge network is designed to secure future traffic between county business units and applications and enable a secure separation of future public safety traffic, voice over IP, public Internet access and surveillance video.

In addition, multiple high-bandwidth Internet service provider connections have provided optimal traffic routing so that the county can offer secure e-government applications and better remote services for teleworkers. All in all, the county has provided a flexible, secure platform for current and future generations of county employees and residents.

PURCHASE CARD ANALYTICS PROGRAM

U.S. Citizenship and Immigration Services

Last year, the U.S. Citizenship and Immigration Services' Office of Security and Integrity teamed with the chief financial officer's staff to detect and deter potential fraud in the agency's purchase card program.

A team of OSI analysts created a process to identify transactions that showed a reasonable potential for abuse of the program. The team used advanced software to routinize analytics, validate data and archive findings for later analysis.

The process is now a model for building oversight tools for other purchase-related programs, including fleet and travel cards.

Within six months of beginning the project, OSI delivered the first report on anomalous purchases for closer review. Today, irregular transactions are provided to the CFO's office on a monthly basis for review and possible action.

OPEN GOVERNMENT AND WEB MODERNIZATION

New Jersey Department of Health

With a nearly 20-year-old web presence, New Jersey's Department of Health resolved to rejuvenate its online operations, a project that affected more than 170 web functions and involved creating a new design that more closely synced with how users interact with the agency.

Web developers focused on enabling users to maneuver more rapidly to the information they needed. The system for paying fees online was redesigned for simplicity and speed, and sources for information about public health, health systems and health quality were overhauled and expanded.

The department generated more than $12 million in revenue annually by moving from paper processes to electronic applications. It also cut costs related to aging content. The old site had more than 5,000 web pages, and in one program, the department eliminated 66 percent of the content, cutting the number of web pages from 83 to 29.

The vetting of trusted users should never end

Managing access to agency systems involves a continuous process of authentication based on context and value

BY ROBERT GRIFFIN

Risk-based, or adaptive, authentication grew out of the recognition that single- and multiple-factor authentication methods were based on the erroneous assumption that identity could be absolutely confirmed and, once confirmed, used as a basis of trust for all subsequent access decisions for the authenticated identity.

It is clear that even the most robust multifactor authentication mechanisms do not give that level of assurance, though one-time passwords are still the most effective method for approaching that goal.

Adaptive approaches were developed to address that inherent limitation by viewing authentication as establishing a certain level of trust that could be factored into subsequent decisions regarding access. Those decisions also considered context (such as deviations from typical patterns of access for that user or all users) and the value of the resource being requested. Those factors could result in a response tailored to the authentication, such as requiring additional (step-up) authentication or limiting the extent to which the resource was provided (for example, permitting only partial access to particular information even if full access had been requested).

Adaptive authentication technologies are well established in government in response to regulatory and application requirements. For example, the passage of the Telework Enhancement Act of 2010 resulted in the proliferation of products that provide risk-based authentication as a way to meet the new regulatory requirements for multifactor authentication for end-user remote access. Some of the products had already been available and were provided by agencies to their users. But the law accelerated the availability and adoption of adaptive authentication.

Adaptive authentication has clearly emerged as an effective technology and as a paradigm that reflects the risk-based world in which we live.

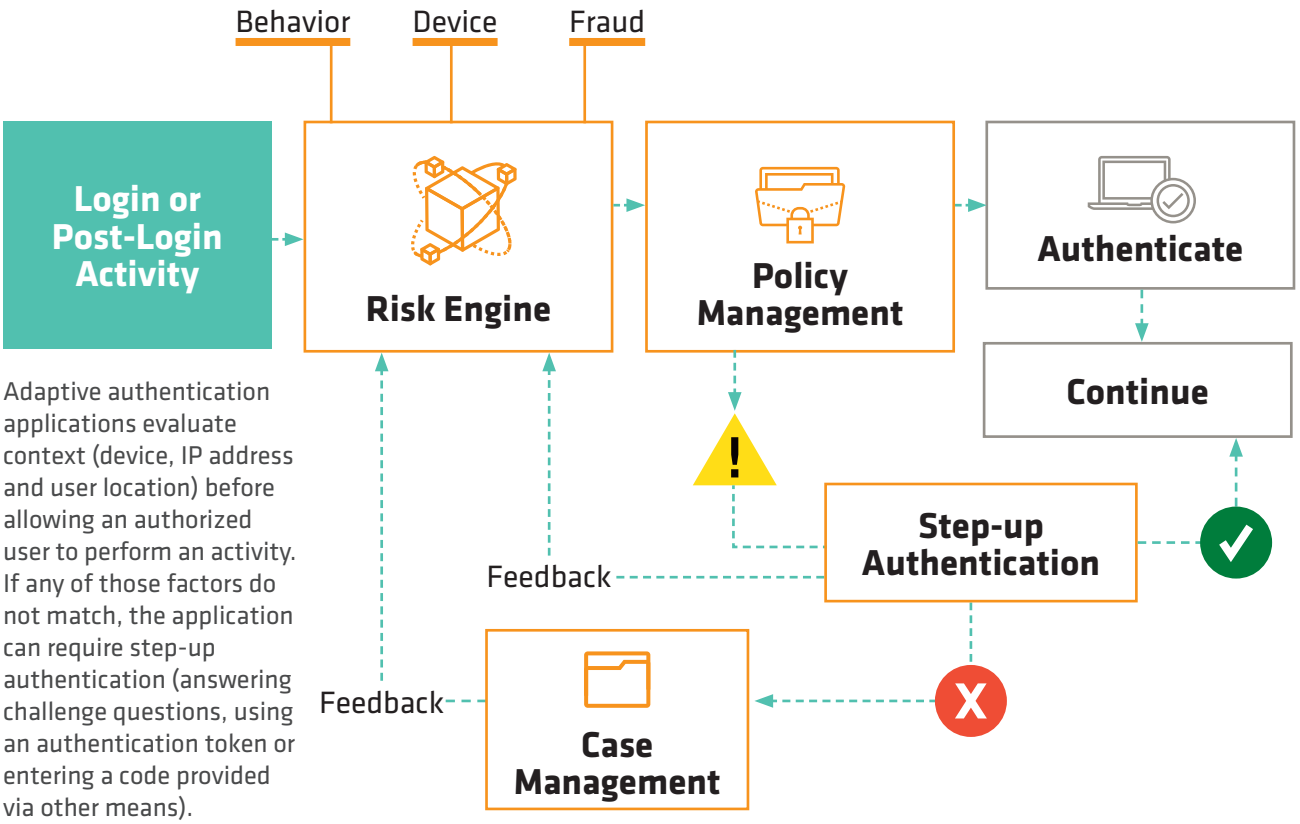
For example, suppose an end user has logged into an online government service with a valid username and password. Before allowing that person to perform any activity, the application can evaluate context related to the user, such as whether the device, IP address and user location are the same as in previous logins. If any of those factors do not match (indicating that this might be a fraudulent login using a compromised username and password), the application can require step-up authentication such as answering challenge questions, using an authentication token or entering a code provided via email, text or telephone.

That kind of authentication is widely used for end-user access to online government services and has been successful in reducing the incidence of fraud. The range of information used as context for the risk decision continues to increase and has expanded from limited geolocation, IP address and device identifier information to behavior profiles (what this user has done in the past or what all users generally do), device profiling (configuration and low-level hardware characteristics), biometrics (fingerprints, gestures, facial recognition and voice recognition) and various forms of shared intelligence (vulnerability information, threat intelligence and phishing attack patterns).

The term "infinite factor" is sometimes used to reflect this ongoing expansion of the context used in making risk decisions. The use of this broad range of factors, especially compared to only using challenge questions or codes provided via text or email, has significantly improved the effectiveness of authentication.

An important development is the recognition that authentication is part of a

A risk-based approach to ongoing authentication



Adaptive authentication applications evaluate context (device, IP address and user location) before allowing an authorized user to perform an activity. If any of those factors do not match, the application can require step-up authentication (answering challenge questions, using an authentication token or entering a code provided via other means).

continuous process of managing access to resources. In other words, instead of applying risk evaluation and response techniques only during the authentication process, they are applied as part of the process of determining whether to allow any request for a resource, transaction or interaction. The importance of a continuous process of managing access is one of the lessons from the massive Office of Personnel Management data breach.

Consider, for example, an agency user who has been authenticated for access to an online government system, perhaps one that manages personal information for applicants to an agency service. Before the first screen showing the list of applicants is displayed, the risk of a compromised credential is evaluated in order to determine whether that data should be shared. If the list is shared and the user selects one of those applicants, risk might be evaluated again (factoring in the greater impact of exposure of the details for an individual before displaying the information). In that case, additional authentication might be required, such as requiring the user to answer challenge questions.

That model of continuous adaptive authentication and access control is extremely valuable across agency resources, where the risk for a given interaction can vary significantly depending on the value of the information, the impact of fraudulent access to that information and the level of difficulty of remediation.

Adaptive authentication has clearly emerged as an effective technology and as a paradigm that reflects the risk-based world in which we live. Phishing and other kinds of social engineering attacks were the most common attacks on enterprises in 2014, according to joint research published in April by ISACA and RSA on the current state of cybersecurity. Nearly 70 percent of respondents cited phishing as having resulted in exploits in the enterprise, while 50 percent cited other social engineering attacks, including watering-hole attacks, SMS phishing and voice phishing.

In a world in which end users are being so aggressively targeted by fraudsters, adaptive authentication with its risk-based approach is an essential technology for authentication and access control. •

— Robert Griffin is chief security architect at RSA.

ADVERTISER INDEX

This index is provided as an additional service. The publisher does not assume any liability for errors or omissions.

MEDIA CONSULTANTS

Mary Martin
(703) 222-2977
mmartin@1105media.com

Matt Lally
(973) 600-2749
mlally@1105media.com

Bill Cooper
(650) 961-1760
bcooper@1105media.com

Ted Chase
(703) 876-5019
tchase@1105media.com

PRODUCTION COORDINATOR

Lee Alexander
(818) 814-5275
lalexander@1105media.com

© Copyright 2015 by 1105 Media, Inc., 9201 Oakdale Ave., Suite 101, Chatsworth, CA 91311. All rights reserved. Reproduction of material appearing in Government Computer News is forbidden without written permission. 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

Statement of Ownership, Management and Circulation

1. Publication Title: *GCN*
2. Publication Number: 0738-4300
3. Filing Date: 3. 09/30/15
4. Frequency of Issue: Monthly except Dec
5. Number of Issues Published Annually: 11
6. Annual Subscription Price: US $125, International $165
7. Complete Mailing Address of Known Office of Publication:
   9201 Oakdale Ave., Ste. 101, Chatsworth, CA 91311
8. Complete Mailing Address of the Headquarters of General Business Offices of the Publisher: Same as above.
9. Full Name and Complete Mailing Address of Publisher, Editor, and Managing Editor:
   Henry Allain, COO and Public Sector Media Grp. President, 4 Venture, Suite 150, Irvine, CA 92618
   Troy K. Schneider, Editor-In-Chief, 8609 Westwood Center Dr., Ste. 500, Vienna, VA 22182-2215
   Terri J. Huck, Managing Editor, 8609 Westwood Center Dr., Ste. 500, Vienna, VA 22182-2215
10. Owner(s): 1105 Media, Inc, dba: 101communications LLC
    9201 Oakdale Ave, Ste. 101, Chatsworth, CA 91311. Listing of shareholders in 1105 Media, Inc.
11. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding
    1 Percent or more of the Total Amount of Bonds, Mortgages or Other Securities:
    Nautic Partners V, L.P., 50 Kennedy Plaza, 12th Flr., Providence, RI 02903
    Kennedy Plaza Partners III, LLC, 50 Kennedy Plaza, 12th Flr., Providence, RI 02903
    Alta Communications IX, L.P., 1000 Winter Street, South Entrance, Suite 3500, Waltham, MA 02451
    Alta Communications IX, B-L.P., 1000 Winter Street, South Entrance, Suite 3500, Waltham, MA 02451
    Alta Communications IX, Associates LLC, 1000 Winter St., South Entrance, Ste. 3500, Waltham, MA 02451
12. The tax status has not changed during the preceding 12 months.
13. Publication Title: *GCN*
14. Issue date for Circulation Data Below: September 2015
15. Extent & Nature of Circulation:

		Average No. Copies Each Month During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
a.	Total Number of Copies (Net Press Run)	47,241	47,266
b.	Legitimate Paid/and or Requested Distribution		
	1. Outside County Paid/Requested Mail Subscriptions Stated on PS Form 3541	37,526	37,014
	2. In-County Paid/Requested Mail Subscriptions Stated on PS Form 3541	0	0
	3. Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid or Requested Distribution Outside USPS®	4,389	4,752
	4. Requested Copies Distributed by Other Mail Classes Through the USPS	0	0
c.	Total Paid and/or Requested Circulation	41,915	41,766
d.	Nonrequested Distribution		
	1. Outside County Nonrequested Copies Stated on PS Form 3541	4,423	4,550
	2. In-County Nonrequested Copies Distribution Stated on PS Form 3541	0	0
	3. Nonrequested Copies Distribution Through the USPS by Other Classes of Mail	0	0
	4. Nonrequested Copies Distributed Outside the Mail	469	589
e.	Total Nonrequested Distribution	4,892	5,139
f.	Total Distribution	46,807	46,905
g	Copies not Distributed	434	361
h.	Total	47,241	47,266
i.	Percent paid and/or Requested Circulation	89.55%	89.04%

16. Electronic Copy Circulation:
    a. Requested and Paid Electronic Copies
    b. Total Requested and Paid Print Copies (Line 15c) + Requested/Paid Electronic Copies
    c. Total Requested Copy Distribution (Line15f) + Requested/Paid Electronic Copies (Line 16a)
    d. Percent Paid and/or Requested Circulation (Both print & Electronic Copies) (16b divided by 16c x 100)
    ☑ **I certify that 50% of all my distributed copies (electronic and paid print) are legitimate request or paid copies.**
17. Publication of Statement of Ownership for a Requester Publication is required and will be printed in the October 2015 issue of this publication.
18. I certify that all information furnished on this form is true and complete:
    David Seymour, Director, Print and Online Production

WISHLIST

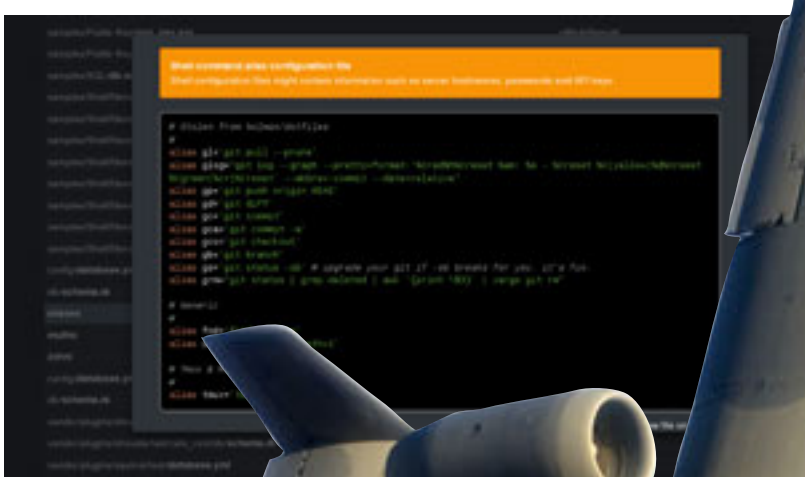
Tech we hope to see in the public sector

Pixel C

Microsoft's Surface Pro and Apple's iPad already have carved out niches in the public sector; Google's new keyboard-packing tablet looks promising for enterprise users as well. The 10.2-inch device runs the Android Marshmallow operating system – not Chrome OS like other Pixel-branded machines – and seems designed for laptop-like multi-window operation. Dual cameras and four microphones offer other messaging options for users who want to leave the detachable keyboard behind.

GitRob

GitHub is home to an ever-increasing array of government agencies' code repositories, but developers sometimes post things that shouldn't be shared – everything from encryption keys to personnel data. GitRob is an open-source, command-line tool (available on GitHub, naturally) that allows an organization to scan its repositories for files that are likely to contain sensitive information and then present the collected data for an administrator's analysis.



Android Tactical Assault Kit

An actual A-10 Thunderbolt II would be of limited (though awesome!) utility to most corners of government, but the prototype targeting system that DARPA recently tested in an A-10 could revolutionize close air support for troops in battle. Automated algorithms recommend travel routes to the target and which weapon to use on arrival, helping the pilot and ground troops execute an airstrike with as little as three clicks on a tablet.

What new technologies do you think GCN readers should learn more about? Tell us on Twitter: **@GCNtech #GCNwishlist**.

ACQUIRE

Acquisition & Management Show

Coming June 2016!

2016

JUNE 8-9

WALTER E. WASHINGTON CONVENTION CENTER

WASHINGTON, DC

Exhibit space is now available!

Contact Stacy Money for pricing & details

smoney@1105media.com 415.444.6933

ACQUIREshow.com

Tracks Include

- ACQUIRE Office Management
- ACQUIRE Professional Services
- ACQUIRE Information Technology
  - FEDERAL IT ACQUISITION SUMMIT
- ACQUIRE Acquisition Management
- ACQUIRE Project Management
- ACQUIRE Industry Days
  - Washington Technology
- ACQUIRE Happy Fed
  - Federal SOUP

CONGRATS!

The GCN Editorial Team would like to congratulate all of the 2015 Winners & Honorable Mentions.

Well done!

GCN.COM/GALA