GCN

TECHNOLOGY, TOOLS AND TACTICS FOR PUBLIC SECTOR IT
JULY 2015 • VOLUME 34, ISSUE 7

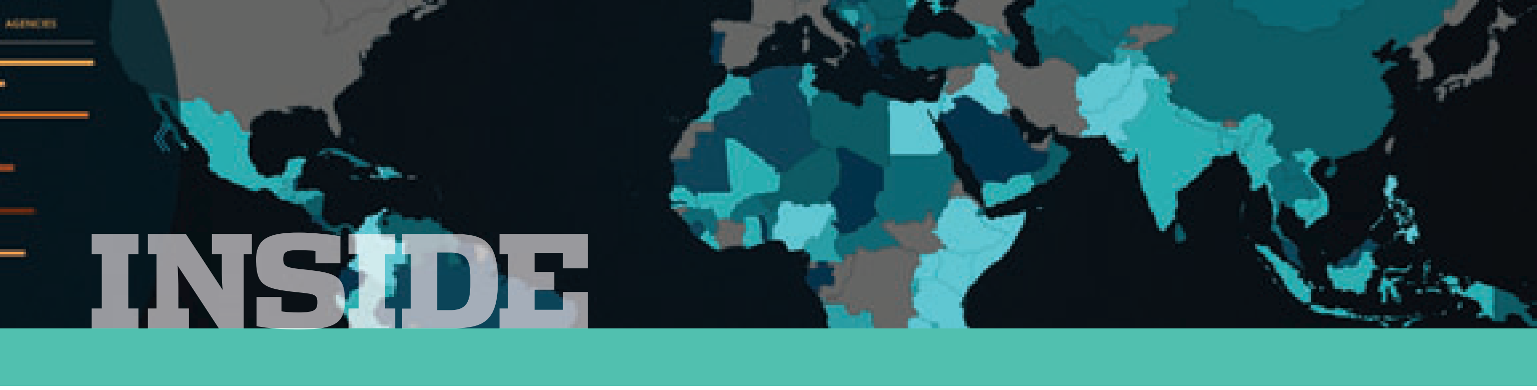
FEATURE:
Mission-driven data visualization
Page 18

CASE STUDY:
At odds over data breach disclosures
Page 31

SCANNING FOR CLUES

The fight against health care fraud

PAGE 24



INSIDE

FEATURES

CASE STUDIES

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.

BRIEFING

COMMENTARY

WISH LIST

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
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**
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 **John Bicknell**
Managing Editor **Terri J. Huck**
Senior Staff Writer **Adam Mazmanian**
Staff Writers **Sean Lyngaas, Zach Noble, Mark Rockwell**
Editorial Fellows **Eli Gorski, 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
Editor-in-Chief **Christopher Piehler**

Campus Technology
Executive Editor **Rhea Kelly**

1105 MEDIA INC

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

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™

NIST explores new tech for tattoo recognition

BY DEREK MAJOR

Although tattoos are often an outward expression of a person's character, to the participants of a challenge sponsored by the National Institute of Standards and Technology, body art can quite literally help confirm a person's identity.

Forensic analysis of tattoos is important to law enforcement activities such as solving crimes, identifying victims and gathering intelligence on gangs, according to NIST. But tattoo recognition is difficult because the composition and patterns of the images vary widely. The current method of cataloging tattoos relies on a keyword-based process, which can be complex and subjective depending on the design of a tattoo and the description of the examiner.

The goal of the Tattoo Recognition Technology–Challenge (Tatt-C) is to advance research into automated image-based tattoo-recognition technology that focuses on retrieving and matching tattoos from still images captured by law enforcement agencies.

In a preliminary trial of existing tattoo-recognition software, the FBI's Biometric Center of Excellence (BCOE) provided thousands of images to NIST, which then asked the six organizations that participated in the challenge to assess the capability of image-based tattoo-recognition algorithms in the following situations:

- Visually similar or related tattoos on different subjects.
- Different images of the same tattoo on the same subject over time.
- A small region of interest contained in a larger image.
- Visually similar or related tattoos in different types of images such as sketches, scanned print, computer graphics or natural images.
- An image that might or might not contain a tattoo.

"The state-of-the-art algorithms fared quite well in detecting tattoos, finding different instances of the same tattoo from the same subject over time and finding a small part of a tattoo within a larger tattoo," said NIST computer scientist Mei Ngan, who organized the challenge.

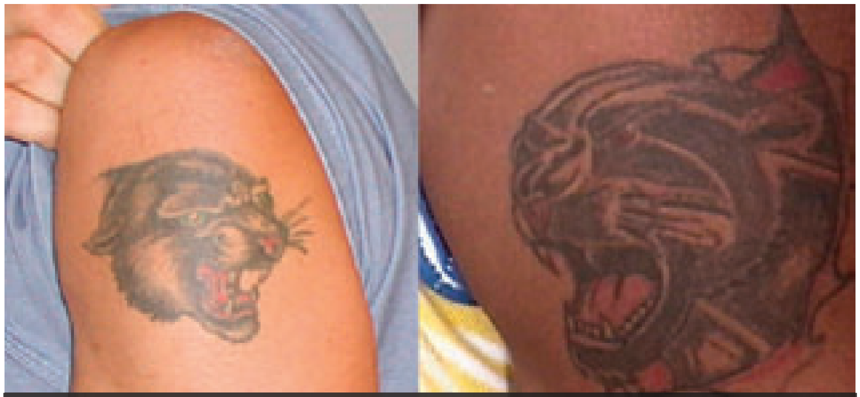
But she added that two areas could use further research: detecting visually similar tattoos on different people and recognizing a tattoo image from a sketch or sources other than a photo.

"Improving the quality of tattoo images during collection is another area that may also improve recognition accuracy," Ngan said.

In addition to discussing the trial's initial findings, Tatt-C participants covered the use of image-based tattoo matching in operations, identified ways to improve tattoo recognition and discussed the next steps NIST might take in that area.

The Tatt-C participants were Compass Technical Consulting; the Fraunhofer Institute of Optronics, System Technologies and Image Exploitation; the French Alternative Energies and Atomic Energy Commission; MITRE; MorphoTrak; and Purdue University.

Government researchers have been working on automated tattoo-recognition technology since 2012, when the BCOE issued a request for information on the best way to build a tattoo database. •



The National Institute of Standards and Technology is refining a tattoo-recognition system that could, among other challenges, identify a visually similar tattoo on two different people.

NIST.GOV

FEMA launches visualization tool for disaster data

BY AMANDA ZIADEH

Thanks to a new tool from the Federal Emergency Management Agency, citizens and local emergency managers can get a better understanding of the relative risk and impact of a variety of disasters.

The interactive tool maps historical data to help communities plan for disasters and gain insight into how assistance funds are allocated. FEMA released the raw historical data and made it available through interactive and readable maps as part of the OpenFEMA initiative.

Users can view disaster declarations by hazard type, location, year (back to 1953) and the financial support provided through an easily viewable and clickable interface, while maintaining access to raw datasets for research and analysis.

Summaries of FEMA support for fire, preparedness, mitigation, individual assistance and public assistance grants are available as well.

The tool offers a step-by-step search process and displays immediate results that include preparation tips, which is a helpful resource during the current hurricane season. Those in affected areas can research the history of hurricanes in their communities and learn what they can do to prepare effectively based on historical data and FEMA's experience.

"Providing data in its raw format and also building visualization tools allow people to look at their past history, look at what kind of hazards they are vulnerable to, and look at the frequency of disaster declarations and the impacts," FEMA Administrator Craig Fugate said in a blog post.

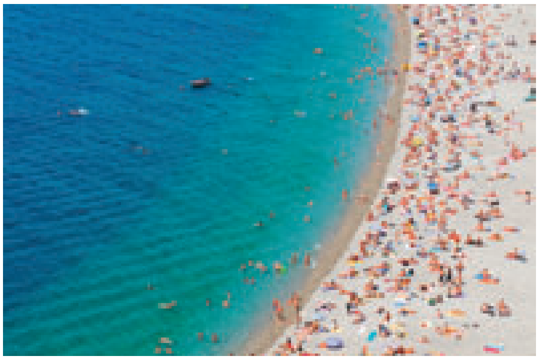
Visualizing the hot spots where disasters and recovery money overlap makes it easier to understand disaster impacts and helps people ask the right questions when it comes to why certain communities have historically received the assistance they have from state and local governments, Fugate added.

The data can also help governments more accurately anticipate the financial impact of a disaster. If a community shares characteristics with another that has experienced a major disaster, local emergency management will have a better idea of how to plan and allocate resources for future potential disasters.

FEMA's motivation is simple and powerful. "By providing this information in a way that is visual and easy to understand, people will be moved to action to prepare their families and communities," said Tim Manning, FEMA's deputy administrator of protection and national preparedness. •

Shark-spotting drone patrols California beach

BY SUSAN MILLER



LUCIAN MILASAN / SHUTTERSTOCK.COM

In Seal Beach, Calif., the Marine Safety Department's new $1,400 drone is working overtime protecting beachgoers this summer.

According to Patch.com, the city's drone was originally purchased to photograph the annual Junior Lifeguard Program, but when video showed 10 to 12 great white sharks close to shore, lifeguards realized the drone's potential.

Previously, lifeguards confirmed shark warnings by jet skiing to the reported location, which took enough time for the sharks to move on.

With the drone, lifeguards can spot sharks from 100 feet up and zoom down for a closer look. Additionally, the drone images allow lifeguards to assess the size of the sharks; the beach closes only when large or aggressive sharks are sighted.

In addition to shark spotting, lifeguards say they can see the shape and length of riptides, which are also hard to see from land. •

Veterans to get virtual rehab

BY MARK POMERLEAU

Researchers have developed a virtual rehabilitation system that will enable therapists to treat disabled veterans without being in the same room.

According to officials at the University of Texas at Dallas, the multimedia system uses 3D cameras and off-the-shelf devices such as Microsoft Kinect to create avatars of the therapist and the patient, then puts them together in a virtual space where they can interact.

Tracking people's movements generates large amounts of data, but for telerehabilitation to be successful, there cannot be any latency between action and reaction. Therefore, the researchers created algorithms and software that enable the data to be transmitted in real time from patient to therapist via the Internet.

"To transfer all of this data requires a bandwidth greater than 100 megabits per second, which we currently can't do over the Internet," said Karthik Venkataraman, who is working on the project at UT Dallas while pursuing a Ph.D. in computer science.

> "To transfer all of this data requires a bandwidth greater than 100 megabits per second, which we currently can't do over the Internet."
>
> – KARTHIK VENKATARAMAN, UT DALLAS

US Ignite and the Global Environment for Network Innovations provided the necessary bandwidth, he said.

At the Beyond Today's Internet summit in March, the team conducted a physical therapy session in which a patient and a physical therapist practiced sawing a log, a task that mimics the movements used to help stroke patients recover. Both participants can feel the resistance of the log and the guiding movements of their partner, just as they would at an in-person therapy session.

The researchers said this is just one example of what can be achieved with high-speed, low-latency networking. The team is working on extending the telerehabilitation system so one physical therapist or physician could work with multiple patients at the same time.

The new system will be deployed in field trials this summer and fall at the Dallas Veterans Affairs Medical Center. •

5 trends that will shape government IT

BY AMANDA ZIADEH

To help government managers plan their IT strategies, Gartner has released a list of this year's 10 most important technology trends in digital government. Here are the top five:

- **Digital workplace.** In an information-driven workplace, most employees will be digitally literate — from those on the frontlines to executives. The resulting work environment will be more social, mobile, open and democratic.
- **Multichannel citizen engagement.** Adopting a multichannel strategy for interactions will give citizens and other stakeholders a seamless, transparent and coherent experience. Many states are already revamping their websites and offering mobile services, information and alerts on multiple platforms. Gartner recommended that agencies redesign their service models by combining their existing marketing tools with innovative approaches.
- **Open data.** Governments have already begun opening public data and offering datasets and Web-based applications, but growth has yet to reach maximum utility. As governments demonstrate the value of open data, major funding obstacles will recede, and as a result, more than 30 percent of digital government projects will treat all data as open by 2018.
- **Electronic IDs.** People will increasingly access public services through a trusted domain accessible via any device — a development that will require trust between government and commercial vendors to ensure that security, privacy and data confidentiality requirements are maintained.
- **Edge analytics.** As mobile services with real-time interaction and contextual capabilities become more pervasive, analytics will evolve from a separate business function into an integrated aspect of system operations and user experiences.

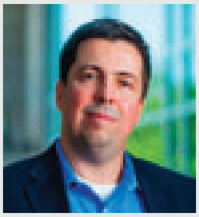
"These strategic technology trends have substantial disruptive potential that is just beginning to materialize and will reach an inflection point within the next three to five years," Gartner Research Director Rick Howard said. "Public-sector CIOs can capitalize on the value of these trends by first determining how they will impact government program operations or service delivery models, and then by building the organizational capabilities and capacity needed to support them."

The full list is available at is.gd/GCN_toptrends. •

EDITOR'S NOTE

Show and tell

“Show, don’t tell.” It’s familiar advice for anyone who went to journalism school or who regularly writes for an audience. Descriptions can only do so much; what readers really need are concrete examples that can illustrate the issue.



That advice increasingly applies to agencies’ use of data as well. Pivot tables and spreadsheets are valuable tools, but too many Americans, including some at senior levels of government, are effectively innumerate. Even for those who have the skills to understand the data, the sheer scope of it means the old approaches are no longer enough.

Fortunately, there are new approaches aplenty. Governments at all levels are now painting pictures in pursuit of countless critical missions. In the pages that follow, there are examples of visualizations used to boost situational awareness for border patrols, increase the transparency of international development, improve federal hiring habits and help keep citizens safe in their neighborhoods.

We take a particularly deep dive into the analytics being used to spot Medicare fraud – a $60 billion-a-year problem that’s hidden away in data that expands by 4.5 million claims every day. Without advanced algorithms, automated flags and ways to picture the broader patterns in the data, such policing would be all but impossible.

There are many more examples worth sharing, some of which are showcased now on GCN.com, while others will be covered in the weeks and months to come. But all of them make one thing clear: Governments are putting more data to work. And that makes for a pretty picture.

– Troy K. Schneider
tschneider@gcn.com
@troyschneider

A decoder ring for GSA per diems

BY GCN STAFF

Managing travel expenses for government employees and contractors can be complicated, given that per diem rates vary by city and change every year.

Certify, a provider of cloud-based travel and expense management software, has added the General Services Administration's per diem services to its systems in an effort to simplify travel and expense reporting for federal employees and contractors.

With Certify's new capabilities, administrators can configure travel and expense reporting requirements using the federal standard allowances established each year. Once configured, Certify calculates allowable reimbursable amounts based on the date of the expense and the destination. Other variables that affect reimbursable rates — such as meal combinations, incidental expenses, reimbursable type and travel days — are also included.

All calculations are compared to the most current GSA-supplied data to ensure accuracy and streamline the approval process.

The new capabilities are included in the Certify Enterprise Plan and are part of the integrated Certify system, which also provides advanced reporting tools for greater visibility into travel and expense management. Administrators can easily see which employees are the most active travelers, which destinations they travel to most frequently, how much individual departments spend on travel and more.

"Navigating the requirements for GSA per diems and reimbursement is anything but simple," Certify President Robert Neveu said. "Now with available GSA functionality, Certify makes travel and expense management easy for even the most complicated transactions and policies." •

READ ME

What: "Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s," a report by the New America Foundation's Open Technology Institute.

Why: The current friction over the public's right to use mobile products with strong encryption is reminiscent of a conflict in the 1990s, dubbed the Crypto Wars.

Tensions came to a head with the Clinton administration's introduction of the Clipper Chip in 1993. The microchip provided strong cryptographic tools for consumer phones without sacrificing access by the law enforcement and intelligence communities. However, the public outcry over the government's storage of each chip's encryption key, known as "key escrow," and a flaw in the system ended use of the chip in 1994.

Takeaway: Since the Crypto Wars ended, an encryption-enabled ecosystem has become essential to the overall security of the modern network. But in the wake of Edward Snowden's disclosures about government surveillance, technology companies have begun to adopt even greater encryption, and the government has revived many of the arguments it used in the 1990s to support key escrow. It seems "to have forgotten the lessons of the past," the authors write. "We may once again be on the verge of another war: a Crypto War 2.0. But it would be far wiser to maintain the peace than to begin a new and unnecessary conflict."

Full report: http://is.gd/GCN_CryptoWars

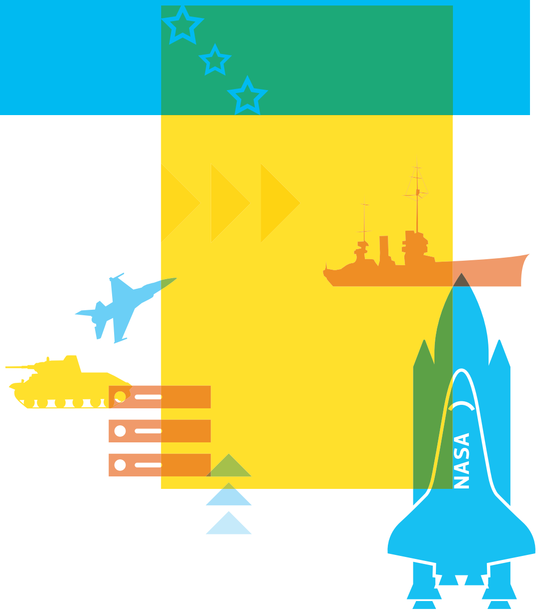
RETRO TECH

GCN was just 10 years old when the IBM ThinkPad debuted in 1992. Now Lenovo, which bought the brand in 2005, is mulling a back-to-the-future design for its business laptop workhorse. There are limits, however: Lenovo's David Hill noted that few users likely miss the "original thickness of 56 mm," and he named the 256-color 700c as his preference, rather than the monochrome 300 pictured here.

OLDCOMPUTERS.NET

SEWP V IS HERE.

All the benefits.
All in one place.



CDWG.com/sewpv
800.808.4239
Contract #NNG15SC04B

CDW·G® PEOPLE WHO GET IT™

CONTRACT PURCHASING WITH CDW·G IS SIMPLE, QUICK and PAINLESS

About SEWP V and CDW·G

The Solutions for Enterprise-Wide Procurement (SEWP V) from CDW·G is a contract open to all government agencies and authorized contractors, and provides a wide range of technology solutions that help your agency connect and communicate effectively.

The SEWP V from CDW·G offering includes Windows-, UNIX-, and Linux-based workstations and servers, along with peripherals, networking and storage equipment, security tools and software from the most trusted brands and manufacturers you need.

BENEFITS OF SEWP

- Purchasing is made easy for the entire federal government as well as authorized prime contractors
- Multiple vendors, numerous product categories
- Product additions are made quickly
- Minimal surcharges
- Orders $0 to $2,222,222 – 0.39% fee

CONTRACT INFORMATION

CDW·G

Carroll Genovese
Program Manager, SEWP V
Phone: 703.621.8227
Email: carrgen@cdwg.com

Kathy Marcheselli
Deputy Program Manager, SEWP
Phone: 703.621.8208
Email: kmarcheselli@cdwg.com

SEWP BOWL
Phone: 301.286.1478
Email: Help@sewp.nasa.gov
Web: www.sewp.nasa.gov

FOR VETERANS AFFAIRS
Agency-specific requirements go to:
http://www.sewp.nasa.gov/VA/info.html

FOR DEPARTMENT OF DEFENSE
Agency- specific requirements, go to:
http://www.sewp.nasa.gov/dod/info.html

SMARTPAY ORDERS

CDW·G accepts SmartPay card payments for SEWP V orders. There is no SEWP contractual limit on purchase card orders. Purchase card limits are based on your agency's limit.

PURCHASE ORDERS

All orders except credit card orders that are phoned in or placed on a website using a shopping site must be sent directly to the NASA SEWP BOWL by the purchasing agency's procurement office. In the typical process, the end user will generate a purchase request and will send any necessary funding information to their procurement office, which results in the issuance of a delivery order number (DO).

The NASA SEWP BOWL does not issue DOs – these must be issued through the issuing agency's procurement office. The NASA SEWP BOWL processes issued orders and forwards them to CDW·G. Under normal circumstances, the time between the receipt of a DO at the NASA SEWP BOWL and delivery of the order to CDW·G for fulfillment is less than one business day.

Every order must include the following:

- Delivery Order number
- Quote from CDW·G verifying the viability of the order

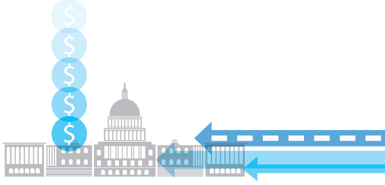
Mail orders and completed forms to:
SEWP Program Office (BOWL)
10210 Greenbelt Road
Suite #270
Lanham, MD 20706

Fax orders and completed forms to:
301.286.0317

Email PDF or image files to:
sewporders@sewp.nasa.gov

If modifications are made to any order, they must also route through the SEWP BOWL.

I.T. SOLUTIONS FROM SEWP V and CDW•G MAKE CONTRACT PURCHASING EASY.



Federal governments were stretched thin even before BYOD initiatives and advanced cybersecurity threats came into play. So how can your organization make the most of your limited IT staff, time and budget? Easy. Turn to CDW•G.

HP Smart Buy

HP EliteBook 850

Proven security, performance and management features

CALL FOR PRICING

- 4th generation Intel® Core™ i7-4600U processor (2.10GHz)
- Intel® Dual Band Wireless-N 7260AN
- Memory: 8GB/180GB SSD
- 15.6" HD SVA display with camera

[1] HP Smart Buy savings reflected in advertised price; savings may vary based on channel and/or direct standard pricing; available as open market purchases only; call your CDW•G account manager for details

Adobe® Creative Cloud® for teams

Re-revolutionize your workflow

Per User for a 12-month subscription; Multiple platforms

CALL FOR PRICING

Once you get your team on Adobe® Creative Cloud®, you'll never look back. The industry-leading creative apps and services are constantly updated. Collaboration is easier than ever, on any device. And managing licenses basically takes care of itself.

APC® Smart-UPS® SMT1500RM2U

2U rack-mountable UPS supporting servers, storage and networks

CALL FOR PRICING

- 1500VA, 1000W, six outlets
- Estimated runtime: up to 25.8 minutes at half-load[2]
- Automatic voltage regulation (AVR)
- $150,000 Lifetime Equipment Protection Policy

[2] Runtime may vary due to load and battery condition

Xerox® WorkCentre® 6505N

Network-ready color laser printer, copier, scanner and fax

CALL FOR PRICING

- Mfr. speed rating: up to 24 ppm, black and color
- Print resolution: up to 600x600 dpi
- Duty cycle: up to 40,000 pages per month
- Scan to e-mail, network scanning, direct scan to applications and scan to USB memory device

Samsung® S19B420BW

19" analog/digital LED display

CALL FOR PRICING

- Height-adjustable stand ensures that the screen can always be set at the optimal eye level
- Can rotate 90 degrees, allowing for more appropriate view depending on the assignment
- Slim design ensures that workspace is maximized while also delivering a sophisticated and professional look

ORDER FROM THESE LEADING BRAND-NAME MANUFACTURERS:

APC
Apple Inc.
Blue Coat Systems, Inc.
BMC Software, Inc.
Cisco Systems, Inc.
ClearCube Technology, Inc.
Corel Corp.
Data Domain, Inc.
EMC Corp.
Fortress Technologies
Hewlett-Packard
IBM
Itronix Corp.
Lenovo Group Ltd.
McAfee, Inc.
Micro Focus International Ltd.
Microsoft Corp.
Network Appliance, Inc.
Overland Storage, Inc.
Research In Motion Ltd. (RIM)
Samsung
Symantec Corp.
VMware, Inc.
Xerox Corp.

Partner with people who get it.

Call us today at 800.808.4239 or visit CDWG.com/sewpv

CDW•G® PEOPLE WHO GET IT™

WHY CDW·G?

WE CONFIGURE IT

We can help by setting up your technology purchases so they're ready to go right out of the box. From hardware and software configuration to custom imaging and asset tagging.

WE IMPLEMENT IT

We have a team of more than 500 engineers available to install and deploy your solution. So you can be sure it's done right and your staff can focus on more important things.

WE SUPPORT IT

Our assistance doesn't stop once your solution is in place. From health checks to training and ongoing support, we're here for you throughout the entire lifecycle of your solution.

WE GET IT

See all the benefits of working with CDW·G for yourself.
Give us a call and learn why many of our customers consider us an extension of their IT team.

DELIVERY ORDER INFORMATION

Delivery orders are required to contain the following information for processing. If the below information does not appear on the delivery order, the order may not be processed or processing may be delayed.

- Delivery Order number (any valid Government DO is allowed)
- Quote from a SEWP contract holder verifying the viability of the order
- SEWP Fair Opportunity Form for orders over $5 million (the form can be found on NASA's website)
- Date Delivery Order issued
- SEWP contract number
- SEWP contract holder's mailing address and phone number
- Issuing office: Agency name and mailing address
- Ship-to office: Agency name and mailing address
- Total dollar amount of order
- Contracting officer's signature
- Contracting officer's phone number
- Date Delivery Order signed
- Line items and pricing

For more information, call your dedicated CDW·G account manager at 800.808.4239 or visit us on the web at CDWG.com/sewpv

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

CYBEREYE
BY BRIAN ROBINSON

What's worse: Living with legacy systems or replacing them?

THE RECENT REVELATION of a breach at the Office of Personnel Management, which resulted in the theft of the personal information of millions of government employees, underscores a broader problem the government has with legacy systems: deciding whether it's worth spending the money to secure them.

Not that securing OPM's systems would have done much good in this case. Andy Ozment, assistant secretary for cybersecurity and communications at the Department of Homeland Security, said the systems were not directly penetrated. Instead, attackers obtained OPM users' network credentials and got to the systems and data from the inside.

OPM CIO Donna Seymour told a recent hearing of the House Oversight and Government Reform Committee that the agency was implementing database encryption, but some legacy systems were not capable of being encrypted.

She added that some of OPM's systems are more than 20 years old and written in Cobol, so they would require a full rewrite to include encryption and other security such as multifactor authentication.

It is a governmentwide problem. Many financial and administrative systems that are central to agencies' daily operations use the nearly 60-year-old Cobol. Most agency CIOs have targeted those systems for replacement, but it's not a simple rip-and-replace job because any mistake could have a severe impact on the agency's ability to fulfill its mission.

Spending on old vs. new IT

$82 billion
total federal IT spending in fiscal 2014

$59 billion
devoted to operations and maintenance

$1.41B out of $1.43B
NASA's 2014 spending on O&M

$1.44B out of $3.13B
Department of Transportation's 2014 spending on O&M

Source: Government Accountability Office

For that reason, many agencies have chosen to maintain those systems for now, but that's not cheap either. OPM said last year that maintaining its legacy systems could cost 10 percent to 15 percent more a year as people with the necessary expertise retire. And throughout government, legacy systems account for more than two-thirds of agencies' annual IT spending.

That expertise is unlikely to be replaced. Colleges aren't turning out Cobol-trained coders anymore, and with Cobol way down on the list of popular languages, that won't change. Agencies could bring in consultants to rewrite the code, but again, that's not cheap.

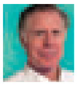
Nevertheless, Cobol is not likely to disappear anytime soon. Because of its ubiquity and utility, many IT officials will continue to use it until it's pried out of their cold, dead hands. Meanwhile, old mainframe companies that have recently refocused on the cloud continue to update their Cobol tools to keep pace with current IT trends.

It's not as though problems with legacy systems were the only reason for the breaches at OPM. Lawmakers also berated agency officials for their lack of attention to security governance issues that had been brought up years ago and were highlighted again last year in a report by OPM's inspector general.

But the legacy issues are real and, according to some reports, extend even to "legacy" security systems such as signature-based firewalls, intrusion-prevention systems and other widely installed devices that are not capable of stopping modern, fast, sophisticated and chameleon-like threats.

However, the situation with the federal government is probably not as bad as that of a public school district in Grand Rapids, Mich., that is still running the air conditioning and heating systems for 19 schools via a 1980s-era Commodore Amiga — the personal computer that was popular for home use — because a replacement system would reportedly cost as much as $2 million.

At least, we hope not. •



EMERGING TECH

BY PATRICK MARSHALL

Mapsense aims to tame location data streams

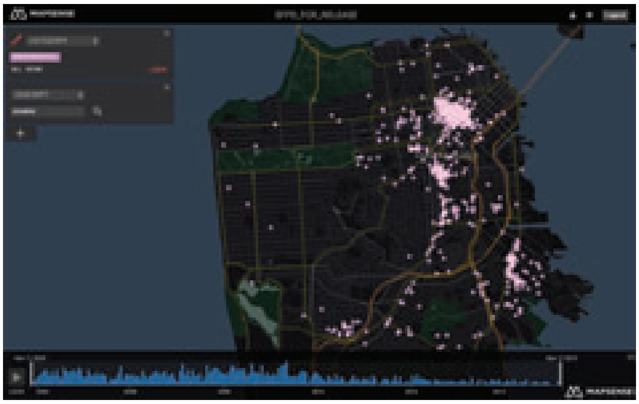
GEOSPATIAL INFORMATION SYSTEMS offer powerful analytic tools for querying and displaying static location-sensitive data on maps. What they haven't been designed to handle is the massive streams of real-time location data that are now emanating from cell phones and the myriad sensors that make up the Internet of Things.

Although some GIS vendors, including Esri, offer extensions to bring in streaming location data, Mapsense has opted to design its product from the ground up.

"One statistic I have heard is that there was more location data stored in 2014 than in all of previous history," said Erez Cohen, CEO of Mapsense. "When it comes to companies that are collecting very, very large streaming location datasets, traditional GIS tools sometimes flounder under the requirements of being able to visualize and analyze these datasets. That's the focus of our company."

Mapsense has two new products. Mapsense Enterprise is a set of data analysis and visualization tools into which companies can port their location data. Generally, the data is hosted in Mapsense's Amazon cloud storage, though on-premise storage is also an option. In either case, access to the data and to Mapsense's tools is via a Web browser.

Mapsense Developer is a set of open-source tools that allows users to create data-driven, fully interactive maps with only a few lines of code. Cartography and styling are simplified with the Mapsense CSS Machine, which lets users quickly create styles for Mapsense tiles, then grab the cascading style sheet and add it to a master style sheet.



Mapsense illustrates cocaine-related crime incidents from the San Francisco Police Department's Open Data Reported Incidents database.

MAPSENSE.CO

"What we pride ourselves on is the data scale that we support and the fact that we can stream datasets," Cohen said. "It's hard to present and visualize very large location datasets in [Esri's] ArcView. And try putting 100,000 data points even on a Google map — you'll start running into browser issues."

Cohen said his team spent significant time building technologies to visualize those large location datasets. For example, Mapsense uses a technique it calls "geographical data sampling." When ingesting, say, 100 million tweets from a customer's data stream, the program displays a subset that is representative of the larger set's spatial distribution. Further data will only be sent when requested by, for example, zooming in.

Data streams from customers can be updated in real time or at specified intervals. Mapsense will ingest the data as it comes in, then port it to the interactive map. Furthermore, although public datasets are available to all, Cohen said data provided by enterprise customers is available only to those customers.

In addition to supporting location searches on Twitter feeds, customers can also perform text searches and filter tweets by time, language or a wide array of attached metadata, such as the number of followers of a specific tweeter.

And Twitter data is far from the only location-sensitive data stream Mapsense can handle. The program has been used, for example, to analyze data from sensors attached to California condors and can poll sensors for the positions of the birds every 15 minutes.

"You can see that they move north in the hot months," Cohen said. "We can actually play back the position of each bird over time."

Apart from the ability to handle massive amounts of data quickly, Cohen said Mapsense's streamlined user interface means customers don't need to have much GIS or data-visualization training.

"Increasingly, people who are not traditional GIS analysts need to make decisions based on location data," Cohen said. "So instead of exposing traditional GIS functionality in a desktop application, we are building everything around [application programming interfaces] that can be built into products." •

Visual Studio LIVE!
EXPERT SOLUTIONS FOR .NET DEVELOPERS

vslive.com/redmond

Redmond AUGUST 10 - 14

MICROSOFT HEADQUARTERS, REDMOND, WA

REDMOND Code Trip NAVIGATE THE .NET HIGHWAY

CODE HOME

No code trip would be complete without a stop where it all began, so we're heading to the idyllic **Microsoft Headquarters** in Redmond, WA, **August 10 – 14, 2015!**

Join us as we explore hot topics like Visual Studio, JavaScript/HTML5, ASP.NET, Database and Analytics, and more in over 70+ sessions and workshops. Rub elbows with Microsoft insiders, have lunch with Blue Badges, visit the company store, and experience code at the source.

DEVELOPMENT TRACKS INCLUDE:

- Visual Studio/.NET
- Web Development
- Design
- Mobile Client
- Windows Client
- Database and Analytics
- Cloud Computing
- Microsoft Sessions

REGISTER BY JULY 8 AND SAVE $300!

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

Use promo code REDJUL1

EVENT SPONSOR Microsoft

SUPPORTED BY Visual Studio msdn magazine Visual Studio MAGAZINE

PRODUCED BY 1105 MEDIA INC

vslive.com/redmond

INDUSTRY INSIGHT

BY PATRICK D. HOWARD

What your agency can learn from the CDM rollout at DHS

IT HAS BEEN a long 18 months since the Department of Homeland Security launched the Continuous Diagnostics and Mitigation (CDM) program in September 2013. Some of the fruits of that planning might soon be coming into view.

DHS is first in line to begin implementing the program's Phase I capabilities, which include hardware and software asset management, configuration management and vulnerability assessment. With DHS as the guinea pig, this presents a unique opportunity for your agency to learn from another's experiences before undertaking your own.

As a former chief information security officer at two federal agencies, I can't overstate the value of learning from another agency's trials, lessons and successes when anticipating and preparing for your own endeavor. The CDM integration across 11 DHS organizational units will deliver a great deal of insight that could help other agencies avoid hazards and optimize technical implementation and project management to reduce information security risk.

Let's consider the areas in which your agency might benefit:

1. Technical implementation. Pilot projects are typically the most effective way to launch projects of this magnitude. DHS will fast-track the technical project at one of its organizational units, and the results will serve as an instruction set of sorts for the rest of the department — and a prototype for the agencies that will soon follow.

Details about how the actual implementation varied from the planned project estimates will be useful to both agencies and vendors.

Other benefits include know-how on integrating Phase I products, overcoming issues associated with connecting to the federal IT Dashboard and learning how best to aggregate and normalize sensor data.

Similarly, the application programming interfaces and integration packs that DHS develops could be repurposed and made available to other agencies.

2. Project management. Understandably, there's a great deal of interest in knowing what effort and resources will be needed for implementing the second task order.

Rather than relying on initial labor and timeline estimates, agencies could draw on DHS' actual experience to gain a far more realistic idea of the staff required and the project's duration.

Details about how the actual implementation varied from the planned project estimates will be useful to both agencies and vendors.

Other lessons from the implementation include how to get employees involved and the types of communications and reporting that are most effective for managing the process.

3. Risk management. Once the CDM capabilities are in place, agencies can see how DHS is using the system outputs to manage and lower risk and how it's making progress on achieving ongoing authorization goals. That insight could include the metrics and processes DHS devised for scoring and prioritizing risk.

It is a great opportunity to show how CDM moves from a compliance-based, three-year cycle of risk management to one of ongoing, real-time information security. The results will help agencies build support for CDM throughout their organizations and position the program for success.

That cycle of feedback also benefits vendors by helping them refine and improve the products and services associated with their solutions and learning how they can best train and assist agencies on their use.

Ultimately, the CDM program's success hinges on communications among DHS, other agencies and vendors. We all have a stake in this information security partnership. By sharing the right information and feedback at the right time, we can learn and adjust — and make improvements as we go forward. •

— Patrick D. Howard is former CISO at the Nuclear Regulatory Commission and the Department of Housing and Urban Development. He is currently program manager for CDM and CMaaS at Kratos SecureInfo.

BY CLAY WILSON

4 defining characteristics of cyber weapons

THE NUMBER and sophistication of cyberattack campaigns by nations will continue to increase because they minimize the need to risk military personnel or costly equipment. Unlike personnel and equipment, computer code can be instantly redeployed to any area, and because code is reusable, it offers a practically bottomless magazine for future attacks.

News reports now describe cyberattacks that can result in severe physical damage to facilities and equipment, and a tendency has arisen for the media to compare malicious cyber code to weaponry. But what is the definition of a weapon, and how can we more clearly identify when a cyberattack should be correctly labeled a "cyber weapon"?

The Tallinn Manual on the International Law Applicable to Cyber Warfare, which was developed after a series of cyberattacks against Estonia in 2007 caused extensive disruption to civilian services, defines a cyber weapon as a "cyber means of warfare" that is capable, by design or intent, of causing injury to persons or objects.

With most cyberattacks, however, the attribution and intention might be unknowable. In addition, cyberattacks often create cascade effects that were outside the original intentions of the attacker.

However, reverse-engineering and analysis of malicious code used in recent sophisticated cyberattacks have revealed four common characteristics that help provide a clearer and more useful definition of a cyber weapon:

1. A campaign that might combine multiple malicious programs for espionage, data theft or sabotage.
2. A stealth capability that enables undetected operation within the targeted system over an extended period of time.
3. An attacker with apparently intimate knowledge of the workings of the targeted system.
4. A special type of computer code that can bypass protective cybersecurity technology.

The most frequently discussed example of a state-sponsored cyber weapon attack resulting in physical damage involved a years-long campaign of stealth, data theft and sabotage targeting the nuclear program in Iran. Malicious programs were crafted to steal sensitive information, monitor internal messages and then disrupt and disable targeted industrial control systems for a specific type of centrifuge equipment in a special nuclear facility in Iran.

The entire campaign might have been operating from 2006 through 2010 before being discovered by security personnel outside Iran. Analysts agree that such a sophisticated and long-running cyber campaign showed that the designers of the malicious code had acquired an intimate knowledge of the targeted systems before launching the cyberattacks.

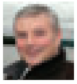
The cyber weapon campaign caused Iran's nuclear program to suffer a setback, but one that lasted only a short time. Since the attack was discovered, Iran has taken steps to increase management of its security and has revived its capabilities for enriching nuclear materials.

Future-generation cyber weapons will undoubtedly take greater advantage of opportunities that are expanding as more intimate knowledge about designs and vulnerabilities of equipment and facilities becomes available over the Internet. Future targets will likely include complex military weapon systems, command and control systems or even missile defense systems.

Although there has been no reported loss of life directly linked to cyberattacks, there is a growing temptation for nations to view cyber weapons as a "cleaner" form of warfare, to be favored over, or perhaps even replace, traditional negotiations that can be prolonged and frustrating. However, the next generation of cyber weapons will increasingly target and destroy physical equipment in industrial and military facilities, and the time might come when we begin to see human casualties. •

> There is a growing temptation to view cyber weapons as a "cleaner" form of warfare, to be favored over traditional negotiations.

— Clay Wilson is a retired program director of cybersecurity studies at American Military University and past program director of cybersecurity policy at University of Maryland University College.



INDUSTRY INSIGHT

BY ALEX ROSSINO

Inconsistent cloud terminology muddies the waters

THE FEDERAL CLOUD COMPUTING MARKET is nothing if not confusing. Despite the best efforts of technical personnel at the National Institute of Standards and Technology to define what cloud is, the cloud market has come to encompass goods and services well beyond the narrow definitions of infrastructure, platform and software as a service. Understanding this is important because the complexity of the cloud market makes finding business opportunities that much harder.

Take for example the booming business of migrating agency datasets to big hosting companies such as Amazon Web Services. AWS provides the cloud (the IaaS), but another vendor does the migration work. In this context, what part of the work should be considered cloud computing?

The hosting services provided by AWS are clearly cloud, but without the data migration work done by the industry partner, AWS provides nothing.

The industry partner is a crucial piece of the cloud puzzle, so shouldn't the migration work also be considered part of the cloud market?

At Deltek, we call these types of services "cloud enabling," and we consider them to be part of the cloud-computing paradigm. Therefore, we include spending on those services in our analysis of the federal cloud market. So if cloud-enabling services fit into a broader definition of the market, companies' business development teams should be searching for opportunities to do that kind of work.

NIST's definition

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

Source: National Institute of Standards and Technology

Data migration services are one shade of gray among many. An even more challenging trend that has emerged in the past couple of years is the use of the word "cloud" to describe a network of communications hardware and switches. That definition first came to my attention in the early stages of the Defense Department's implementation of Multiprotocol Label Switching routers for the Joint Information Environment. Referred to as an MPLS cloud, the "cloudiness" of the gear appears to refer to the scalability of the hardware. But does the MPLS cloud really fit the definition of cloud provided by NIST?

DOD is now taking the cloud analogy one step further and referring to sensor arrays as clouds. Do sensor arrays constitute cloud computing? Their description as cloud confuses the issue quite a bit.

Seeking clarity in the terminology is not simply the complaint of a picky analyst. Using cloud terms for things that are not cloud has a serious impact on our understanding of the market and the size of the business opportunity related to cloud.

For example, the Federal Aviation Administration has requested $24.3 million in fiscal 2016 for its Terminal Voice Switch Replacement program. TVSR replaces aging and obsolete voice switches related to air traffic control. Those switches are basically boxes of hardware that enable the use of voice over IP.

In its fiscal 2016 IT budget proposal, the Transportation Department requested $71.5 million for cloud computing. The question must be asked, however: Does a collection of FAA switching hardware constitute a cloud? If so, then DOT will be spending $71.5 million on cloud. If not, then it will spend $47.2 million.

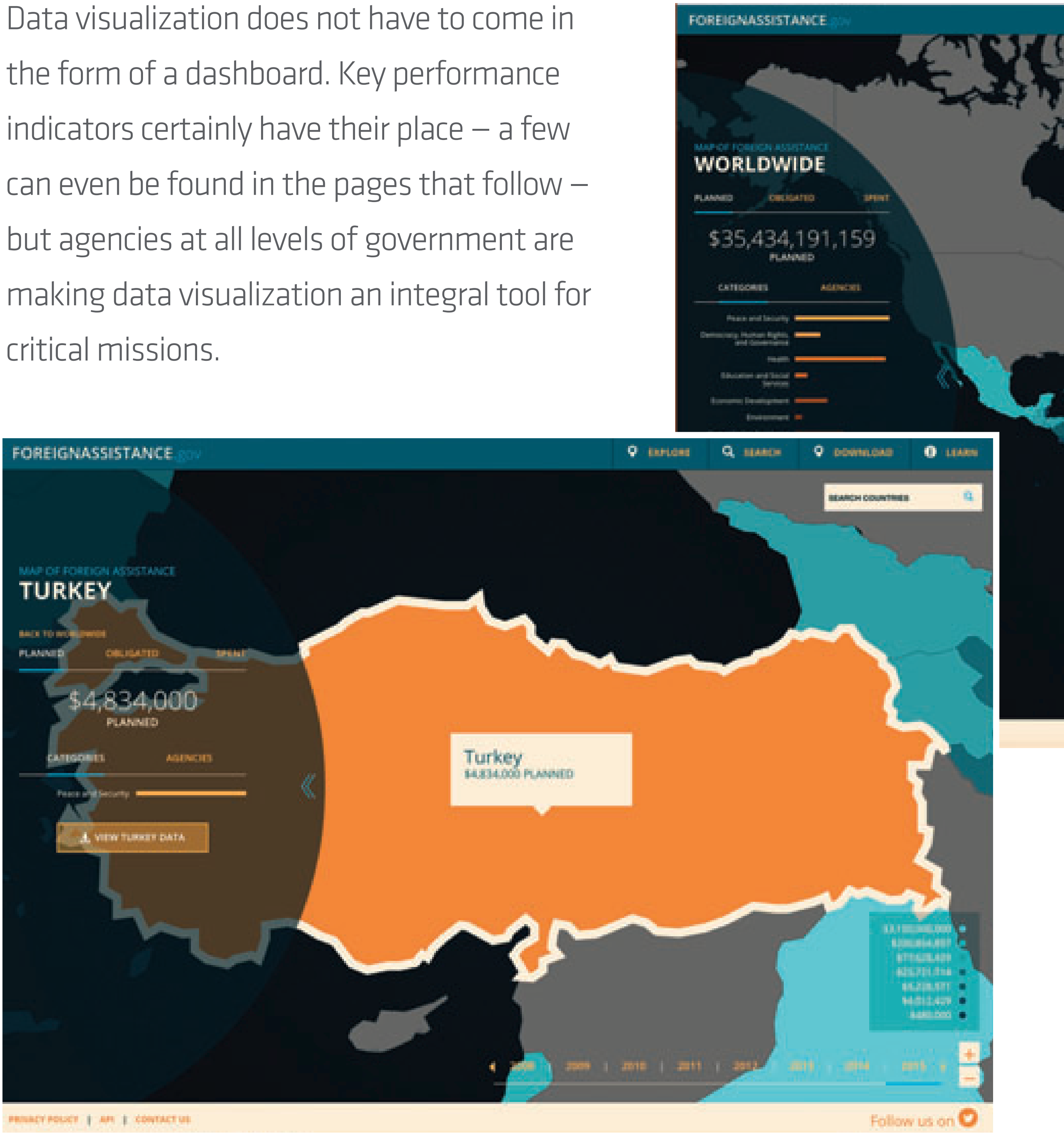
The correct use of terminology is important because the definition of cloud computing informs business decisions across the government market. If the definition is flawed, the resulting decisions are as well. That's why the terminology matters and why clearing up the confusion is relevant. •

— Alex Rossino is a principal research analyst at Deltek. This article originally appeared on Deltek's GovWin blog.

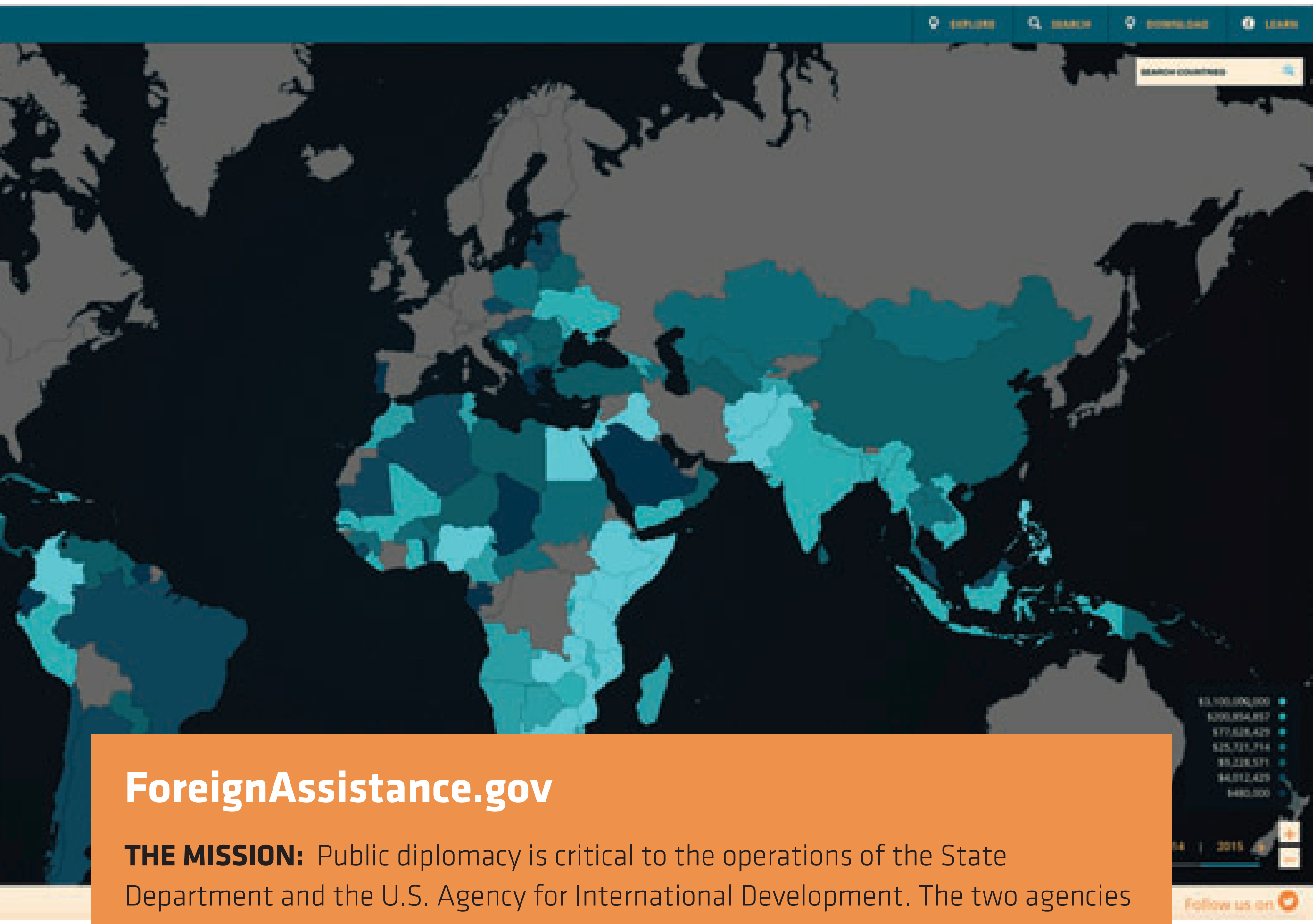
GCN
Technology, Tools and Tactics for Public Sector IT
GCN Newsletter
Sign up for our newsletter.
Email Address
Agencies must update to newer versions of Transport Layer Security
Build a more robust
DENIAL-OF-SERVICE
DEFENSE

Mission-driven da

Data visualization does not have to come in the form of a dashboard. Key performance indicators certainly have their place – a few can even be found in the pages that follow – but agencies at all levels of government are making data visualization an integral tool for critical missions.



ta visualization

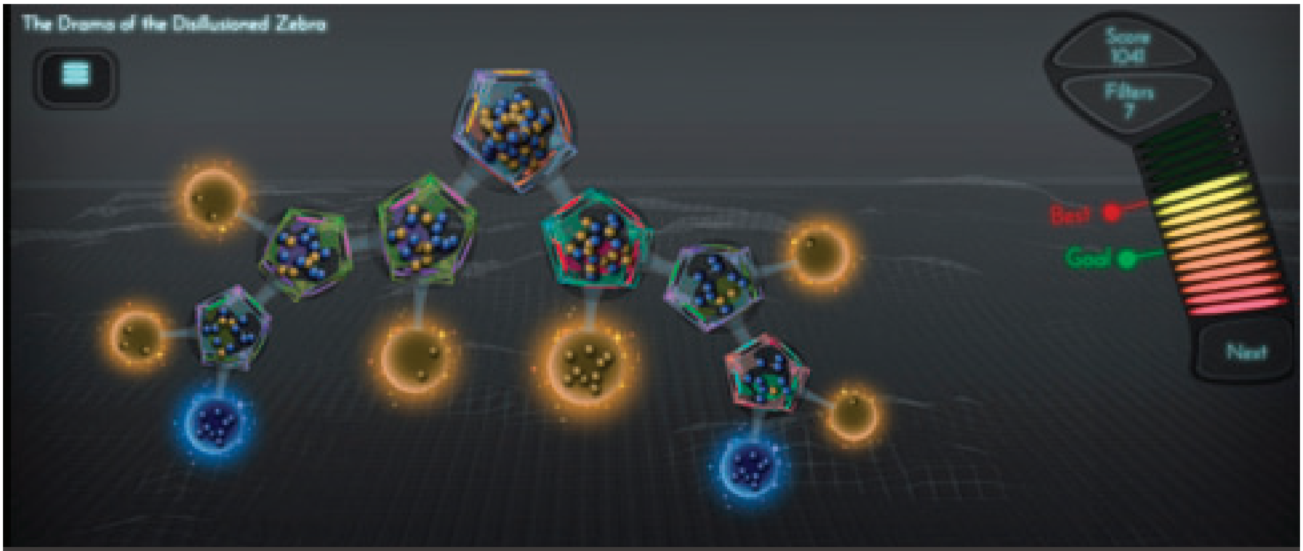


ForeignAssistance.gov

THE MISSION: Public diplomacy is critical to the operations of the State Department and the U.S. Agency for International Development. The two agencies created this beta site in consultation with the National Security Council to better explain U.S. foreign assistance investments around the world.

THE TECH: The beta version debuted earlier this year, after State's Office of U.S. Foreign Assistance Resources created "personas" for the sites' likely users and followed an agile development path to create iterations toward the current design. ForeignAssistance.gov is hosted on the Microsoft Azure cloud platform and offers easy downloads for the various datasets. A developer application programming interface is in the works.

LEARN MORE: http://beta.foreignassistance.gov



Binary Fission

THE MISSION: Finding flaws in software is tedious and usually requires coding expertise that is in extremely short supply. Binary Fission is a game that puts a fun front end on the critical task of identifying loop invariants that could create vulnerabilities in critical applications.

THE TECH: Binary Fission encourages players to sort colored "quarks" in as few steps as possible. The quarks represent values of variables inside the software while the sorting filters represent the potential invariants to be explored and applied. Players' actions are translated into program annotations that help experts generate mathematical proofs to verify the absence of important classes of flaws in software written in the C and Java programming languages. SRI International developed Binary Fission in partnership with the University of California, Santa Cruz; the Air Force Research Laboratory; and the Defense Advanced Research Projects Agency.

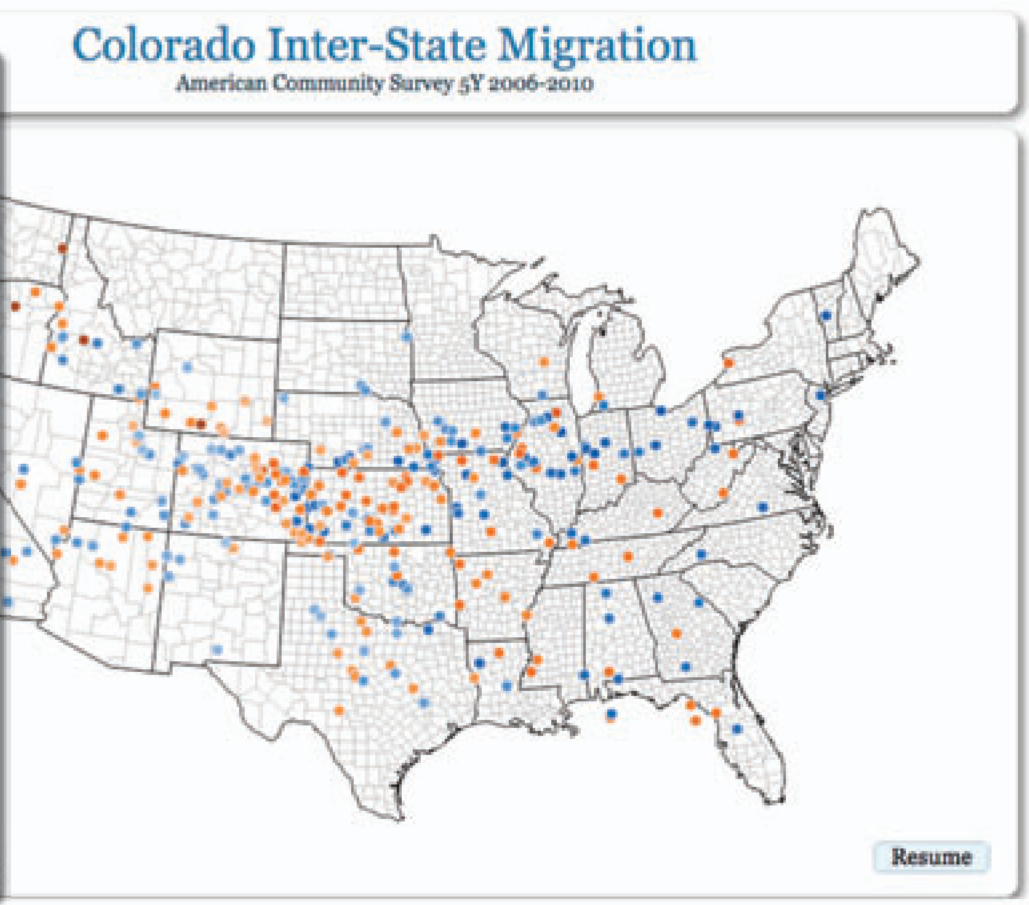
LEARN MORE: https://binaryfission.verigames.com

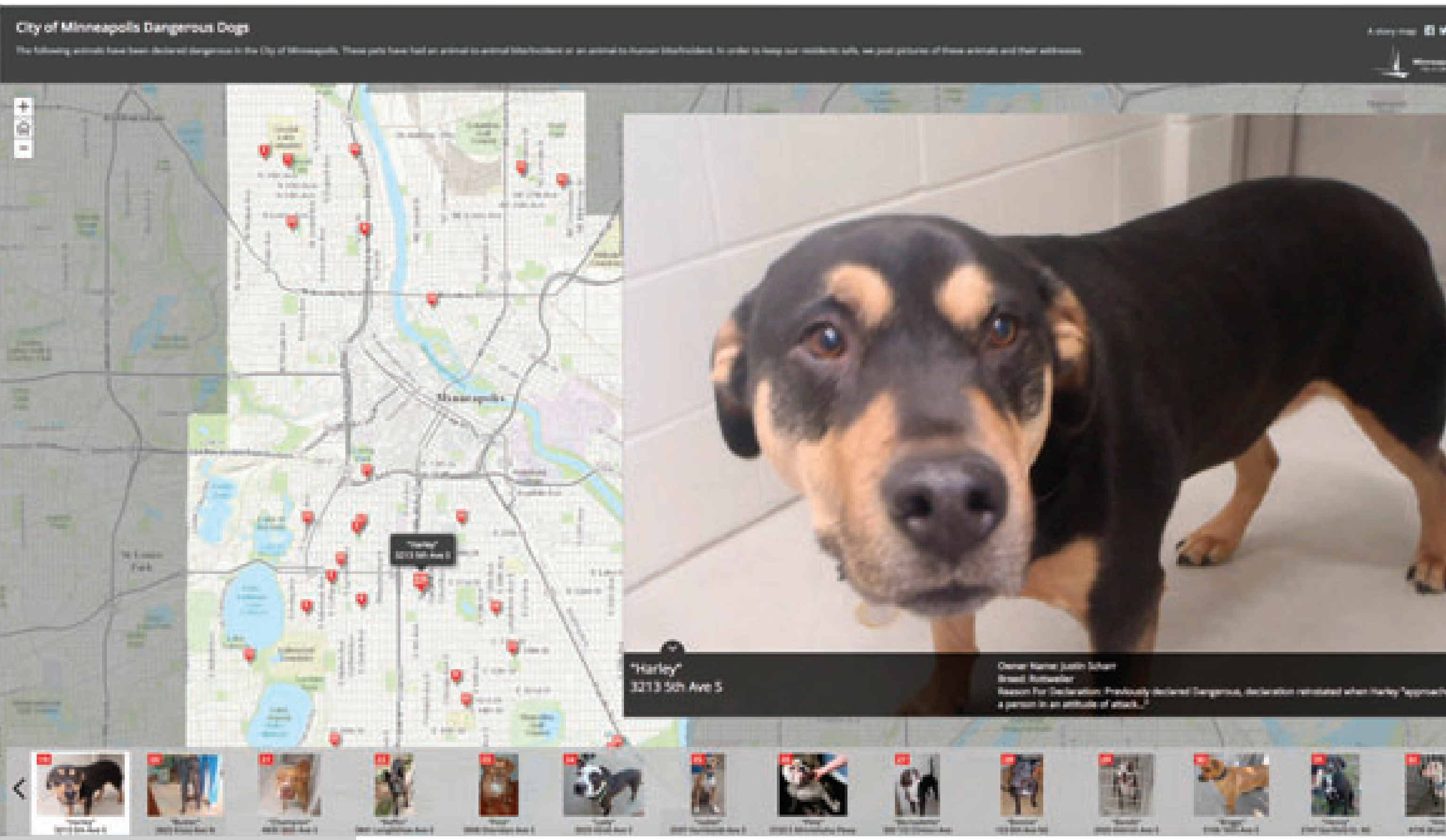
Colorado Inter-State Migration

THE MISSION: Migration to and from Colorado has swung drastically in the past 15 years, and accurate projections are crucial for forecasting demand for state and local facilities and services.

THE TECH: The Colorado State Demography Office visualizes data drawn from the U.S. Census Bureau's American Community Survey to track moves into and out of the state. Built with D3.js, a JavaScript library for mapping and charting data, the migration map uses a probability matrix to show who's moving where and when.

LEARN MORE: http://dola.colorado.gov


Colorado Inter-State Migration
American Community Survey 5Y 2006-2010
Resume



City of Minneapolis Dangerous Dogs

The following animals have been declared dangerous in the City of Minneapolis. These pets have had an animal to animal bite/incident or an animal to human bite/incident. In order to keep our residents safe, we post pictures of these animals and their addresses.

"Harley"
3213 5th Ave S

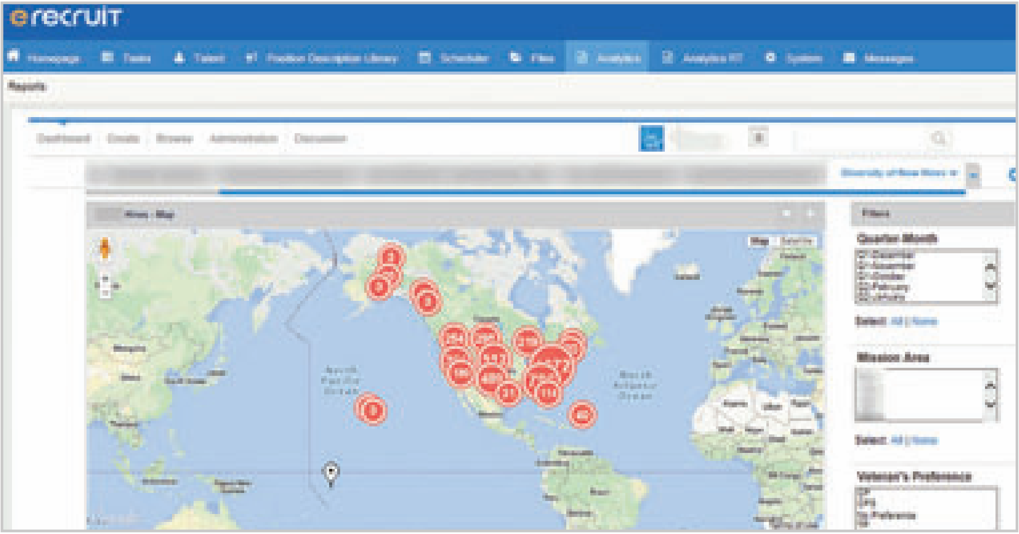
Owner Name: Justin Schan
Breed: Rottweiler
Reason For Declaration: Previously declared Dangerous, declaration reinstated when Harley "approach
a person in an attitude of attack..."

MapIT Minneapolis

THE MISSION: Minneapolis has gone all in with GIS-supported citizen services. Since a citywide mapping portal launched in 2012, hundreds of employees have stepped out of departmental silos to create shared tools that help manage snow emergencies, identify buildings that are suitable for solar energy and even alert citizens to dangerous dogs in their neighborhoods.

THE TECH: MapIT Minneapolis is built on Esri's ArcGIS Online platform. It allows city departments to easily share data and applications when they're ready and work privately when required.

LEARN MORE: http://cityoflakes.maps.arcgis.com/home



One USDA

THE MISSION: The Agriculture Department has spent the past three years moving to a shared hiring and human resources platform while also working to improve component agencies' recruiting and management of employees. Reports like this one allow USDA's chief human capital officer, seven mission-area HR directors and their teams to track the department's progress. (The U.S. Patent and Trademark Office has created a similar system.)

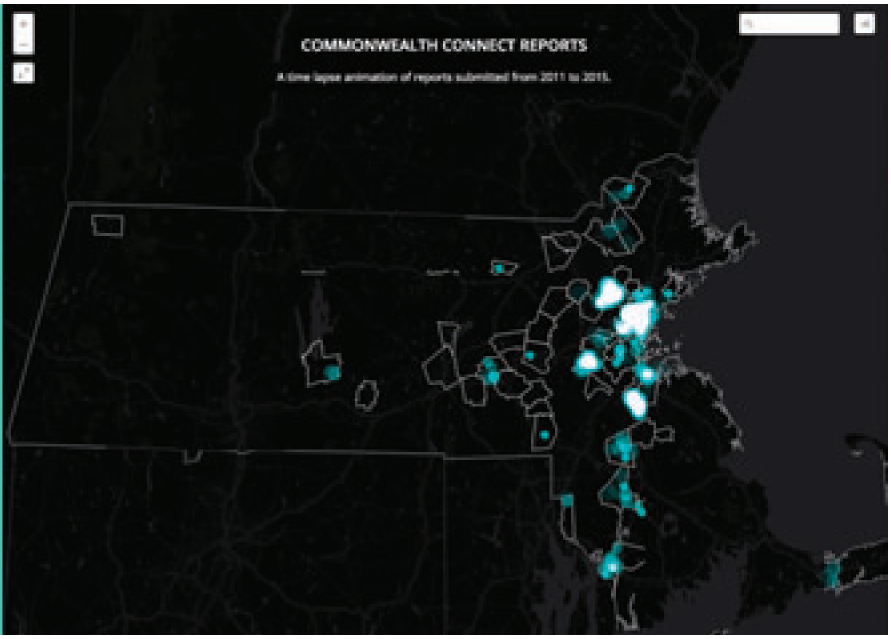
THE TECH: NGA.net's eRecruit – a cloud-based, software-as-a-service solution – tracks both workforce-wide demographics and individual applicants' progress through the hiring process. It also integrates with EODonline, the onboarding software provided by the Commerce Department's National Technical Information Service, and other HR systems.

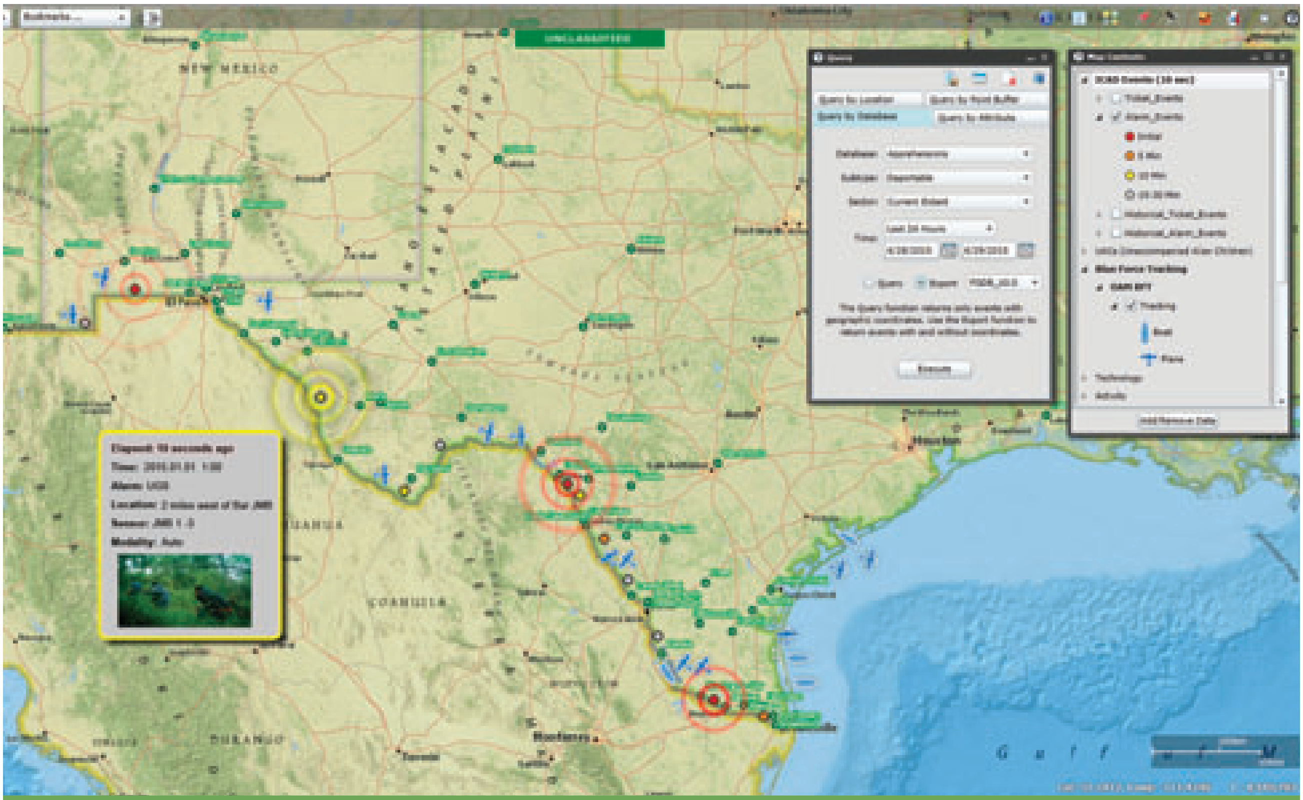
Commonwealth Connect

THE MISSION: Like many of its counterparts at the state and local level, Massachusetts is seeking to improve citizen services with an online 311 system. This map helps monitor use of the service, which was launched in 59 towns and cities over the past four years.

THE TECH: Commonwealth Connect is powered by the SeeClickFix Web tool for reporting non-emergency issues. The data from that system is presented using CartoDB, an open-source tool for storing and visualizing geospatial data on the Web.

LEARN MORE: http://www.mass.gov/opendata


COMMONWEALTH CONNECT REPORTS
A time lapse animation of reports submitted from 2011 to 2015.

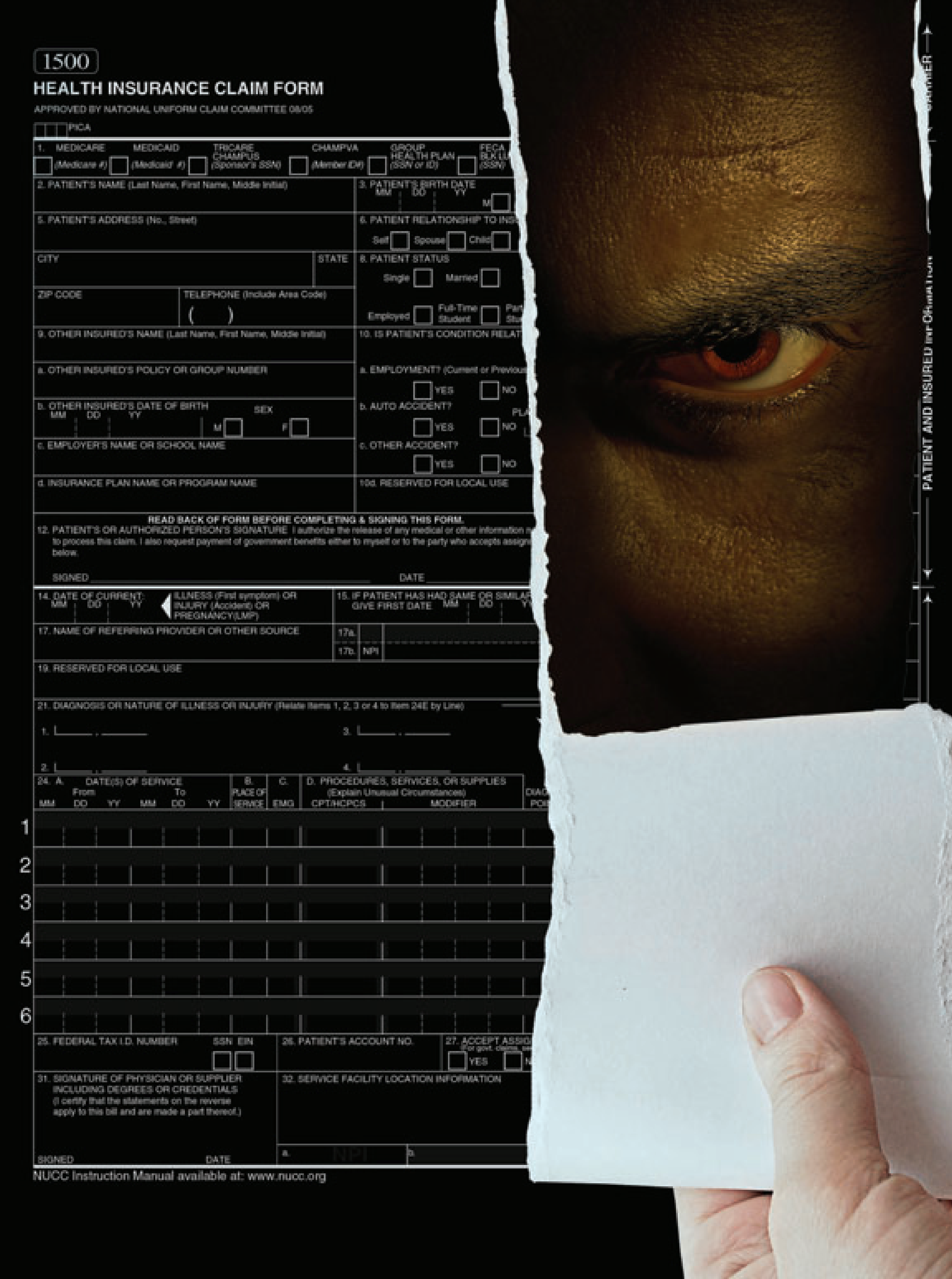


eGIS

THE MISSION: Customs and Border Protection increasingly uses sensors and other technology to monitor America's borders and ports of entry. As the data feeds multiply, situational awareness becomes ever more important.

THE TECH: The Enterprise Geospatial Information Services (eGIS) system is centrally managed and available agencywide. Powered by a SQL Server 2005 geospatially enabled database and Esri ArcSDE software, the system maps patrols, local weather and suspicious border activity, all in real time. The eGIS system also displays border enforcement data that has been imported from various transactional systems, but that data is not housed in the eGIS database.

LEARN MORE: https://catalog.data.gov/dataset/enterprise-geospatial-information-services



1500

HEALTH INSURANCE CLAIM FORM

APPROVED BY NATIONAL UNIFORM CLAIM COMMITTEE 08/05

□□□ PICA

1. MEDICARE MEDICAID TRICARE CHAMPUS CHAMPVA GROUP HEALTH PLAN FECA BLK LU

□ (Medicare #) □ (Medicaid #) □ (Sponsor's SSN) □ (Member ID#) □ (SSN or ID) □ (SSN)

2. PATIENT'S NAME (Last Name, First Name, Middle Initial)

3. PATIENT'S BIRTH DATE MM DD YY M□

5. PATIENT'S ADDRESS (No., Street)

6. PATIENT RELATIONSHIP TO INS

Self □ Spouse □ Child □

CITY

STATE

8. PATIENT STATUS

Single □ Married □

ZIP CODE

TELEPHONE (Include Area Code)

( )

Employed □ Full-Time Student □ Part Stu

9. OTHER INSURED'S NAME (Last Name, First Name, Middle Initial)

10. IS PATIENT'S CONDITION RELAT

a. OTHER INSURED'S POLICY OR GROUP NUMBER

a. EMPLOYMENT? (Current or Previous

□ YES □ NO

b. OTHER INSURED'S DATE OF BIRTH MM DD YY SEX M□ F□

b. AUTO ACCIDENT? PLA

□ YES □ NO

c. EMPLOYER'S NAME OR SCHOOL NAME

c. OTHER ACCIDENT?

□ YES □ NO

d. INSURANCE PLAN NAME OR PROGRAM NAME

10d. RESERVED FOR LOCAL USE

READ BACK OF FORM BEFORE COMPLETING & SIGNING THIS FORM.

12. PATIENT'S OR AUTHORIZED PERSON'S SIGNATURE I authorize the release of any medical or other information n to process this claim. I also request payment of government benefits either to myself or to the party who accepts assign below.

SIGNED ____________________ DATE ________

14. DATE OF CURRENT: MM DD YY ILLNESS (First symptom) OR INJURY (Accident) OR PREGNANCY(LMP)

15. IF PATIENT HAS HAD SAME OR SIMILAR GIVE FIRST DATE MM DD YY

17. NAME OF REFERRING PROVIDER OR OTHER SOURCE

17a.

17b. NPI

19. RESERVED FOR LOCAL USE

21. DIAGNOSIS OR NATURE OF ILLNESS OR INJURY (Relate Items 1, 2, 3 or 4 to Item 24E by Line)

1. ___ . ___

3. ___ . ___

2. ___ . ___

4. ___ . ___

24. A. DATE(S) OF SERVICE From MM DD YY To MM DD YY

B. PLACE OF SERVICE

C. EMG

D. PROCEDURES, SERVICES, OR SUPPLIES (Explain Unusual Circumstances) CPT/HCPCS MODIFIER

DIAG POI

1

2

3

4

5

6

25. FEDERAL TAX I.D. NUMBER SSN EIN □□

26. PATIENT'S ACCOUNT NO.

27. ACCEPT ASSIG (For govt. claims, see □ YES □ N

31. SIGNATURE OF PHYSICIAN OR SUPPLIER INCLUDING DEGREES OR CREDENTIALS (I certify that the statements on the reverse apply to this bill and are made a part thereof.)

32. SERVICE FACILITY LOCATION INFORMATION

SIGNED DATE

a. NPI b.

NUCC Instruction Manual available at: www.nucc.org

Government and industry are developing increasingly sophisticated tools to see beyond the smoke screen of fraudulent claims for medical payments

THE FIGHT AGAINST HEALTH CARE FRAUD

BY PAUL McCLOSKEY

Health care fraud is one of the government's costliest problems. It's a hall of mirrors where billions of dollars are lost to swindlers looking to cash in on the millions of transactions generated by insurance-paying agencies every day.

Last year, the federal government lost $124.7 billion in fraudulent or improper payments through 124 programs, according to the House Ways and Means Committee's Oversight Subcommittee. Medicare fraud accounted for about half, or $60 billion, of the losses.

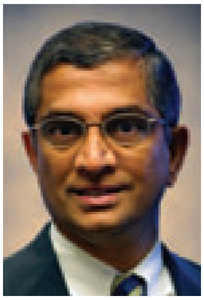
Behind that backdrop, for the past three years officials at the Centers for Medicare and Medicaid Services (CMS) have been working on a system designed to scan for clues to fraud in aggregated claims data. The Fraud Prevention System (FPS) flags anomalies before a payment is made, much like credit industry systems can spot a potentially fraudulent charge and withhold payment while the transaction is investigated.

FPS' developers say the system's biggest challenge could be the sheer complexity of the government's health care payment system. According to the National Health Care Anti-Fraud Association, Medicare Parts A and B process 4.5 million claims every day from 1.5 million health care providers, which means fraudulent patient records and treatments could slip through.

"Preventing fraud is so difficult because the schemes and participants are constantly...evolving to elude enforcement actions," Charlene Frizzera, president of CF Health Advisors, told the subcommittee.

As FPS continues to grow, companies are also building new analytics tools that identify fraud more quickly, accurately and earlier in the payment cycle.

Those companies cite advances in predictive analytics to flag probable fraud leads, case-management platforms to help assess risk throughout a fraud case and a greater emphasis



"The concept of continuous monitoring is what everyone is now waking up to." An individual whose security status is not updated "can do significant damage in 10 years."

RAJ ANANTHANPILLAI, INFOZEN

SHUTTERSTOCK/1105 MEDIA

"A big component that has been missed in authentication – which the government is really in a game-changing position to demonstrate the value of – is around tying a unique identity to the authorization process."

KEN AMMON, XCEEDIUM

on sharing information to help catch fraudsters.

"There is no silver bullet in protecting against fraud," said Mark Nelsen, senior vice president for risk products and business intelligence at Visa. Instead, payers should field a combination of technology, processes and people, and use data analytics as a "critical component in making all three of these effective."

The company's analytics suite evaluates as many as 500 data elements to identify suspicious transactions as they occur. The evaluations provide an instantaneous rating of a transaction's fraud potential by checking the history, geolocation and transaction speed of a potentially fraudulent event.

THE INVESTIGATION CONTINUUM

Vendors say anti-fraud campaigns depend on the sharing of pertinent datasets so that data scientists, program integrity experts and software developers can mount successful fraud cases.

"Integration within the data warehouse is absolutely vital because it lets you visualize things you would not see with smaller datasets," said Elizabeth Snavely, director of fraud, waste and abuse products at General Dynamics IT.

Data-visualization techniques also allow risk managers to monitor a fraud scheme as it unfolds, which Snavely compared to seeing maps of an epidemic spreading from one side of the country to another.

General Dynamics offers a number of applications designed to support the individual stages or the continuum of a fraud case, she said. The first application generates investigative leads by, for example, flagging the number of patients seen by a clinical provider in a single day.

"Let's say you are looking at a series of providers and they are indicating that they saw 52 patients in a day," Snavely said. "That's a red flag. Either that provider is extremely dedicated or the dates in their computer program are wrong."

Could they be telling the truth? "Absolutely," she said, and that's why lead generation is only the first part of the continuum.

Snavely added that although it seems straightforward, "it can take two years to train someone to be a good investigator and pick out those data anomalies." In the early stages of an investigation, "it's not necessarily fraud you're seeing, but it's finding that string of thread that you're going to start pulling on."

The next stage of an anti-fraud sequence involves applying analytics to promising leads. In the scenario in which a doctor claimed to see 52 patients a day, risk managers would look beyond report summaries and ask for all the data on the claims received.

At this stage, investigators might seek information on whether all 52 claims had been paid, whether they were all for the same procedure and whether they all had the same diagnoses. "It's where you start to follow a process and use analytic tools to see what you really have," Snavely said.

In addition to lead generation and analytics, General Dynamics offers a fraud case-management tool that helps maintain program integrity by moving an investigation forward based on the best anticipated financial recovery.

One of the last pieces in the company's product line is a prepayment review that provides a final layer of analytics. "You take all that stuff that you learned during your investigation and you feed it into a prepayment system that begins to flag [problems] before the payment is made," Snavely said.

SETTING THE RISK DIAL

Given the complexity of a typical fraud case, industry executives say prepayment analytics are useful but not perfect tools.

For one thing, most systems flag too many false positives, creating conflict between payers and providers.

"I've seen these put in place in a few different states," said Monty Faidley, director of market planning, health and human services at LexisNexis. "The provider community gets upset because too many claims are being stopped or being flagged; they've got delays in payments. Those provider networks are often strong lobbying groups, and their complaints get heard very quickly."

Therefore, using prepayment analytics requires the ability to fine-tune the risk equation by balancing the requirements of payers and providers. "You need a soft touch," which might involve putting a test in place and tracking its impact over several months, Faidley said.

LexisNexis recently helped New York City's Human Resources Administration use predictive analytics to study costs related to providing benefits to its 2.9 million Medicaid recipients, 1.8 million Supplemental Nutrition Assistance Program recipients and 350,000 Cash Assistance recipients.

The company combined the agency's data with LexisNexis' public records data, "which gives us broad context of information about each beneficiary," Faidley said. By applying its analytics scoring model to differentiate low-risk beneficiaries from those who "definitely need to be investigated," the city was able to flag costs associated with 9,700 cases and save more than $52 million.

> "Integration within the data warehouse is absolutely vital because it lets you visualize things you would not see with smaller datasets."
>
> **ELIZABETH SNAVELY, GENERAL DYNAMICS IT**

THE MOVE TO ZERO TRUST

Predictive analytics allow organizations to broaden their searches for patterns of fraud. In addition, new identity security tools are emerging to help keep tabs on enterprise players who might be victimized in fraud schemes.

"These are privileged users with access to everything in the database — not just their records; they have the ability to go from system to system inside a corporate or government infrastructure," said Ken Ammon, chief strategy officer at Xceedium.

Those users have been at the center of several recent high-profile attacks. Their privileges were exploited as the result of sophisticated spear-phishing attacks, including the one on health insurer Anthem earlier this year in which

CMS' ANTI-FRAUD POWER TOOL

The Fraud Prevention System (FPS) is a nearly four-year effort by the Centers for Medicare and Medicaid Services to help automate the review of health care claims before, during and after they are filed. CMS considers FPS a power tool in its plan to move away from "pay and chase" to a prevention model of claims management in its fight against fraud.

In the past, CMS typically paid a claim then checked its validity before making a decision to try to recover the funds if it discovered they had been paid improperly. That approach has made it easy for fraudsters to elude regulators by sending up a smoke screen of false claims and counter-claims during the payment process.

FPS uses predictive analytics to flag providers and other players in the health care supply chain who might have participated in payment fraud.

As in anti-fraud approaches in the credit card industry, FPS enables CMS to assign risk scores to specific claims and providers, thereby establishing a starting point for analysts to pursue a potential fraud case.

When FPS identifies irregular activity, it automatically generates potential investigative leads for program integrity contractors – the teams of experts and data scientists who can help identify actions that can be taken immediately, such as suspending payment or launching a case review.

CMS officials say the success of FPS often depends on quickly detecting fraudulent payments, a goal for which it is enhancing some of its response systems. Responding to a suggestion by the Government Accountability Office, CMS has improved the integration of FPS with its claims-processing system, giving FPS the ability to stop payment of improper claims by transmitting a claim denial message directly to the payment system.

"What this means is that FPS can identify billing patterns and claim aberrancies that would be undetectable or difficult to detect by CMS' current claim edit modules or a single contractor reviewing on a claim-by-claim basis," said Shantanu Agrawal, director of the CMS Center for Program Integrity, during a hearing held earlier this year by the House Ways and Means Committee's Oversight Subcommittee.

Industry players say FPS shows promise but is still young. Louis Saccoccio, CEO of the National Health Care Anti-Fraud Association, told the subcommittee that "it will take time to effectively refine and adjust the models for such a large and complex system as Medicare in order to realize the full potential that these powerful technologies offer."

– Paul McCloskey

80 million records were stolen.

"What happens is the criminal targets those individuals because they know their roles or their accounts are extremely powerful in the organization," Ammon said. "If they can send them an email that they might click on, it installs as a super user who now can download the entire corporate database from network to network."

To help defend against that vulnerability, Xceedium has embraced a policy of "zero trust," whereby access is extended only for a specific reason and for a specific amount of time.

"It's a method in which you are now managing the enablement rather than trying to curtail certain transactions on the network," Ammon said. It gives network managers "a very small subset of items [that] an individual has credentials and capabilities to do."

The company's Xsuite is built around that policy. "A big component that has been missed in authentication — which the government is really in a game-changing position to demonstrate the value of — is around tying a unique identity to the authorization process," Ammon said. Without that capability, security managers "really have no idea who you are."

Xsuite denies network access to all systems and applications except those that are expressly allowed. The product also monitors, records and audits privileged access to systems in legacy IT, cloud or hybrid configurations and provides DVR-like recordings of privileged user sessions, which eases continuous monitoring and forensic activities.

"If you have 10,000 people in an organization, you might have 700 people or less that you might consider privileged," Ammon said. The tool gives those high-level users "the equivalent of a video camera watching their screen for everything that they do. And we will enforce a policy while they're doing the job."

Identity security is behind another application designed to flag the activities of agency employees who might be involved in or subjected to fraud. InfoZen's IDentrix continuously monitors personnel data, starting with prehire background checks, to alert organizations to potential internal threats.

The software checks more than 65 public identity attributes, including criminal and court records, to keep employees' risk profiles continuously updated and correlated through their entire work history.

"The concept of continuous monitoring is what everyone is now waking up to," InfoZen CEO Raj Ananthanpillai said. An individual whose security status is not updated "can do significant damage in 10 years. If you had alerts set up saying, 'If anything in these categories happens to that individual,' you could investigate and take preemptive action."

However, he added, "I'm not saying this is going to solve problems, but at least you would mitigate a big chunk of the problem."

Partial fixes to big threats might ultimately cut the fraud problem down to size, but anti-fraud developers don't see fail-safe solutions ahead.

"Fraud is always evolving, but these solutions are beginning to make a difference," Faidley said. "We see more procurement and interest, especially at the legislative levels. They're starting to ask some hard questions and are saying, 'It's time to emphasize this and really make a difference.'" •

3 INGREDIENTS FOR SUCCESSFUL FRAUD ANALYTICS

Companies are bringing a blend of analytics, computing and investigative approaches to the fight against fraud. But three ingredients are essential for any successful program, said Doug Coombs, vice president of fraud solutions at Verisk Health. They are:

1. Data smarts. Successful analytics call for creating teams of the smartest possible data scientists working with the most experienced fraud investigators and health clinicians.

"If you don't have people investigating these cases talking with data scientists at the time the analytics are developed, what you end up with at times are results that are theoretically interesting but practically not actionable," Coombs said.

2. Data quality. In order to understand whether fraudulent behavior can be acted on, analytics firms must obtain data from many sources, including clients, internal resources and public databases. That data should produce promising leads without creating too many false positives, Coombs said.

3. Teamwork. Fraud-busting organizations must have the capacity to gather data on claims, licensing and sanctions placed on providers – all of which should sometimes be acquired and examined over long periods of time.

Agencies must have teams of scientists and investigators working together because "each specialty brings to that process a unique perspective that allows you to create a high-value result," Coombs said.

– Paul McCloskey

Consolidated 311 boosts efficiency, savings

A new system in Tulsa, Okla., consolidates customer services across 15 city departments to help resolve calls faster

BY STEPHANIE KANOWITZ

When residents contact the Tulsa, Okla., Customer Care Center using any of several dozen phone numbers, they get an automated response asking them to press a number corresponding to their need. That routes the call to the correct agent for the job, and that agent uses five pieces of software to track down the answer or set up a work order. All work orders go to a single administrative agent who reviews them and creates official orders.

This month, however, residents will begin using a new 311 system to get non-emergency help via phone, text message or Web form, and they can even set up service requests themselves. What's more, 311 agents will use a single platform to answer questions and submit work orders. The result is a consolidation of customer services across some 15 municipal departments.

"Once 311 goes live and we promote that to the community, we're going to be getting phone calls into our contact center that were going to other department groups across the city," said Michael Radoff, the center's director. "We don't want to just be a transferring service. We want to be able to answer those calls and drive first-call resolution as high as we possibly can."

Because the system is completely new, Radoff and his team had to start from scratch. For the 311 element, they spent almost a year contracting with about 10 telephony providers — including AT&T, Cox Communications and Windstream Communications — that will participate in the 311 conversion. Next, they made a bidirectional map to set up phone switches, which took more than a year.

To consolidate the software, the city tapped LAGAN Enterprise from KANA, part of Verint. It will replace Lockheed Martin's Intranet Quorum service order tool and eventually another system that handles code violations. For questions related to the Tulsa Municipal Court, which has the highest call volume, the city will continue to use the court's JURIS information system, which was developed and is maintained by the Tulsa Police Department's Systems Development and Support team.

KANA's LAGAN helps 311 call takers progressively ask questions to pinpoint the appropriate response. For example, for a pothole complaint, they can ask which side of the street the pothole is on and how big it is. That approach also helps prioritize the service orders based on rules set in the system.

In addition, city residents will be able to take matters into their own hands — to a degree. They can create profiles

FFOOTER / SHUTTERSTOCK.COM

and enter their own service orders and then track them. The system sends automatic email alerts when orders are set up and as they are completed.

"We'll be able to do a 360-degree, close-the-loop process with citizens so they don't have to call us back to see if what they requested got done," Radoff said.

Tulsa's 311 system will also have interactive voice response (IVR) with as many as 38 self-service paths for callers to follow for smaller issues such as missed trash pickups and payments.

"That's really going to drive down call volume that comes in to our agents [and] drive up efficiency for us," Radoff said.

Additionally, when someone who has set up a profile calls 311, that caller's information will pop up on an agent's screen via computer telephony integration (CTI), which means agents don't have to spend time confirming the person and the request.

"I'm expecting to save 20 to 30 seconds per call just by having a CTI screen pop in place," Radoff added.

The system also includes a mobile app through which users can submit photographs of problems such as graffiti. Those submissions will be linked to their profiles and tagged with GPS data so officials can locate the problem more quickly.

"The real unique challenge of modern 311 call centers is that even though they're branded as 311, it's so much more than a phone number," said Steve Carter, senior director of public-sector accounts at KANA. To provide context-aware knowledge, 311 systems must be able to tap the right knowledge base, manage the agents' computers and combine scripting and search.

Additionally, Tulsa is launching reactive and proactive chat services. Reactive chat means users click on an icon to launch a chat session with an agent, while proactive chat lets agents engage with people they suspect need help finding information or locating services, Radoff said.

"For example, on our permits page, if we see a citizen who's been hunting around to find the right permit form to fill out so that they can start a project, we would like to be able to pop in and say, 'Hey, we see you're looking for a permit. What kind of project are you trying to get done and we'll tell you what we need to do.'"

The LAGAN Enterprise from KANA cost the city about $980,000, and the 311 phone exchange will likely cost $3,000 to $4,000 per month depending on call volume, Radoff said. But the savings will be significant, he added. For instance, the IVR system should reduce call volume by 30 percent.

"Take our call volume, which is in the 550,000 to 600,000 range per year, and if you can drop 30 percent of those calls off, that's [more than] 150,000 calls," he said. "That's about three and a half to four minutes per call. That adds up to a lot of money very quickly." •

Michael Radoff: A public/private perspective

To overhaul the city's customer service, the mayor of Tulsa, Okla., asked Michael Radoff for help. After all, he had 35 years of experience helping Fortune 500 companies consolidate customer service operations.

Before taking his first public-sector job as director of Tulsa's Customer Care Center two and a half years ago, Radoff was part of a team that handled the national consolidation of customer service operations for Gannett.

He found shepherding a project in the government to be quite different.

"There were a lot more experts within corporate who really knew a lot about the components that we needed to implement," Radoff said. "You really had a much broader support team than what I've seen in government."

The government's existing technology also tends to be older. For instance, Tulsa has systems that date to the 1970s, and that makes upgrades more challenging, he said.

Additionally, the procurement process is slower in the public sector, and as a result, implementing the new 311 system is taking longer than Radoff anticipated. "I really thought we'd be up and running on this system eight or nine months ago, but the procurement process alone took us a year and a half to get through," he added.

Based on his experiences, he said many cities would benefit from recruiting private-sector experts to help with projects.

"You need to bring some people in from the corporate world" because they can have a different perspective, Radoff said. In the private sector, "if I had something that had [a return on investment] of 20 percent on it, whether it was in the capital plan or not, I got an instant green light. Those are not the driving factors that let you do things [in government]. You can use those to help you sell your case, but there are a lot of other things that go on in the background before decisions are made."

– Stephanie Kanowitz

CASE STUDY DATA BREACHES

States at odds with feds on data breach proposals

Pending legislation would enforce a definition of personal information that is narrower than what many states use

BY SARAH BREITENBACH

As Americans' personal information continues to move online, everything from medical records to mothers' maiden names, Social Security numbers and fingerprints are increasingly up for grabs. And the states and the federal government are at odds over how to respond.

Since California first began enforcing data breach reporting requirements in 2003, 46 other states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have implemented varying degrees of regulation, including requirements to provide free credit monitoring to victims, quickly notify consumers of a breach and tell state attorneys general or other agencies about compromised records.

States are toughening their laws by broadening the definition of "personal data," requiring timelier reporting and expanding the number of people or agencies companies must notify.

In contrast, Congress is just now coalescing around federal standards. Pending legislation would preempt state laws and enforce a definition of personal information that is narrower than what many states use.

Caught in the middle are businesses, which would prefer a single federal standard to the different state requirements, and consumers, who must scramble to protect their bank accounts, credit cards and credit worthiness from thieves who steal their identities.

Scott Talbott, senior vice president of government affairs at the Electronic Transactions Association — which represents banks, companies that make credit card swipe terminals and online payment companies — said his organization welcomes a tough federal standard. Without one, reporting breaches will continue to be a cumbersome and expensive task, he added.

Data breaches by the numbers

$6.5 million
the average cost of a data breach to a U.S. company in 2015

5,000 / 780 million
number of breaches in the U.S. since 2005 and number of records affected

348 / 100 million
number of breaches in the U.S. this year and number of records affected

"Letting consumers know what to expect with one law we think is preferable, is more efficient and works better for all parties involved in the current system," Talbott said.

David Thaw, an assistant professor of law and information sciences at the University of Pittsburgh, said the proposed federal Data Security and Breach Notification Act of 2015 is just a reporting law — one that is less stringent than many state laws. What's really needed is a broad federal law that would require companies to better protect consumers' information and privacy from breaches, he added.

He said the patchwork of state laws more effectively protects consumers, and complying with them is not as hard as companies say it is.

"I am 100 percent certain I could write a computer program [that] would take all of the inputs from a given data breach and spit out all the notification letters," he said. "It's not hard. There are very good attorneys out there who can put out all the notifications for all the jurisdictions and get it right and get it done."

BREACH REPORTING ACROSS THE STATES

According to the Identity Theft Resource Center, there have been more than 5,000 breaches in the United States affecting more than 780 million records containing personal information since 2005, when the center began tracking them. So far this year there have been

348 breaches that compromised more than 100 million records, according to the center.

At least 32 states have considered legislation this year that would establish or expand data breach policies, according to the National Conference of State Legislatures. The proposals include expanding the kinds of compromised personal information that would trigger a notification to consumers and requiring companies to report breaches to state attorneys general.

In May, Illinois lawmakers updated the state's 2005 Personal Information Protection Act to require companies to report breaches to the attorney general's office. The updated law expands the definition of personal information to include online browsing details and purchase histories.

Illinois Attorney General Lisa Madigan said the bill is one of the most comprehensive in the country. Gov. Bruce Rauner has not said whether he will sign it.

"Identity theft is an enormous problem," Madigan said. "It's sometimes very difficult to identify, very difficult to clean up, and it can have an enormous impact on somebody's ability to function in our world."

Twenty-one states and Puerto Rico require companies to report data breaches to the attorney general's office or another state agency. Three more states — Montana, North Dakota and Washington — have similar laws that will take effect by the end of the year.

In Connecticut, considered to be at the forefront of data breach policy, companies have been required to report breaches to the attorney general since 2012. Connecticut's attorney general, George Jepsen, said the law has forced many companies to disclose breaches they otherwise wouldn't have reported. His office now receives about 400 notifications a year.

Most of the breaches are small and not harmful, Jepsen said, adding that Connecticut residents are better protected because his office has the power to investigate the breaches and pursue legal action if companies don't do what they are supposed to do.

"If Connecticut has 400 breaches, I guarantee you there's no way the feds are going to be looking at all 400," Jepsen said. "There continues to be an important role for states' attorneys general. We've got the boots on the ground to do the work."

The ability of attorneys general to investigate breaches and enforce data breach laws holds companies accountable to consumers whose data is lost or stolen, Thaw said.

"State attorneys general bring a lot more enforcement resources to bear," he added. "In this case you have 47 different entities, any of which [have enforcement authority] for a large-scale breach.... That's a pretty big threat to make sure you report a breach."

A FEDERAL STANDARD

Jason Brewer, vice president of communications and advocacy at the Retail Industry Leaders Association, said his organization favors a federal standard that would preempt state laws.

Reacting to a breach often involves setting up and staffing call centers, communicating with Internet service providers to ensure that email notifications aren't caught in spam filters and then identifying and reaching out to people affected by a breach, Brewer said.

"Part of the challenge is there's a lot more that goes into notifying than hitting send on an email," he added.

> "Part of the challenge is there's a lot more that goes into notifying [breach victims] than hitting send on an email."
>
> – JASON BREWER, RETAIL INDUSTRY LEADERS ASSOCIATION

The average cost of a data breach to a U.S. company in 2015 is $6.5 million, according to a study conducted by the Ponemon Institute. The average cost per lost or stolen record is $217. Much of that amount — $143 — covers indirect costs such as lost customers. The remainder covers direct costs such as technology and legal fees.

Edward Marshall, a partner at Atlanta-based law firm Arnall Golden Gregory, represents payment card processers. He said a federal standard would streamline the reporting process and reduce the legal fees for companies, which are often dealing not only with the cost of reporting a breach but also with fallout from shareholders and consumers.

"It is a very cumbersome process that I would argue takes away from where the emphasis should be placed," which is fixing the breach, Marshall said. "I've heard a lot of people say when you've become a victim of a breach, it becomes your full-time job for a year."

For Eva Velasquez, president and CEO of the Identity Theft Resource Center, there are pros and cons to a federal law. She said a federal law could protect citizens in the three states — Alabama, New Mexico and South Dakota — that don't have data breach reporting laws, but it could provide less protection to consumers in states with tougher laws. •

— *Sarah Breitenbach is a reporter for the Pew Charitable Trusts' Stateline.org, where this article originally appeared.*

Advertiser	URL	Page
CDW Government, Inc	www.CDWG.com/sewpv	10a-10d
Enterprise Architecture East	www.GovEAconference.com	35
Face-to-Face Event Series	www.GCN.com/events	23
Hewlett Packard	www.hp.com/go/pubsecsecurity	2
QTS	www.GCN.com/2015snapshotcybersecurity.	9
Shure Inc.	www.shure.com/conferencing	5
Visual Studio Live- New York	www.vslive.com/newyork	36
Visual Studio Live - Redmond	www.vslive.com/redmond.	13

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

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

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

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

PRODUCTION COORDINATOR

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

PUBLIC SECTOR MEDIA GROUP

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

WISHLIST

Tech we hope to see in the public sector

HGST 10TB 'helium' drive

The Ultrastar Archive Ha10's sealed helium platform offers less resistance and greater storage density by squeezing seven thinner platters into a space that usually allows five. A smaller motor runs cooler and on less power, bringing down the storage cost per gigabyte. And it uses what HGST calls shingled magnetic recording (SMR) to layer data tracks across one another.

The Ha10 cannot simply be dropped into a traditional storage system, however. Host applications must be customized to account for the SMR, and native driver and file system support for server platforms is not expected until 2016.

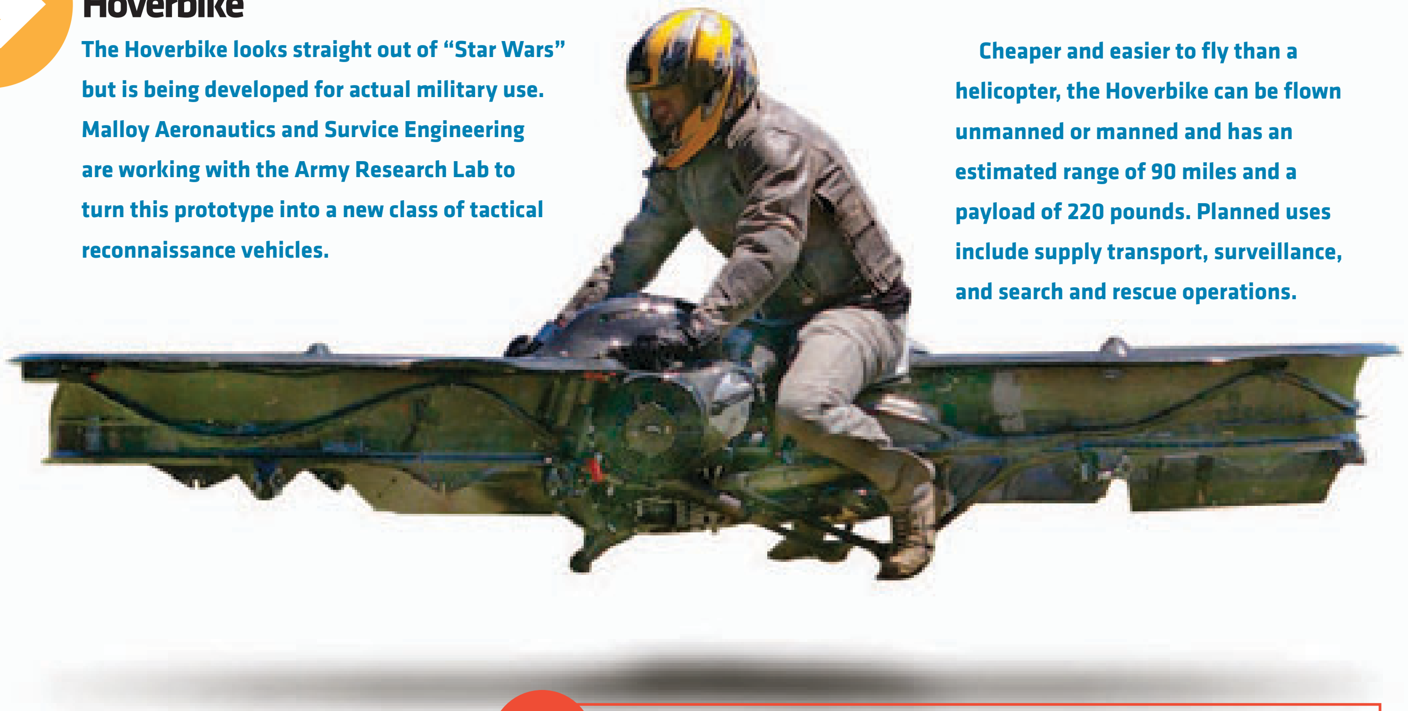
Pwn Pad 3

The Pwn Pad 3 from Pwnie Express gives penetration testers a lightweight tablet for easy, mobile evaluation of wired and wireless networks. It boasts a Tegra K1 2.2 GHz quad-core processor, 2GB of RAM, more than 100 of the most popular open-source testing tools and the Kali Linux security distribution. The first units are expected to ship this summer.

Hoverbike

The Hoverbike looks straight out of "Star Wars" but is being developed for actual military use. Malloy Aeronautics and Survice Engineering are working with the Army Research Lab to turn this prototype into a new class of tactical reconnaissance vehicles.

Cheaper and easier to fly than a helicopter, the Hoverbike can be flown unmanned or manned and has an estimated range of 90 miles and a payload of 220 pounds. Planned uses include supply transport, surveillance, and search and rescue operations.



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

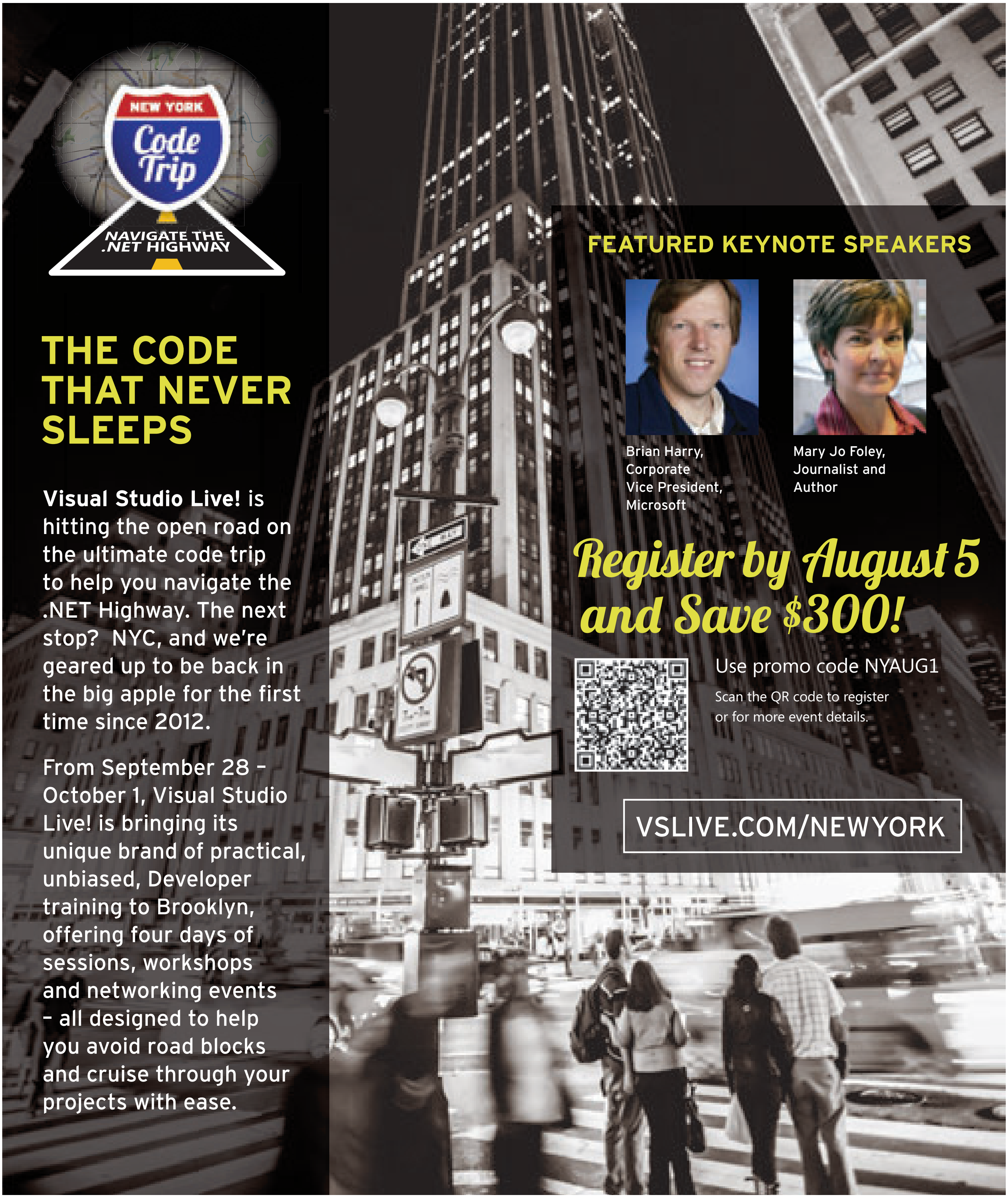
Visual Studio LIVE!
EXPERT SOLUTIONS FOR .NET DEVELOPERS

VSLIVE.COM/NEWYORK

New York

SEPTEMBER 28 –
OCTOBER 1

MARRIOTT @ BROOKLYN BRIDGE • NEW YORK, NY



THE CODE THAT NEVER SLEEPS

Visual Studio Live! is hitting the open road on the ultimate code trip to help you navigate the .NET Highway. The next stop? NYC, and we're geared up to be back in the big apple for the first time since 2012.

From September 28 – October 1, Visual Studio Live! is bringing its unique brand of practical, unbiased, Developer training to Brooklyn, offering four days of sessions, workshops and networking events – all designed to help you avoid road blocks and cruise through your projects with ease.

FEATURED KEYNOTE SPEAKERS

Brian Harry,
Corporate
Vice President,
Microsoft

Mary Jo Foley,
Journalist and
Author

Register by August 5 and Save $300!

Use promo code NYAUG1

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

VSLIVE.COM/NEWYORK

GOLD SPONSOR
GitHub

SUPPORTED BY
Microsoft
Visual Studio
msdn magazine
Visual Studio MAGAZINE

PRODUCED BY
1105 MEDIA INC