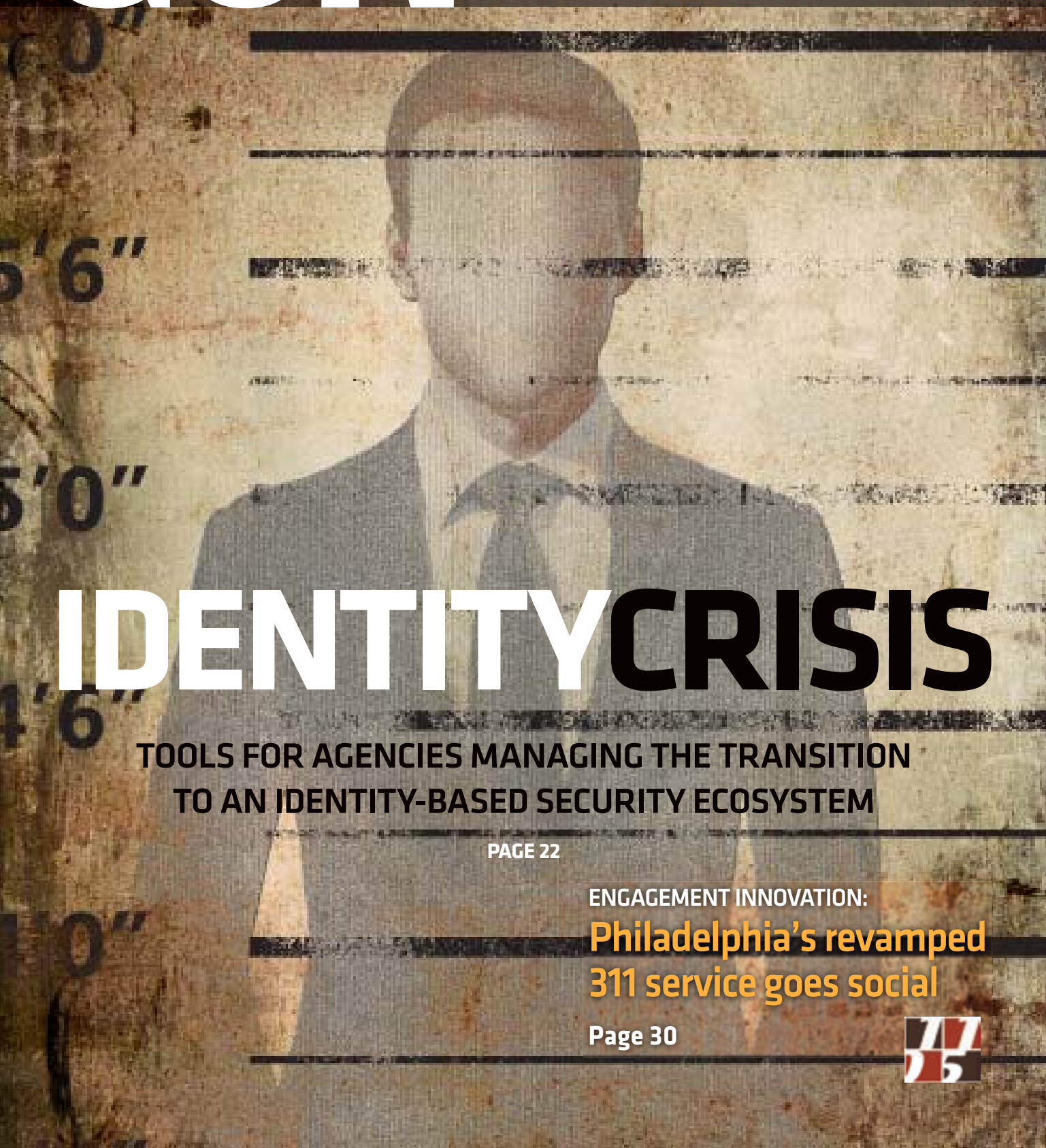
GCN

MARCH 2015 VOLUME 34, ISSUE 3

Technology, Tools and Tactics for Public Sector IT

THE INTERNET OF DATA HUNGRY, AUTONOMOUS SUPER SENSORS

PAGE 26



IDENTITY CRISIS

TOOLS FOR AGENCIES MANAGING THE TRANSITION TO AN IDENTITY-BASED SECURITY ECOSYSTEM

PAGE 22

ENGAGEMENT INNOVATION:

Philadelphia's revamped 311 service goes social

Page 30

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™

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

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

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

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

INSIDE

FEATURE

CASE STUDIES

BRIEFING

COMMENTARY

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.

Agencies struggle to move beyond digital strategy

BY STEPHANIE KANOWITZ

Federal agencies still have work to do more than two years after the White House issued its mobile-focused Digital Government Strategy, according to a December report from the Government Accountability Office.

All 24 agencies required to comply with the strategy have made efforts to improve their digital services for those who use mobile devices, but so far much of it has been in planning rather than execution.

"Strategy is always a challenge when you're dealing with digital technology," said Jacob Parcell, manager of mobile programs within the General Services Administration's Office of Citizen Services and Innovative Technologies.

The Digital Government Strategy, released in 2012, aims to let citizens access high-quality digital government information and services anywhere, anytime on any device; manage devices, applications and data securely and affordably; and open more government data.

"I think that what the digital strategy did is it got the ball rolling on this conversation," said Chris Roberts, vice president of public sector at Good Technology, a Sunnyvale, Calif.-based mobile security solutions provider. "It got the government to focus on ways that it might be able to create more efficiencies, save costs and essentially execute its mission a little better."

Some agencies are leading the way in this effort, mainly through the development of mobile websites and native apps, Parcell said. For example, the Census Bureau created two apps out of its open data. One called dwellr lets users enter preferences and then suggests the top 25 U.S. cities best suited to them. The other, Census Pop Quiz – a play on the word "population" – uses gamification elements, giving badges for every correct answer people can give about the 50 states.

Despite agencies' best efforts to meet the strategy's 2013 deadlines for mobile accomplishments, legitimate challenges have hindered them, Roberts said, including sequestration, continuing resolutions and midterm elections.

But the No. 1 challenge – and one that President Obama referenced in his State of the Union address Jan. 20 – is cybersecurity, he said.

"Even just a few years back, I don't think we took security nearly as seriously," Roberts said. "We assigned that to the Department of Defense, the FBI, Homeland Security, folks like that, but it's become clearer and clearer that whether you're at any department – whether it's the [Veterans Affairs] or Labor or Commerce or housing [departments] that may not have been in a direct line with regard to national infrastructure – that every agency has got to have security."

Going hand in hand with security nowadays is privacy, Parcell added. For example, the Internal Revenue Service's IRS2go mobile app lets users check their tax returns, so the agency needs to ensure the system is not only secure, but able to maintain privacy of the data. "It's sort of like yin and yang with privacy and security. They're like peas in a pod," he said.

Policy is another obstacle that started with the bring-your-own-device debate, Roberts said.

The policy issue went in three waves, he said. Initially, senior-level employees were given or had their own iPads and wanted to use them at work. The IT organizations tried to find ways to accommodate that.

The second wave involved the BlackBerry, once the device of choice among feds, and whether it would remain intact or be sold. "The question marks around BlackBerry forced many in government to look at a Plan B when it came to mobile," he said.

> "Strategy is always a challenge when you're dealing with digital technology."
>
> – JACOB PARCELL, GSA

"The third wave is where we are currently with government, and that is how do I take a so-called front foot with this?" Roberts said. "How do we decrease costs, increase efficiencies and better execute our missions knowing that budgets are likely going to be shrinking and that we're going to be asked to do more with less, and that is the real question or the right question that government should be asking right now."

Technical challenges emerged, too. Responsive W eb design, or making sites that adjust to the screen size of the viewing device, gave some feds pause, Parcell said. For example, agencies had

a tough time figuring out how to make charts responsive. The Department of Health and Human Services found an answer – and then it shared it.

"What HHS did was they created some code – about four or five lines of code – that makes charts mobile-friendly," Parcell said. "The Defense Financial Accounting Service actually took this code and implemented it on their website in about two hours, and they said it saved them a bunch of time and a bunch of headaches because 5 percent of their website is charts and graphs."

Another problem is that many mobile devices exist and in many sizes, but some agencies are limited to using only one or two. That makes testing responsive design difficult, Parcell said. To help with that, the DigitalGov team started a Federal CrowdSource Mobile Testing program. Through it, feds can volunteer to evaluate an application on a variety of devices.

Looking ahead, the government is well positioned to be more proactive with mobility, Roberts said.

"We've got a lot of security coming in. We're not facing a midterm election, the budget situation is relatively stable, we're not facing a presidential election, so I do think we're going to have a pretty successful year when it comes to mobile," he said.

Although agencies fell short of the digital strategy's goals in many ways, it's still a useful document, Parcell said.

"I think the good thing about deadlines is they put you on course to actually meet a goal, but you also have to be rethinking those goals along the way," he said. •

DOE pilots big data infrastructure projects

BY GCN STAFF

Over the past few months, researchers at the Department of Energy have been exploring new approaches for collecting, moving, sharing and analyzing massive scientific datasets.

Researchers at Lawrence Berkeley National Laboratory recently led four science data pilot projects to show what could be gained when the facilities and tools were specifically linked to carry out specialized research and to show the potential of a highly focused science data infrastructure, according to DOE.

"As each new generation of instruments and supercomputers comes on line, we have to make sure that our scientists have the capabilities to get the science out of that data and [that] these projects illustrate the future directions," said Steven Binkley, director of DOE's Office of Advanced Scientific Computing Research.

All of the projects are researching new, more efficient technologies, and the goal is to reuse as many existing tools as possible and to develop new software as necessary, making it easier for the scientists to be able to examine their data in real time.

The first project demonstrated the ability to use a central scientific computing facility – National Energy Research Scientific Computing Center (NERSC) – to serve data from several experimental facilities in multiple formats using DOE's ultra fast ESnet. The teams built tools to transfer the data from each site to NERSC and to automatically or semi-automatically analyze and visualize the information.

The second project illustrated the concept known as a "super facility," which integrates multiple, complementary user facilities into a virtual facility offering fundamentally greater capability. This demonstrated for the first time that researchers will soon be able to analyze their samples during preliminary or "beamtime" tests and to adjust their experiment for the maximum scientific results.

In the third project, the teams built a "data pipeline" for moving and processing observational data from the Dark Energy Survey. Using Docker virtual machine software that automates deployment of applications inside software containers, they built self-contained packages that included all the necessary applications for analysis.

The containers could then be pushed out from to supercomputers at the national labs and fired up on the various systems pulling the data that they needed for processing. Then the results were pushed back to NCSA over ESnet.

The fourth project, the virtual data facility, was a multi-lab effort to create a proof of concept for some of the common challenges encountered across domains, including authentication, data replication, and a framework for building user interfaces. Data endpoints were set up at Argonne, Brookhaven, Lawrence Berkeley, Oak Ridge and Pacific Northwest labs, and the service demonstrated datasets being replicated automatically from one site to the other four.

Science teams across the DOE laboratory system are increasingly dependent on the ability to efficiently capture and integrate large volumes of data that often require computational and data services across multiple facilities. These projects demonstrate the scientific potential of big data infrastructure. •

How to avoid the coming 'dark age' for digital records

A leading light of the Internet is worried that the time is rapidly approaching when email, photos, documents and other digital relics may be lost to history because the tools needed to view them are becoming obsolete.

Vint Cerf, a Google vice president who is credited with nursing Internet development from its beginnings as a defense research project, said we risk entering a "dark age," when digital objects could become lost because software needed to access them no longer exists.

In a recent talk at the American Association for the Advancement of Science's annual meeting in San Jose, Cerf called for the development of "digital vellum," a way to maintain support for technology that could open original files regardless of their age.

"We don't want our digital lives to fade away," Cerf told the conference. "If we want to preserve them, we need to make sure that the digital objects we create today can still be rendered far into the future."

The cost of not addressing the issue would be painful, he warned. "When you think about the quantity of documentation from our daily lives that is captured in digital form, like our interactions by email, people's tweets and all of the World Wide Web, it's clear that we stand to lose an awful lot of our history."

Cerf is backing a plan to take an X-ray snapshot of the content, the application and operating system, together with a description of the machine that it runs on, and store the information in the cloud in perpetuity.

That snapshot "will recreate the past in the future," he said, by preserving both the data and technical specs necessary for future users to access the data and recreate the image.

"The key here is when you move those bits from one place to another, that you still know how to unpack them to correctly interpret the different parts. That is all achievable if we standardize the descriptions," Cerf said at the conference.

A version of Cerf's digital vellum has been tried at Carnegie Mellon University by Mahadev Satyanarayanan, a professor of computer science, with the support of IBM Corp.

The system, called Open Library of Images for Virtualized Execution or OLIVE, aims to preserve digital information as executable content, by "freezing" and reproducing the execution state that generates the information, according to a report on NewsFactor.

Using OLIVE, researchers have already archived the Mystery House, the original 1982 graphic adventure game for the Apple II, an early version of WordPerfect and Doom, the original 1993 first-person shooter game. •

Warehouse fire raises questions about perishable public records

A seven-alarm fire that wreaked havoc in a New York City warehouse holding paper records for the city, New York state and a variety of commercial firms is raising important questions for records managers.

Besides the loss of the paper records, those strolling close to the warehouse could spot private information of individuals in the fire's debris, which included medical records, court transcripts, lawyers' letters, sonograms and bank checks the CitiStorage Company kept, according to a New York Times report.

Various municipal agencies housed their records in the CitiStorage facility. Such records included confidential information such as Social Security numbers and sensitive medical information one might find useful for stealing the identities of others.

In a release on CitiStorage's homepage, the company assured customers that teams had been dispatched to the site of the fire to retrieve the sensitive documents. CitiStorage also maintained that an on-site incident command center was established after first responders arrived and that a significant number of documents had been recovered and accounted for.

"As an early adopter of electronic medical records systems, HHC keeps duplicates of vital patient records in electronic form, and we do not anticipate this will affect our operations," said a spokesman for Health and Hospitals Corporation, which said it housed only older records at the warehouse.

Additionally, the warehouse fire ignited fears of identity theft and data breaches in which hackers might now be able to infiltrate a database to gain even more personal information.

– Mark Pomerleau

Besides the loss of paper records, those close to the warehouse could spot other private information in the fire's debris.

AP IMAGES

Is Your Agency's Data Safe from Mutating Threats?

Over the past few years, malware has rapidly evolved from broader threats to more targeted attacks. To keep pace, your agency needs to move beyond simple antivirus protection. Symantec Endpoint Protection brings enhanced security, blazing performance, and smarter management to provide protection that blocks mutating threats. With over 20 years of experience developing Information Assurance solutions for the Federal Government, Technica Corporation can customize a solution for your agency that is both FISMA compliant and works with your legacy security infrastructure. And as a prime contractor on the DHS CDM-CMaaS BPA, we can help you navigate the often complex government buying process.

To find out more, visit our website: **technicacorp.com/CMaaS**

Symantec™ DHS CDM MaaS BPA Technica®

New Jersey opens regional Real Time Crime Center

BY KATHLEEN HICKEY

New Jersey officials recently opened a regional information-sharing center that will allow state and local law enforcement agencies to access technology and information, with the ultimate goal of reducing crimes and improving the quality of life in Newark and surrounding communities.

The Corr-Stat Real Time Crime Center (RTCC), launched in Newark in December 2014, "increases the response, analysis and support police officers need at crime scenes," according to a blog from the Office of the Director of National Intelligence's Information Sharing Environment (ISE).

Its mission is to develop a network that will gather, receive, analyze and distribute real-time tactical intelligence and support to law enforcement agencies operating within the Corr-Stat Region, which represents more than 80 cities along the Route 21 Corridor of Northeast New Jersey, from Jersey City to Paterson, and including Newark.

Housed at the Newark Police Department headquarters, RTCC will function as part of a broader information-sharing initiative among the New Jersey Regional Operations Intelligence Center, the Newark Police Department and other law enforcement agencies.

RTCC will allow investigators to access and analyze data from a range of agencies through a single portal. With a unified data access point, users will more readily "find connections between the all crimes suspicious activity reports, other data such as arrests, shootings, carjackings and incident information," noted a fact sheet from the Division of Criminal Justice, New Jersey State Police.

RTCC's technology was created from equipment already owned by various local law enforcement agencies, said officials at the unveiling, some of which was acquired for last year's Super Bowl and other major events.

They used tools such as GitHub-based Project Interoperability, a start-up guide for information interoperability for government employees, and the National Information Exchange Model, a standards-based approach to exchanging information, according to ISE.

New Jersey chose Newark as RTCC's base because a disproportionate amount of crimes, including 20 percent of burglaries across the entire state, are committed in the Corr-Stat Region, according to the fact sheet.

The RTCC technology is part of a broader information-sharing initiative among the New Jersey Regional Operations Intelligence Center, the Newark Police Department and other law enforcement agencies, according to an announcement to the media of the launch.

"RTCC will save money, allow for enhanced use of technology and equipment (both at the state and local levels) and support the regional partnership of state, county and local law enforcement agencies."

Prior to RTCC, there was no automated or formalized way to capture, analyze and share information on criminal activities or suspicious behavior across New Jersey, limiting an investigator's access to data and ability to identify patterns and trends in criminal activity.

"Bad guys aren't hindered by jurisdictional boundaries. They're not hindered by information silos. They don't hoard information. Actually quite the opposite, they love to brag about what they do," Newark Police Chief Anthony Campos told NJ.com. "So why were we always? You know what? We no longer are."

"This is going to be the first time in this country that we're looking at crime as a region," said Col. Rick Fuentes of the State Police. Officials are in talks to expand the collaboration initiative to New York, added Fuentes.

The Smart Policing Initiative, a Bureau of Justice Assistance-sponsored initiative supporting law enforcement agencies in building evidence-based, data-driven law enforcement tactics, has provided funding to 30 law enforcement agencies to help them with their technology initiatives. •

Housed at the Newark Police Department, RTCC will function as part of a broader information sharing initiative with New Jersey law enforcement agencies.

NASCIO MIDYEAR2015

#NASCIO15

ARE YOU READY?

Disruptive Change is the New Norm

April 26-29, 2015 **Alexandria, Virginia**

Network with State Chief Information Officers this spring!

Join state, federal and local CIOs for the 2015 Midyear Conference. NASCIO conference attendees include the highest-profile government and corporate technology experts in the nation. In addition to state, federal and local CIOs and corporate partners, past conference attendees have included governors, state and federal legislators, and other elected and appointed officials.

NASCIO is the premier network and resource for state CIOs and a leading advocate for technology policy at all levels of government.

Visit *www.NASCIO.org* to learn more about the conference and to review sponsorship opportunities.

NGA sets up geospatial intell portal on Amazon cloud

BY GCN STAFF

The National Geospatial-Intelligence Agency (NGA), Lockheed Martin and Esri have deployed software to the Amazon Web Services Commercial Cloud Services (C2S) environment, a move that will help agencies more freely share and analyze geospatial intelligence worldwide.

The move creates a portal for Esri's ArcGIS geographic information system that will provide a single, secure environment via the cloud for analysts throughout the intelligence community to organize and share geospatial data.

ArcGIS offers a range of tools and applications that let users link to geographic information data to assemble and share maps.

The companies involved called the development a "foundational step in consolidating multiple geospatial intelligence portals into the single NGA-provided portal, resulting in technology and license cost savings."

"This cloud implementation also further shapes the government's processes for architecting and implementing enterprise-class services within a cloud environment," said Jason O'Connor, vice president of analysis and mission solutions for Lockheed.

The move creates a portal for Ersi's ArcGIS geographic information system that will provide a single, secure environment via the cloud.

Esri President Jack Dangermond said the move underscores the importance of "consolidating geospatial intelligence information via a single portal to facilitate rapid situational awareness and response by our intelligence community."

The move to set up a GIS portal on the cloud comes on the heels of the NGA's move last fall to work with Lockheed to move its Map of the World to the Amazon C2S environment.

The Map of the World is an interface for geospatial intelligence data, designed to explore continuously updated content and link geospatial features to intelligence observations, according to NGA.

Lockheed Martin and Esri have also partnered for the last eight years on the Geospatial-Intelligence Visualization Services (GVS) program, which helped NGA and the intelligence community accomplish the cloud migration.

The Total Application Services for Enterprise Requirements GVS contract vehicle, originally awarded in 2012, offers geospatial visualization context and analytic capabilities to intelligence officers and policy-makers through classified and unclassified networks. •

FHWA seeks no-cost cloud for transportation data

BY MARK POMERLEAU

The Federal Highway Administration has issued a request for information for developing a streamlined, one-stop shop that would open up its transportation datasets for broad analysis and economic development by commercial and other government groups.

One option being considered is the use of no-cost agreements wherein the data hosting company could create and charge for value-added services.

The cloud-based repository would open the agency's vast holdings of information on road and bridge inventories, travel and operational data, system user data, fiscal data and pavement research, all of which the FHWA says provide economic value and promote environmental awareness.

Currently only a small percentage of FHWA's data is posted on public servers and websites. In many cases the data is hosted on multiple servers in various formats, making it difficult to find and integrate data from these sources for analysis and decision-making.

Additionally, the FHWA's large datasets require users to have substantial network, storage and computing capabilities of their own in order to work with the data. FHWA wants to reduce the bulky government framework in order to make its information more readily available for integration into business applications.

Besides surveying industry for a suitable cloud hosting solution, FHWA is interested in the feasibility of collaborating with companies using no-cost agreements to make FHWA's data more publicly accessible and usable.

The idea calls for companies seeking to partner with FHWA to be responsible for funding the data shift to the cloud and costs related to their own technology infrastructure.

The FHWA data moved to the cloud is expected to remain free to the public in its original, unaltered form. And though the agency wants to move its data to the cloud, it would still retain and maintain a "reference copy" of data provided to industry partners.

In return, the hosting partner can establish and perhaps charge for new value-added services and products. Proposals are due by March 26. •

Software freezes devices that fall offline

BY GCN STAFF

In a time when cybersecurity is every day's front page news, a government employee's lost or missing device can be a nightmare for an agency IT manager. One way to control this scenario would be to "freeze" the device so that it would be unusable until reactivated by administrators.

Absolute Software Corp.'s Device Freeze Offline Policy enables this fix by letting IT managers set an automated freeze command for any device that remains offline for a specific period of time.

The policy is engaged each time a device disconnects from the network. When this occurs, a timer is activated in the device with a duration assigned by IT. If the time elapses before the device makes contact with the Absolute Monitoring Center, the device will automatically freeze and the IT department will be alerted.

The Device Freeze Offline Policy extends the security capabilities of the company's Computrace service – which allows IT administrators to remotely control and secure IT assets using a cloud-based interface – to devices that may be unassigned or misplaced, the firm said in an announcement.

That way, forgotten devices are secured even if they remain in a dormant state, satisfying corporate and regulatory concerns about data security and device usage.

The Device Freeze Offline Policy is easily customizable and allows IT managers to define a window of time that best supports their security requirements. To maintain oversight, a summary reporting function also provides details on every endpoint that has been frozen, allowing administrators to investigate each device, validate its status and unlock devices that are not at risk.

"Information security must be enforceable even when a device is not plugged in or powered up," said Geoff Haydon, CEO at Absolute Software. "With this policy, our customers can actively protect all of their devices – and the sensitive information they contain – regardless of Internet connection, user or location."

Device Freeze Offline Policy for Absolute Computrace is available now. •

SSA websites big winners in user satisfaction survey

BY KATHLEEN HICKEY

Thirty-one percent of federal government sites provide an excellent government experience for citizens, according to the ForeSee E-Government Satisfaction Index.

ForeSee, a customer experience analytics provider, gathered 220,000 survey responses across 100 federal government websites, as well as mobile sites and applications. The index, which quarterly measures citizen satisfaction with e-government, is now in its 12th year.

On a 100-point scale, average citizen satisfaction was slightly up in Q4 (75.1 points) from 75 in Q3. Scores 80 and above are ranked as having highly satisfied visitors. Below 70, sites are rated as having highly dissatisfied visitors. Interestingly, average citizen satisfaction with e-government substantially outscored citizen satisfaction with overall government, which was 64.4, according to the American Customer Satisfaction Index Federal Government Report.

The Social Security Administration's Extra Help with Medicare Prescription Drug Plan Costs site was the top performer (90) and outscored some of the top private-sector sites such as Amazon (83), L.L. Bean (82) and Apple (80), according to the Answers Experience Index: 2014 Retail Edition.

Only 31 sites achieved an excellent rating. The lowest ranked site was the Department of Veterans Affairs' main website – va.gov (56).

The most improved site was the Internal Revenue Service's main site, IRS.gov, which achieved a citizen satisfaction score of 72 in Q4 – a 15 point increase from Q3. The most likely driver, according to ForeSee, was Direct Pay, which allows citizens to pay taxes directly from a checking or savings account at no additional cost.

On the downside, satisfaction with mobile sites and apps decreased. Aggregate satisfaction was 77 in Q4, down from 78 in Q3.

"In order to help improve the citizen experience on mobile websites and applications, government agencies need to prioritize several areas of focus regarding their mobile offerings," said Dave Lewan, vice president of ForeSee. The top priority should be navigation, followed by look and feel of site information, he said.

ForeSee further divided site rankings according to top gainers and site functions, including the Bureau of Economic Analysis, NIH's Senior Health and DOD's Tricare.mil.

"Why does satisfaction matter? If agencies can deliver a satisfactory experience, the likelihood of desired outcomes is increased," said Lewan. "For example, for this quarter's index, highly satisfied website visitors were 83 percent more likely to use the website as a primary resource (versus a more costly channel like the contact center) and 80 percent were more likely to put their trust behind the agency. "

"For mobile, those who were highly satisfied with their experience were 85 percent more likely to return to the site or app and a whopping 118 percent more likely to recommend the site or app!" he added.

Navigation, search, functionality and online transparency are driving satisfaction, said Lewan. "It's important to note that online transparency (providing thorough, easy-to-find information on a site) has been proven to be a driver of increased trust in the agency," he added. •

Top 10 agency sites

Of the top ranked sites, five of the top 10 were from SSA. Here are the top 10 sites, from highest to lowest score.

1. SSA's Extra Help with Medicare Prescription Drug Plan Costs (90)
2. SSA's Retirement Estimator (89)
3. National Institutes of Health Senior Health (88)
4. SSA's Social Security Business Services Online (88)
5. My Social Security (88)
6. SSA iClaim (88)
7. Health and Human Services MedlinePlus (87)
8. HHS MedlinePlus in espanol (87)
9. U.S. Citizenship and Immigration Services Espanol (87)
10. American Battle Monuments Commission (85)

'Spark' triggers the next stage of near-real-time big data

BY BRIAN ROBINSON

With the "next big thing" in IT there inevitably comes a time when user experience falls short of the hype. So it is with big data and its promise of fast and precise analysis of huge volumes of distributed data.

In the current big data universe, Hadoop is the software used to store and distribute large amounts of data and MapReduce is the engine used to process it. The combination has proven itself in non-time-critical batch processing of data.

But what about analysis of near-real-time big data?

Apache Spark, the most advanced of these next-generation, open-source technologies, sets the stage for analysis of streaming data from video, sensors and transactions.

Like MapReduce it can be used for batch processing, but for those algorithms that perform a number of interactions on a dataset, Spark can store the intermediate results of those actions in cache memory. MapReduce, in contrast, has to write the result of each action to disk before it can be brought back into the system for further processing.

That rapid in-memory processing of resilient distributed datasets (RDDs) is the "core capability" of Apache Spark.

"Once operations are done (on the datasets) they can be streamed and connected to each other so that transformations can be made very quickly," said Dave Vennergrund, director of predictive analytics for Salient Federal Solutions, which is working on developing analytics products for government organizations using Spark.

"Couple that with the ability to do this across many machines at the same time, and you have a recipe for a very strong response," he added.

Proponents of Spark claim both scale and speed advantages for the Apache tool compared to its competitors. It's been shown to work well for small datasets up to volumes measuring in the petabytes.

A November 2014 benchmark contest had Apache Spark sorting 100 terabytes of data three times faster than Hadoop MapReduce, on a machine cluster one-tenth of the size of that used for the MapReduce sort.

A recent survey by Typesafe, a software developer, showed a rising level of interest by organizations in using Spark.

Only 13 percent were currently using it, but more than 30 percent were evaluating it, 20 percent of the respondents were planning to begin using it sometime this year, and another 6 percent expected to use it in 2016 or later. However, 28 percent of those surveyed had no knowledge of Spark, which emphasizes its still "bleeding edge" status.

For the government space, "testing and evaluation is where it's at right now," said Cindy Walker, vice president of Salient's Data Analytics Center of Excellence. Agencies that have "sandboxes and R&D budgets" are the early adopters, she said.

"Many of our customers aren't yet signing on the bottom line to implement big data, in-memory analytics, streaming solutions," she said. "So, at this time, we are using Spark to help guide them to what they can expect once they get to that point."

So while Spark won't be a replacement for MapReduce, it will eventually claim a section of the big data analytics spectrum devoted to speedy data processing, according to analysts. •

What's in the Apache Spark ecosystem?

The Apache Spark ecosystem comprises several integrated components:

- **Spark Core,** the underlying execution engine for the platform, supports a range of applications, as well as Java, Scala and Python application programming interfaces.
- **Spark SQL** (Structured Query Language) allows users to explore data.
- **Spark Streaming** enables analysis of streaming data from sources such as Twitter. This is in addition to Spark's ability to also do batch processing.
- **Machine Learning Library (MLlib),** a distributed machine learning framework, delivers high-quality algorithms up to 100 times faster than MapReduce.
- **Graph X** helps users build and manipulate graph-based representations of text and tabular data to find various relationships within the data.
- **SparkR,** is a package for the R statistical language with which R users can use Spark functionality from within the R shell.

SNAPSHOT

CONVERGED INFRASTRUCTURE

HyperConvergence: The Next Wave of Convergence

When agencies need to spin up a new application, start a new project or simplify the infrastructure at a branch office, some are turning to a converged infrastructure instead of traditional data center resources. Doing so can simplify management, improve efficiency and lower costs.

There are times, however, when even a converged infrastructure isn't enough—not enough performance, automation or integration. In those cases, there is another, related option: the hyper-converged infrastructure. While converged infrastructure provides integrated compute, storage and networking components designed to work together, the components often come from different vendors. Converged infrastructure also doesn't include a hypervisor or software-defined storage. A hyper-converged infrastructure provides compute, networking and storage from one vendor, full pre-tested and configured for the intended workload. It includes the hypervisor, and uses software to eliminate the need for external storage.

Inclusion of the hypervisor is critical, because it sits between the underlying infrastructure and the applications. That means that it can abstract all underlying resources—a major key to efficiency.

Hyper-converged infrastructures are built to specifications and shipped as a single unit. For example, an agency that needs to spin up 500 Microsoft Exchange users would be able to choose a pre-configured, pre-tested hyper-converged infrastructure designed to do exactly that. All they would have to do is plug it, and it would be ready for use. If more users needed Exchange, an agency could simply buy another module for the system.

The hyper-converged infrastructure provides excellent performance and convenience for the price. It can track which data belongs to which virtual machine, making it much easier to move virtual machines around. It also eliminates redundant read and write operations; routinely includes deduplication, compression and data optimization; and takes automation to a new level. This further reduces labor-intensive activities and prevents over-provisioning and over-purchasing.

There are other benefits to the hyper-converged infrastructure. With less physical hardware in the data center, power and cooling costs are reduced, and IT staffs don't have to spend as much time on maintenance, patches and troubleshooting. Performance tends to be higher because the components are so tightly integrated and tested. Because the storage is fully integrated, for example, there tends to be less latency. Since the networking also is integrated, there are fewer bottlenecks and better throughput. It's also much easier to scale the infrastructure because of the building-block approach.

One example of a hyper-converged infrastructure is VMware's new EVO line, consisting of EVO:RAIL for branch offices, VDI deployments or workloads like test and development; and EVO:RACK for large deployments. Both are preconfigured, pre-integrated infrastructure stacks available from vendors like Dell, Hitachi Data Systems, HP and NetApp. Both EVO:RAIL and EVO:RACK use vSphere, along with vSAN and local-attached storage. •

Other Converged Infrastructure Report Articles:

- When Moving to a Converged Infrastructure Makes Sense
- Making the Most of Convergence
- The Business Case for Converged Infrastructure
- The Data Center of the Future

FULL REPORT ONLINE
Go to GCN.com/2015CONVERGED INFRASTRUCTURE

vmware®

Cut storage costs up to 50% and improve performance.

VMware® Virtual SAN™

Radically simple Software-Defined Storage

To learn more about Virtual SAN, visit
vmware.com/products/virtual-san

NEW ERA.
NEW THINKING.

BY BRIAN ROBINSON

Cyber info sharing: More noise than signal?

THE NEED FOR timely sharing of information about both potential and actual attacks has been considered a prime focus for government and industry cybersecurity for at least the past decade. The 911/Commission Report first brought to light the lack of intell sharing among agencies, for example, and that lack was seen extending into the cybersecurity realm.

The language used in the report, though aimed at terrorism, speaks as much to the problems surrounding cybersecurity today. The events of 9/11 showed "an enemy who is sophisticated, patient, disciplined, and lethal," and also the "fault lines within our government (and the) pervasive problems of managing and sharing information across a large and unwieldy government."

The Obama administration's most recent push to improve U.S. cybersecurity tries to ratchet up efforts to boost information sharing both within government and with the private sector. Shortly after, the administration announced the formation of a new Cyber Threat Intelligence Integration Center that's intended to be the government's focus for rapid collection and dissemination of information on cyberthreats.

How far this will go is an open question. While some have welcomed the new proposals, others wonder if the new center will just add to the organizational confusion. The National Security Agency, the Department of Homeland Security, the FBI and the military already have responsibility for collecting this kind of information, and after years of acrimony and pushback, they've managed to develop cohesion about sharing it.

Technically, the tools for sharing have also progressed, leading to a number of acronymic specs such as TAXII (the Trusted Automated eXchange of Indicator Information), STIX (the Structured Threat Information eXpression) and the Cyber Observable eXpression (cybOX). Joining them recently is the Data Aggregation Reference Architecture (DARA), a first response to the 2012 National Strategy for Information Sharing and Safeguarding.

These and other tools all perform important roles. DARA, for example, is aimed at providing a model for how various groups can pull data sets together in order to improve security while also protecting individual privacy, which has been one of the big stumbling blocks to sharing of information.

But is all of this enough? If 2014 showed anything, it's that cybersecurity efforts are falling behind the speed and the level of sophistication attackers apply to the way they get threats into the cyber infrastructure. President Obama in fact mentioned the attack on Sony Pictures late last year as just the latest reason behind his new legislative proposals.

Industry looks to the government for a lead on many aspects of cybersecurity, but the fact is that government is not noted for its speed in dealing with cyber threats or for convincing industry to share information about attacks with it. However, it is trying. The FBI, for example, released an unclassified version of its Binary Analysis Characterization and Storage System (BACSS) as an additional incentive to public/private sharing.

BACSS is an automated malware analysis system used by the FBI enterprise-wide that can link cases where instances of the same malware are present.

Now industry seems to be expanding its own efforts to improve sharing. Facebook has launched a framework for "importing information about [threats] on the Internet in arbitrary formats, storing it efficiently, and making it accessible for both real-time defensive systems and long-term analysis." Early partners already include Bitly, Dropbox, Pinterest, Tumblr, Twitter and Yahoo.

Microsoft last year also introduced Interflow, its own attempt to collaborate more closely with the cybersecurity community. Interflow is a distributed system that enables users to form communities to decide what information to share and with whom. That adds to a number of other international collection and sharing efforts, as well as the global infrastructures that individual security companies have established to collect information about threats.

There are still major barriers to sharing, particularly privacy and the need for encryption. How government manages to live within, and profit from, this growing sharing ecosystem while improving how fast it reacts to threats is the real question it has to address. •

How government manages to live within this growing data-sharing ecosystem while improving how fast it reacts to threats is the real question it has to address.

INDUSTRY INSIGHT

BY PATRICK D. HOWARD

CDM phase 2: how to avoid déjà vu all over again

YOU DON'T GET many do-overs in life, but if you did – like Bill Murray in the movie Groundhog Day – what might you revisit? While I can't promise a life-changing replay, here's food for thought as it relates to the Homeland Security Department's Continuous Diagnostics and Mitigation Program (CDM).

The program, begun in 2013, was divided into three implementation phases, with the next Phase 2 devoted to various identity and access management services. So, as we round the quarter rail with CDM, agencies may want to consider how Phase I unfolded and what they can do differently or better in preparing for Phase 2.

When we look back to 2013, there were valuable lessons learned as Phase 1 began with a requirements definition process. At the time, agencies were asked to assess their capabilities and identify deficiencies or gaps that the Department of Homeland Security could then help them fill through its CDM/Continuous Monitoring as a Service (CMaaS) blanket purchase agreement.

But back then perhaps the concepts of CDM weren't as clearly understood as they are now. Or maybe assessments weren't conducted agencywide or weren't performed by those with the right skillsets.

In fact, a 2014 survey by the SANS Institute found that only 21 percent of government-focused IT professionals had conducted a formal foundational assessment before starting the program. Considering you can only improve security by knowing your baseline and where the holes are, this indicates that many groups may need to go back and conduct additional preparation work prior to starting Phase 2.

Soon it will be déjà vu all over again, requiring an assessment process be repeated for Phase 2. This time, the assessment will be for a set of requirements that include: management of network access controls, people granted access, security-related behavior, credentials and authentication.

To help agencies ensure their Phase 2 needs are thoroughly and accurately identified, here are four key recommendations:

Get the right people involved. The process of determining whether Phase 2 requirements are being met should include all those with a relevant perspective on agencywide business needs. Rather than being performed by just one person or limited to one component, it should involve IT operations, affected business units, security compliance, legal, human resources and privacy specialists.

Address the non-technical. When evaluating Phase 2 requirements, review your agency's personnel and the skills they'll need to deploy and operate CDM tools, along with any training that will be required. Personnel processes that need to change should also be reflected in the policies and procedures that support them.

Use what works. Look for pockets of excellence that can be leveraged, and identify gaps that can be closed in-house. For example, there may be an identity management solution that's working well elsewhere within the agency that can be used enterprisewide, eliminating the need to procure a duplicate. By evaluating the tools or products it already owns, an agency may also uncover capabilities that simply aren't being used. It may be just a matter of activating or licensing additional features or modules, without deploying an entirely new solution that would demand more funding or retraining.

Continue to evaluate gaps. Considering that change is a constant, other gaps may arise and their priority may shift. Just because the initial task of identifying Phase 2 gaps has been successful does not mean the work is done. Ongoing risk management means bringing a CDM strategy to life, not just dusting it off once a year for the Inspector General.

> Performing a foundational assessment is not only the best way to avoid the déjà vu of previous mistakes, it's also the essential first step for improving security through CDM.

Performing a proper foundational assessment is not only the best way to avoid the déjà vu of previous mistakes, it's also the essential first step for improving security through CDM.

While the CDM program offers great promise and benefits, there will be challenges along the way. But there's no need to go it alone. Agencies without the necessary expertise or resources can rely on the CDM/CMaaS program for help. The BPA holders selected by DHS are experienced in assessing Phase 1 and Phase 2 requirements, recommending mitigation strategies and implementing capabilities. •

— Patrick D. Howard is program manager for CDM and CMaaS for Kratos SecureInfo.

INDUSTRY INSIGHT

BY ALEX STEIN

How dynamic case management can modernize citizen services

GOVERNMENT CIOS are under a lot of pressure to raise their standard of service, and not just from constituents brandishing smartphones.

President Obama's 2011 Executive Order specifically urged agencies to advance into the digital age by offering "popular lower-cost, self-service options accessed by the Internet or mobile phone and improved processes that deliver services faster and more responsively, reducing the overall need for customer inquiries and complaints."

Budget restraints create another strain – the relentless push to do more with less. CIOs know that major infrastructure overhauls are too slow, costly and fraught with risk. They are looking for easily deployed solutions that will adapt to frequent changes in politics, business and technology.

Cloud-based platforms require less intensive development resources, and software-as-a-service offerings can be updated and expanded incrementally. The ability to test upgrades and new processes without disrupting the course of business is essential to government agencies, most of which provide critical services to large populations.

Dynamic case management (DCM) solutions built on cloud-based platforms can create viable opportunities for government agencies to catch up in these areas.

DCM enables a unified, holistic and real-time view of case progress, agent workflow and performance metrics. Informed by business rules, case management processes can be customized to the particular type of service or investigation. Forms and documentation are integrated into workflow, intelligent decisions automated and casework routed efficiently. Tracking metrics helps managers by highlighting bottlenecks, service gaps and underperforming employees. Predictive analytics likewise detects areas of risk and aids longer-term planning.

> "DCM solutions give knowledge workers flexibility, allowing them easier access to research, documentation and case history tools."

Meeting citizen service requests and expectations and overcoming bureaucratic limitations are primary challenges for public-facing agencies and can be quickly and efficiently addressed with scalable, pay-as-you-go DCM solutions.

Meeting citizen expectations in a digital world

The combination of mobile devices and sophisticated business-to-citizen digital services has affected customer expectations well beyond retail. Citizens increasingly see themselves as government's customers and are frustrated by the lack of responsiveness and accessibility they encounter. They want to communicate online via interactive web sites, mobile apps, email and text alerts.

Moreover, they expect consistency across all these channels. They want to be able to access their case histories and rely on agencies to track their interactions. The bottom line is that everyone wants faster resolution of inquiries and complaints. Opening up more online and self-service communication channels should relieve burdens on understaffed call centers and promote accuracy and accessibility.

Knowledge workers in government agencies are just as exasperated as the citizen-customers they aim to serve. They don't have the tools they need to make decisions and deliver results. The information they need is stuck in silos, barricaded by aging systems that don't play well together and are rarely connected to external sources.

DCM solutions give the modern knowledge workers mobility and flexibility, allowing them easier access to tools such as research, documentation, forms and case histories. These solutions, unlike traditional systems of record, can help agents handle structured, unstructured and unexpected work.

Predictive analytics, business rules and collaborative tools improve contextual, data-driven decision-making, optimize productivity and inform better employee training. Public sector knowledge workers empowered by DCM tools to better address constituent needs are likely to be more satisfied with their jobs. And improved workplace morale feeds back into more positive interactions with the public and lower turnover, which leads to significant cost savings.

The digital era brings with it an unprecedented amount of data in a dizzying array of formats. Data can't just be collected, stored and retrieved; it requires indexing, integrating, searching, analyzing and sharing, all while adhering to privacy and security regulations. DCM can help agencies move toward end-to-end digitalization.

Social, mobile, cloud and data technologies open up a whole new world to agencies often limited by bureaucratic challenges. Gartner calls this convergence of digital powers the Nexus of Forces, and it is already driving innovation in government, especially at the municipal level. As government IT reinvents itself, DCM solutions will play a powerful role in establishing more interactive and productive relationships with the public. •

— Alex Stein is founder and chief strategy officer for Eccentex Inc.

GCN

Technology,
Tools and Tactics
for Public Sector IT

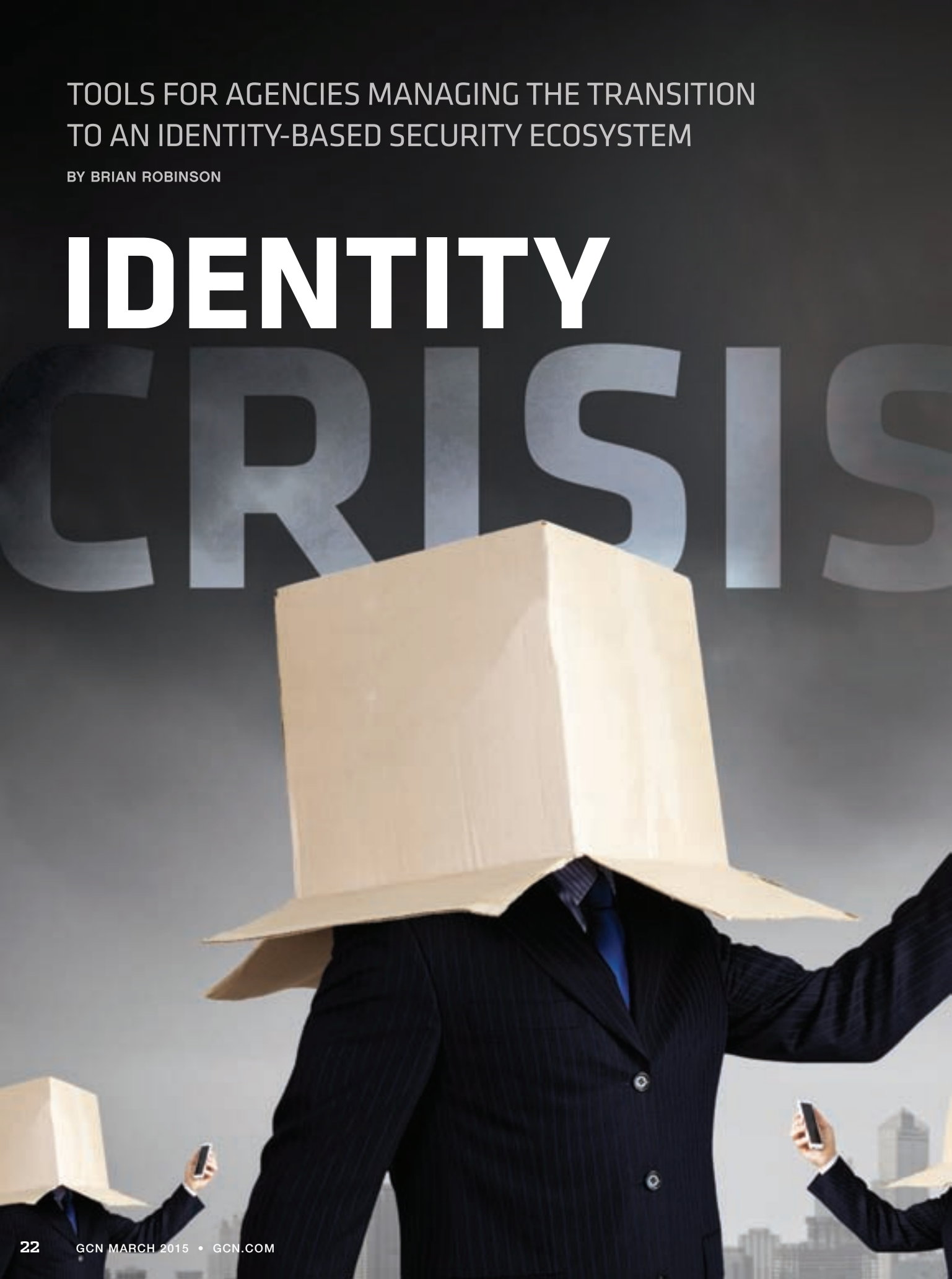
Where you need us most.

Mobile **Tablet** **Desktop** **Print**

TOOLS FOR AGENCIES MANAGING THE TRANSITION TO AN IDENTITY-BASED SECURITY ECOSYSTEM

BY BRIAN ROBINSON

IDENTITY CRISIS



For most of the history of the Internet, security has meant stopping attackers from breaching the walls surrounding networks and computer systems. While that's still important, identity systems – and the electronic formats for managing them – have become the top priority for organizations looking to safeguard the government data attackers now target.

Homeland Security Presidential Directive-12, put into action in 2005, is the basic policy underlying the use of security credentials in the federal government. The Obama administration took that a step further in April 2011, with the release of the National Strategy for Trusted Identities in Cyberspace (NSTIC), which set a focus on public/private collaboration to "raise the level of trust" associated with online identities.

Following a rash of high-profile data breaches in the both the public and private sector in 2014, the Obama administration has raised the pressure even more. In October it issued an executive order aimed at cutting down on identity-related crimes and directed various agencies by the beginning of this year to start issuing credentials with stronger security.

The government "must further strengthen the security of consumer data and encourage the adoption of enhanced safeguards nationwide in a manner that protects privacy and confidentiality while maintaining an efficient and innovative financial system," Obama said.

Even before the release of the order, the market had been responding to this need by providing multi-factor authentication that has stopped many common types of attacks, according to Jeremy Grant, the senior executive for identity management at the National Institute of Standards and Technology. Grant also heads the NSTIC National Program Office.

"Through more than a dozen NSTIC pilots, the private sector has demonstrated material progress in advancing more secure, privacy-enhancing, easy-to-use identity solutions," he said in a recent blog post. "It's time for the government to make sure our own services are embracing the best the market now has to offer."

Government agencies at least now understand the need to become more data-centric in how they look at security, said Jerry Irvine, chief information officer at Prescient Solutions and a member of the National Cyber Security Task Force.

The use of data-supported security has become more urgent even though traditional forms of perimeter-based security such as firewalls, intrusion detection systems and virus detection continue to be the most common solutions currently used, according to Irvine.

What's more, mobile phone proliferation has exposed agencies to a steady shifting of vulnerability across their networks.

"Firewalls look like so much swiss cheese these days because there are so many open ports and types of applications that people are allowed to access from their mobile phones and other devices and through the Internet," said Irvine.

"Now it's become a matter of seeing how you can better secure data with … protocol protection, access control rights and data loss prevention applications," he said. And managing the identities and security credentials needed for that is no small project.

For one thing, each agency has its own needs when it comes to security and the level of information assurance it can apply to its data.

For example, military and intelligence agencies will have different requirements from the National Oceanic and Atmospheric Administration.

The idea of what identity actually means within an agency may also change over time, said Jill Canetta, public sector vice president for Experian, a global data analytics company.

"It's no longer just about being able to prove the identity of an individual, but also what attributes are needed for that," she said. "We are also seeing an evolution from identity proofing to identity relationship management, as there is more of a need to see how a particular identity and the relationships its had with various devices and other things that are also assigned identities on a network have changed."

> Following a rash of high-profile data breaches in the both the public and private sector in 2014, the Obama administration has raised the pressure even more.

Mobile is proving to be a particularly thorny ID management challenge, given the explosion of smartphones and other mobile devices in government. It's also not an easy one to fix, according to mobile security experts.

The way government employees and contractors use their personal identity verification (PIV) cards to log on to desktop systems, for example, is not readily transferable to the mobile arena. Desktop users normally put their cards into a reader on the computer and leave it there, so having to take it out for use with mobile card readers is an ongoing ergonomic challenge.

NIST's release of special publication 800-157 in December of last year, which describes technical details by which PIV credentials can be provisioned on mobile devices in lieu of a physical smart card, could go a long way to solving the problem.

While it may take a while for the derived PIV credentials to make their way into products, they are already prompting changes.

"The guidance has helped move some projects from pilot to development," said Paul Nelson, chief technology officer for Thursby Software Systems, a government IT integrator. "The trick is how to provision devices with necessary certificates," he said. "The [National Security Agency] thinks it can make it work, and the DOD supposedly has an aggressive schedule where they want to get something out by July of this year."

In fact, this could be the year when the government smart card reader market dries up, according to Nelson.

"If the government is not willing to commit to readers as its credential authentication solution in significant numbers, "then there's going to be no reason for us to continue making them," he said. Mobile authentication will, by default, then become a software-based solution.

Meanwhile, other identity-based security problems that must be grappled with are piling up across the government security community.

So-called insider threats, where data and systems are compromised – by willful theft or employee error – are becoming a major problem, for which the Edward Snowden and Wikileaks breaches are just the most notorious examples.

Inside attackers are becoming much more sophisticated in how they do their work, increasingly targeting the theft of security credentials themselves.

And despite such measures as SP 800-157 and NSTIC, there are still "fundamental questions about whether we have the technologies we need, and whether they will work on the scale we intend, to be able to do such things as identity-driven encryption," said Mark Cohn, chief technology officer of Unisys Federal Systems, who contributed to the technical basis for NSTIC.

"I would hope that, by the end of this decade, we will wrestle these issues to the ground, but I'm not optimistic that we know yet exactly how we are going to do that," he said.

That hasn't stopped federal and industry efforts to develop solutions to at least some of these problems, however. The programs and products listed here represent some of the more far-thinking attempts to address the pressing identity issues, and the resulting security concerns, associated with weak passwords, the proliferation of mobile devices connecting to networks and the dangers posed by employee data handling errors and theft.

Meanwhile, government agencies will have to rely on existing technology solutions – like those highlighted below – to help manage their ongoing and embryonic security threats. The following is set of solutions – a best of breed of sorts – of what's in the government's identity management arsenal for attacking some of its most pressing security threats.

CONNECT.GOV

A government federated identity management hub, overseen by the General Services Administration, started life several years ago as the Federal Cloud Credential Exchange, but became Connect.gov in late 2014. It allows personnel verified through the hub's sign-in partners – including Verizon, ID.me, Google, Paypal and Yahoo – to use one set of digital credentials for accessing a range of both commercial and public sector sites. The exchange itself doesn't validate identities, leaving that up to its various partners.

Still classified as a pilot, it already has a number of federal agency participants, such as the Veterans Administration, the Postal Service, the Agriculture Department, NIST and others. High profile agencies such as the IRS have said they won't use the site for now, but hub officials expect a slew of other agencies to sign up for the service over the next two years.

Any credential users now have to access government sites or bank accounts could be used with Connect.gov, once it's been validated by one of the sign-in partners. Or users could create a new credential with a partner. That will help cut down on the "identity fatigue" users now suffer from handling numerous passwords, officials believe, which is fueling the bring-your-own-identity movement.

The end goal, according to Connect.gov Director Jennifer Kerber, is to have government agencies organize around one sign-in platform and move away from the siloed identity proofing they've relied on so far. The result will be government providing citizens and businesses with better data.

UNISYS STEALTH

The Unisys Stealth system is used to establish "secure communities of interest" within an enterprise, where only authorized users can access information. Its origin lies in the Defense Department, where multiple, physical networks were used to segregate information depending on it security classification.

However, that can be tough to manage when there can be 20 or more networks on a single ship or at one site. Having those logically rather than physically isolated makes them much easier to manage, plus it allows for faster support of operations when new physical networks don't have to be deployed or wires run to desktops.

In developing the platform, Unisys's Cohn said the company was looking at the requirements of cloud computing and how to protect and isolate customers' data in the cloud as needed.

The Stealth solution has a "light fingerprint" as it basically sits on top of existing IT infrastructure.

"It's essentially a packet filter that sits between layers two and three of the Internet stack," he said. "It examines the packet to see if it's intended for a particular community of interest, and, if the person logged on is not a member of that, it ignores it so it's not translated up the stack."

Stealth provides a way to do things that are identity related, and that isolates and protects information without a lot of administrative headaches, he said.

METALOGIX REPLICATOR CROSS DOMAIN EDITION

Metalogix developed the Replicator in concert with the Defense Information Systems Agency as a way of securely and automatically transferring content between SharePoint farms that sit on different networks and at different security levels. It can, for example, synchronize content between secret SIPRNet and sensitive but unclassified NIPRNet domains.

Replicator is aimed at stemming data leaks from insiders, much of which happens because of unintended or careless actions.

With deployed forces, whose commanders had to operate within their own organizations but also to cooperate with NATO and other forces, sharing information "was a hugely manual process," involving removable media, said retired Maj. Gen. Steven Smith, a former Army chief information security officer and now advisor with Metalogix.

That level of complexity inevitably led to mistakes from people who didn't follow procedures, he said, and that involved, "a lot of work" to clear the resulting data spill.

The Replicator tool works with existing data guards in place at organizations. Metadata tags in SharePoint indicate what other organizations and security levels it can be shared with. Sharing is also bidirectional so any changes are automatically pushed back to the originators of the information and others who have shared it.

EXPERIAN TRAP

Experian's Tax Return Analysis Platform is aimed at helping federal and state organizations combat tax fraud, though the basic technology can be used in circumstances that require identity verification and device proofing.

It has three main components:

A fraud and identity proofing platform that works with both public and private sources to authenticate a user remotely, in real time.

Knowledge-based authentication, which asks questions only the particular person being asked will know the answers to.

Fraudnet, a proofing tool that compares the device being used to file a tax return with a database of devices that are known to have been used in fraudulent activity.

Experian is using the same technology to service identity proofing systems for the Social Security Administration's online statement system and for the Centers for Medicaid and Medicare Services for identity proofing involved with the Affordable Care Act.

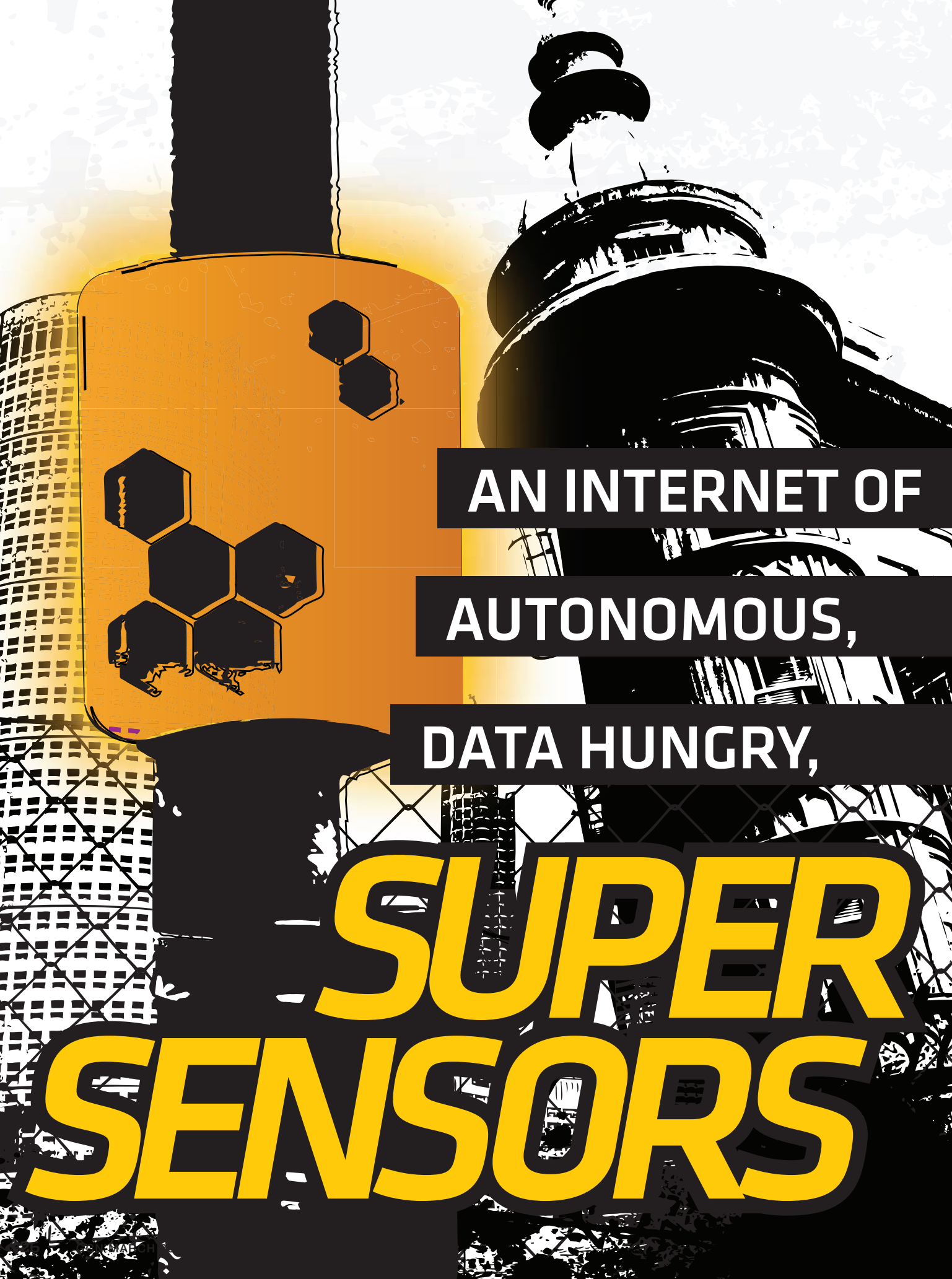
WAVE VIRTUAL SMART CARD

Wave Systems Corp.'s virtual smart card (VSC) is intended to replace the need for passwords or external tokens such as physical smart cards by using the Trusted Platform Module. The TPMs are security chips built into the motherboard of most current business-class computers with a full-featured Windows operating system.

The combination of a hardware-based root-of-trust provided by the VSC and the user's personal identification number (PIN) delivers strong two-factor authentication. The fact that it's a hardware solution both reduces much of the administrative overhead involved with software-based tokens as well as the cost of replacing lost physical tokens, according to the company.

"With around a fifth of physical tokens being lost each year, that's just a massive burden on the support infrastructure," said Greg Kazmierczak, Wave's chief technology officer.

The VSC hasn't been transitioned to other operating systems such as those for Android or Apple smartphones because a number of the specifications and capabilities are not yet mature enough, he said, unlike the market for Microsoft tablets, laptops and other devices. But they eventually will emerge, Kazmierczak said, helped along by NIST's recently published SP 800-157 mobile PIV guidelines. •



AN INTERNET OF AUTONOMOUS, DATA HUNGRY, SUPER SENSORS

The cities of Chicago and San Francisco are partnering with local national labs to develop a network of large, remote sensing platforms capable of gathering data on traffic congestion, air quality, buildings' energy consumption and the direction of gunshots on city streets.

BY PATRICK MARSHALL

Federal, state and local agencies are just now beginning to explore applications of the Internet of Things (IoT), which, despite its build-up as "the next big thing," seems destined to live up to the billing.

The IoT generally comprises networks of remote sensors capable of detecting everything from traffic to air quality, to buildings' energy consumption, to the direction of gunshots on city streets.

The Array of Things is a network of interactive, modular sensor boxes around Chicago collecting real-time data on the city's environment, infrastructure and activity for research and public use.

GOVERNMENT AGENCIES SEE PLENTY OF OPPORTUNITIES

The U.S. Postal Service, for example, has called on vendors to propose IoT projects that might make USPS operations more efficient and might also generate new products that can provide value for businesses, government and local communities.

The military is also interested. The Defense Information Systems Agency includes IoT on its list of important technologies to develop and declared in its strategic plan for 2014-2019 that "from improved logistics tracking to optimized building security and environmental controls to health monitoring of individual soldiers, the Internet of Things will impact everything we do."

Many of the most forwardly focused civilian agency projects are those participating in the second round of the SmartAmerica Challenge, called the Global City Teams Challenge, sponsored by the National Institute for Standards and Technology. The challenge is specifically aimed at encouraging collaboration and the development of standards for IoT projects.

But the real action in actually implementing IoT in a public sector environment is happening with a pair of federal research labs and the cities where they are based.

THE ARRAY OF THINGS

The Array of Things, a joint project of the Argonne National Laboratory, the University of Chicago and the city of Chicago, is considered ready to move from prototype to initial deployment.

While the project was initially aimed at monitoring air quality, said Charlie Catlett, team leader and senior computer scientist at Argonne, it is capable of much, much more.

Ultimately, sensors deployed around Chicago in the Array of Things will not only be able to monitor air quality block-by-block, but applications that tap into its data will be able to alert users to areas with traffic congestion, pedestrian traffic or even icy patches on sidewalks. City planners will also use the data to work on reducing vehicle emissions by controlling traffic flows.

According to Catlett, the first set of boxes being deployed – about the size of a briefcase and attached to light posts – are filled to capacity with 17 sensors, including those that measure temperature, humidity, light, carbon monoxide, nitrogen dioxide and vibration. The boxes also include a sound sensor and an infrared camera that can pick up surface temperatures.

"We had been working here at Argonne with remote sensing since 2005 or so," said Catlett. "We developed a remote sensing platform that is designed for sensors or cameras in locations where you can't easily get back there to fix things, so they have to be self-healing and very autonomous."

Catlett saw an opportunity to work with the city of Chicago to help both researchers and residents. "With the movement toward smart cities, a lot of research groups and companies will want to experiment with urban-scale technology where

you need to deploy something," he said.

"I suggested that if we could deploy a network of secure enclosures with power and Internet in Chicago then we could essentially host the development and prototyping and research associated with next-generation technologies." The city agreed to place and deliver power to 500 of the boxes produced by Catlett's team.

Even before fully deploying the first set of boxes, the team is preparing to expand the reach of the Array of Things.

"Right now we are in a six-month force march to be able to produce these things in quantity – going from handmade prototypes to mass-manufacturable design," said Catlett. "At last count, we have 11 other cities that expressed interest in them."

Eventually, the sensor boxes will be solar powered. And Catlett's team is working to make them smaller and more intelligent. "We want to be able to do as much data processing at the node as we can before we transmit data," he said. "Part of the strategy is to reduce the amount of communication you need. If you can process right and on the node you can actually get much more bang for your buck out of these kinds of sensors. That's where we are headed. We view this as a programmable device, not just a set of sensors to deploy."

According to Catlett, data collected by the Array of Things will be open to the public. Data will also be available through Plenar.io, a centralized hub for open datasets from around the world that was created by the Urban Center for Computation and Development, a joint project of Argonne and the University of Chicago.

5D SMART SAN FRANCISCO 2030 DISTRICT

Another promising federal lab-city government collaboration on IoT is the 5D Smart San Francisco 2030 District, a joint undertaking of the city of San Francisco, CityZenith, a SaaS platform provider, and Lawrence Berkeley National Laboratory. The project has recently moved from prototype to the deployment state, according to its developers.

The 5D Smart San Francisco began when CityZenith, looking for a pilot project for its data visualization platform, approached the city. "Our original goal was to work with the Department of the Environment to visualize compliance with the city's green building ordinance," said Michael Jansen, CEO of CityZenith.

The plan was to incorporate the city's annually aggregated data on the energy consumption of city buildings into CityZenith's platform for analysis and display. But plans quickly grew to include other information, including real-time data. "Now we're starting to layer additional sets of relevant data to create a more complex and dynamic understanding of the scope and breadth of the problems as well as the scope and breadth of the available solutions to the problems," said Jansen.

Among the data providers currently working with the project is EcoMesh, which provides real-time energy usage data, StreetLightData, which combines and analyzes data streams from real-time monitors of traffic and wireless mobile devices and Helios, which offers an integrated suite of building energy analytics related to energy retrofits.

According to Barry Hooper, a private-sector green building specialist, "The city is acting as the anchor by ensuring that we provide basic information about how large commercial buildings are performing, their annual energy consumption. Our starting point is to offer just a clear visualization of the annual energy consumption data and then to invite in other players who have more detailed information."

Hooper envisions the project as a way to increase awareness on the part of planners and building owners and to encourage the adoption of best practices and best-in-class energy management solutions.

"Cities have generated more data in the past couple of years than they have in the previous hundreds," added Jansen. "And the vast majority of that is unstructured and therefore either unused or underused. We're now working with ways to make that data more useful, visible and interactive."

The initial model of 5D Smart San Francisco was expected to be released by the end of February, with additional datasets to be linked in over the following weeks. •

SECURITY AND STANDARDS FOR THE IOT

As is not uncommon with emerging technologies, adoption of the Internet of Things (IoT), especially in government, is being slowed by concerns about security and a lack of standards.

With respect to security concerns, the Federal Trade Commission in January released a report, "Internet of Things: Privacy & Security in a Connected World," that noted that connecting a wide array of insecure devices presents potentially major risks. According to the report, "Unauthorized persons might exploit security vulnerabilities to create risks to physical safety in some cases." The report cited one instance in which a hacker was able to access two different connected insulin pumps and change their settings so that they no longer delivered medicine. In another case, a hacker was able to access a car's telematics unit and take control of the vehicle's engine and braking systems.

"Although the risks currently may be small, they could be amplified as fully automated cars, and other automated physical objects, become more prevalent," warned the report.

As for IoT standards, the major push is by the Industrial Internet Consortium, a non-profit group formed by AT&T, Cisco, General Electric, IBM and Intel in March 2014. Already the group has more than 150 members, including a handful of major universities.

In response to both security and standardization concerns, NIST launched a public working group in June 2014 to explore the array of related issues facing those working to implement IoT projects in both the public and private sectors. – Patrick Marshall

Revamped Philly 311 goes social

A new blueprint for handling Philadelphia's 311 services passes some of the power over city services to residents

BY STEPHANIE KANOWITZ

Announced Feb. 18 at the city's first Citizen Engagement Innovation Summit, the new Philly 311 system updates what's been in place since 2008 with some notable additions, including a cloud-based neighborhood portal that lets residents view nearby requests and organize events to address their concerns. It also helps the city better track service requests.

"We're moving towards a model where the government doesn't have to provide all the solutions, but it can be a platform upon which citizens are able self-organize," said Vivek Kundra, executive vice president of Salesforce, a cloud computing company. "What you're seeing is a huge shift. Philly 311 is the customer service tool, the front office for the city of Philadelphia."

And that front-office focus is crucial, he added. "For the last 40 years we've seen massive investments in [information technology] that, frankly, have not paid off, which were all in the back office," said Kundra, former chief information officer of the United States. "Now what you're seeing in terms of the cities is that they're making these investments in the front office and addressing the problems that citizens actually have."

Since the Philly 311 call center opened in 2008, it has received more than 7 million calls from citizens and businesses with service requests, ranging from pothole repairs and cleaning graffiti to removing drug paraphernalia from playgrounds and reporting abandoned vehicles, the city said.

Philly 311 expands citizens' access to city services via a wide range of channels including telephone, Internet, the Philly 311 mobile app and Facebook and Twitter. The system also provides comprehensive service reporting capabilities to city management on system performance and geographic-based service needs, according to Unisys, which set up the system.

With the portal, residents don't have to wait for government workers to respond. Instead, they can interact with one another on concerns about, say, drug use, graffiti or crime in a particular section of the city. For instance, if people want to build a playground, they can organize an event via the portal, according to a CBS Philly report in which city Chief Customer Service Officer Rosetta Carrington Lue described the portal as "kind of like Facebook for government."

Other new features of the app include better mapping to geolocate problems and improved tracking for service requests. Predictive analytics will also be used to anticipate residents' needs, such as scheduling trash pickup ahead of a snow storm, Kundra said.

The new Philly 311 is built on Salesforce's government customer relationship management (CRM) cloud computing platform. It was part of a $120 million capital investment by Mayor Michael Nutter to upgrade technology infrastructure and part of his "Philly Innovates Blueprint," a seven-step plan for making America's fifth largest city more connected. Since the new app was first released in 2012, it's become the second most used tool for logging service requests and has a 93 percent customer satisfaction rating, the blueprint states.

Since then, Philadelphia has seen the number of people who walked into a city government building to request services drop by 30 percent, while the number who used mobile as the point of contact rose 344 percent, according to Salesforce statistics.

> "The old debate about big government or small government is over. It's about smart government."
>
> – VIVEK KUNDRA, SALESFORCE

"With the new Philly 311 customer service platform, our goal is not only to create a more connected, citizen-responsive city, but also to inspire other cities to follow our model and engage their citizens," Nutter said in a statement.

"The old debate about big government or small government is over," Kundra said. "It's about smart government. It's much bigger than just a technology story. It's about redefining the business model of government." •

NASA launches 'paper-less' procurement

Executive support and solid processes were key enablers of JPL's plan to go paperless

BY STEPHANIE KANOWITZ

It's not rocket science to know that digitizing paper-based processes can save money and time, but a NASA field center is setting an example for how to best tackle the task.

The Acquisition Division of NASA's Jet Propulsion Laboratory has digitized hundreds of thousands of documents as part of its plan to make the procurement process paperless. The project began as "Work Different" in October 2012, and 20 months later the Interactive Acquisition Network (IAN) was rolled out.

"We chose paper-less, not paper-free because there's always going to be some amount of paper," said Martin Johnson, manager of the Acquisition Strategic Planning Office.

IAN is built on three Microsoft tools that were already part of JPL: Office 2013, SharePoint 2013 and OneNote 2013. Working with the JPL Office of the Chief Information Officer (OCIO), the division created a system that electronically manages from start to finish all procurement packages.

"Subcontract packages are built on OneNote template-driven forms, then routed though SharePoint workflow using InfoPath 2013 forms to gather reviews, comments and approvals," Steve Simpson, the acquisition technical lead for Work Different, and Wayne Wong, an enterprise apps software engineer at JPL, wrote in an announcement.

"The system allows for reassignments, rework and resubmittals. Once the approvals have been gathered, the acquisition subcontract manager files the approvals and can then submit the final OneNote package for internal signature workflow – with external signature to be rolled out in the new fiscal year."

Before IAN, workers created binders filled with tabs and printouts. "If there's a mistake, heaven forbid, they had to reprint and redo," Johnson said. Now "we're able to take that information while it's done on your system and just drop it into an actual e-binder…. It looks very much like the binders, but it's all done digitally now."

A routing process for signatures was important, he added, because sometimes a trip to physically bring paper to be signed took 750 steps one way.

"We had people walking files around for somebody to look at and review," Johnson said. "Now the system technologically allows us to route things to various levels and once it releases from one, it goes to the next [and] to the next, and if they have to send it back, it sends it back all within the system."

Another benefit has been data access and control. Because everything is in a unified location with a unified naming convention, JPL can provide access permission to anybody across the lab based on need.

Since IAN launched on June 2, 2014, JPL has digitized 320,000 to 350,000 documents, and more than 5,000 subcontract packages have gone through the process.

Currently, JPL does not use cloud storage or mobile access for the system, although much of the work is done on laptop computers, Johnson added, which lends an aspect of mobility.

> "We chose paper-less, not paper-free because there's always going to be some amount of paper."
>
> – MARTIN JOHNSON, ACQUISITION STRATEGIC PLANNING OFFICE

To gauge the success of the program, even the commodities section of the division is saving about $30,000 a year because of fewer printer and copier leases and less need for ink.

To encourage cultural support, employees were integral to IAN from the start. At any point in time, at least 40 percent of staff was involved in subteams building this, he said.

Executive support, leadership from the business side – rather than the information technology department – and solid processes were also key enablers.

"You need to have highly skilled OCIO people embedded into the project," Johnson said. "They're managed and pushed by the business side, but they're enabled by the technical side." •

Indiana ramps up mobile apps for gov

Access to public information has been streamlined, and downloads to the state's app store have boomed

BY PATRICK MARSHALL

A little over a year ago, Indiana's Office of Technology (IOT) adopted MobileIron's mobile device management software to administer and secure its network of 2,500 iPhones. Since then the state has streamlined citizen access to state services and seen subscriptions to its home-grown apps store skyrocket.

MobileIron allows state IT staff to detect rooted and jail broken phones, to enforce security policies and to wipe lost or stolen devices. The MobileIron server also provides access to email, calendaring and contacts for its mobile staff.

Now the IOT is moving to the second and third stages of its mobility strategy: First, it is implementing a just-approved BYOD policy that will support an expected 3,500 Android, Windows and iOS devices. Second, IOT is rapidly developing and deploying its own mobile apps for both agency staff and for Indiana residents.

Already, according to Bob Clarke, manager of the IOT's application development group, the team has deployed five apps, including:

- IN.gov, an app that gives Indiana residents access to state resources that lets them search job postings, receive alerts for job openings, check employee directories and find maps of state facilities.
- DamagWise, an application for the state's Department of Transportation that field inspectors use to track, photograph and document accidents involving state property. The reports are transmitted to insurance companies, including quotes for damage repair, for rapid payment.
- A travel advisory app that allows residents to receive warnings and advisories about travel conditions around the state.
- An app that system administrators use to monitor servers and to troubleshoot IT problems.
- An app that interfaces with IOT's help desk ticketing system.

According to Clarke, since the IN.gov app was posted to the apps store last year it has been installed over 8,000 times and it has been launched 42,690 times. The travel advisory app, which was released only a month ago, has been installed over 41,000 times and launched approximately 340,000 times.

In addition, since IOT is using MobileIron's Apps@Work storefront, the team no longer has to go through the extensive hurdles involved in getting apps into the Apple app store.

"We brought MobileIron in because we wanted to be able to push internally developed applications, line of business apps, productivity apps to devices without going through that process of vetting through the Apple iOS App Store," said Clarke.

Apps@Work also gives the state control over how its apps are deployed. Administrators can select which applications are available to which users, as well as track app downloads and launches.

The IOT team has also developed an app for the Department of Natural Resources. "It will be DNR's public interface to all their fishing, hunting, state parks and camping resources," said Clarke. "It has a help feature where you can report poachers and identify fish species. It will tell you where you can fish for particular species or where you can fish in general."

The team is also working on an app to help the state Department of Education in its efforts to reach out to families of migrant workers who qualify for medical and educational services. "My department is only two years old," noted Clarke. "We are so busy and I love it."

According to Dewand Neely, director of End User and Support Services, the state is also serious about training developers for other agencies to further the use of mobile apps. "We just had a training class where we trained about 18 of the internal state developers so that they can start writing apps for their agencies," said Neely. •

IOT's mobile initiative by the numbers

2,500
iPhones secured by IOT adopting MobileIron's mobile device management software

8,000/42,690
times the IN.gov app has been installed and launched, respectively

41,000/340,000
times the travel advisory app has been installed and launched, respectively

ADVERTISER INDEX

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

BY PATRICK MARSHALL

Using smartphones for ID authentication

PEOPLE ARE MORE LIKELY to leave their ID badge in the jacket they wore yesterday than they are to forget their cell phone. So why not use the phone itself as an authenticating device? Many companies and some government entities are beginning to do just that.

The Iowa Department of Transportation, for example, announced in December 2014 that it was about to release a driver's license app for smartphones. Initially, the digital license would only be an alternative to the paper temporary licenses issued by the department. But according to Mark Lowe, director of the state's Motor Vehicle Division, "The ultimate goal is that we get to the point where we see customers elect to use this in addition to or in lieu of the driver's license."

Apart making for one less document to lose, Lowe said that unlike with physical licenses, which are generally only examined visually, the owner of a digital license can also be confirmed by biometric devices on smartphones. And while a lost physical license can be used for nefarious purposes by others, digital licenses on lost smartphones can be remotely wiped clean.

In the private sector, United Airlines is using smartphone cameras to determine the authenticity of passports and the identification of travelers during the process of issuing boarding passes for international flights. The airline has deployed Jumio's Netverify Mobile, which launched last year, to offer travelers a way to avoid standing in long lines.

According to Marc Barach, chief marketing officer at the credentials management company, the user is prompted to click on a button that is marked, "Show your passport." The customer is then guided to hold up his passport open to the photo page to the camera.

"We're not taking a picture and nothing is stored on the device," explained Barach. Instead, the document is scanned and analyzed by Jumio's software. The process takes about 90 seconds. "We are able to detect with a very high degree of certainly when we see a fraudulent document," said Barach. "Also, we extract information from it – name, passport number – and put it right into the form. About 90 seconds later you're issued your international boarding pass."

A critical second step in the process, of course, is determining that the person with the document is who he claims to be. "Step two of the process is the face match," said Barach. "That is where the individual then holds up their camera to their face and in real time we scan their face and match their face with the image on the document. Then we render a score as to what extent we think it's one and the same. Clearly it can never be 100 percent. Maybe someone is a twin, or maybe someone has grown a beard."

Ultimately, of course, a human may have to judge whether a partial match is accurate or not. And at present the 90 seconds required for processing can make the technology inappropriate for some purposes, such as accessing buildings or rooms. But Barach said the company is working on improvements. "We're working to bring that time down, hopefully ultimately down to just a few seconds," he said.

Smartphones are also beginning to be used in lieu of smartcards and tokens for access to physical spaces or devices.

For example, Symantec recently introduced VIP Access for Mobile, software that turns a smartphone into a security token. (The VIP stands for validation and ID protection.) The hosted service eliminates the need for IT staff to configure and distribute hardware tokens to users.

Smartphones serving as authentication devices can, in short, offer convenience to both system administrators and end users. But the technology promises some unexpected benefits for the latter group. Just as consumers are already receiving boarding passes on their smartphones, soon they can be receiving digital keys to their hotel rooms, eliminating the need to wait in a line at the front desk.

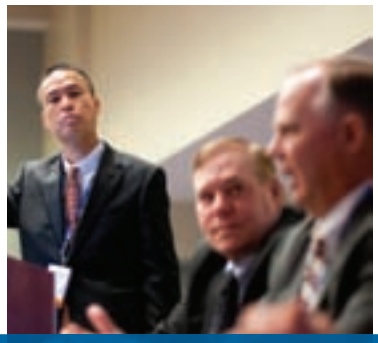
Best of all for many of us who are short-term-memory challenged, once smartphone authentication is supported by the other devices we use, including our computers, we will be relieved of the need to remember and to change complex passwords. •

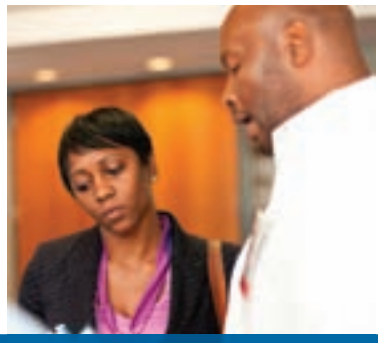
> The ultimate goal is that we get to the point where we see customers elect to use this app in addition to or in lieu of the driver's license.
>
> - MARK LOWE, DIRECTOR OF THE IOWA MOTOR VEHICLE DIVISION

INAUGURAL 2015

ENTERPRISE ARCHITECTURE WEST

SPECIAL GOVERNMENT PRICING ENDS SOON





EA EDUCATION NOW ON THE WEST COAST!

WORKSHOPS: APRIL 20
CONFERENCE: APRIL 21
SACRAMENTO, CA
CITIZEN HOTEL

At Enterprise Architecture West, enterprise architects, project managers and industry experts will convene to discuss contemporary EA and how to apply it to make the mission possible.

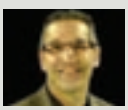
Trending topics impacting the EA community to be discussed include:

- Increasing efficiencies and fostering innovation by using cutting-edge EA methodologies
- Using enterprise architecture as a medium for restructuring

TUESDAY KEYNOTE DETAILS

Enterprise Architecture: 30 Years Young – Moving from the Age of Compliance to the Age of Outcomes

John A. Zachman
Chairman, Zachman International and Executive Director, FEAC Institute



Carl E. Engel
Chief Strategy Officer, Zachman International

Covering:

- How integrating framework approaches will yield better results.
- EA's current compliance mindset and how to give greater emphasis to its outcome-yielding role.
- And more!

Don't Miss This Inaugural Event — **Register NOW** for Best Savings!

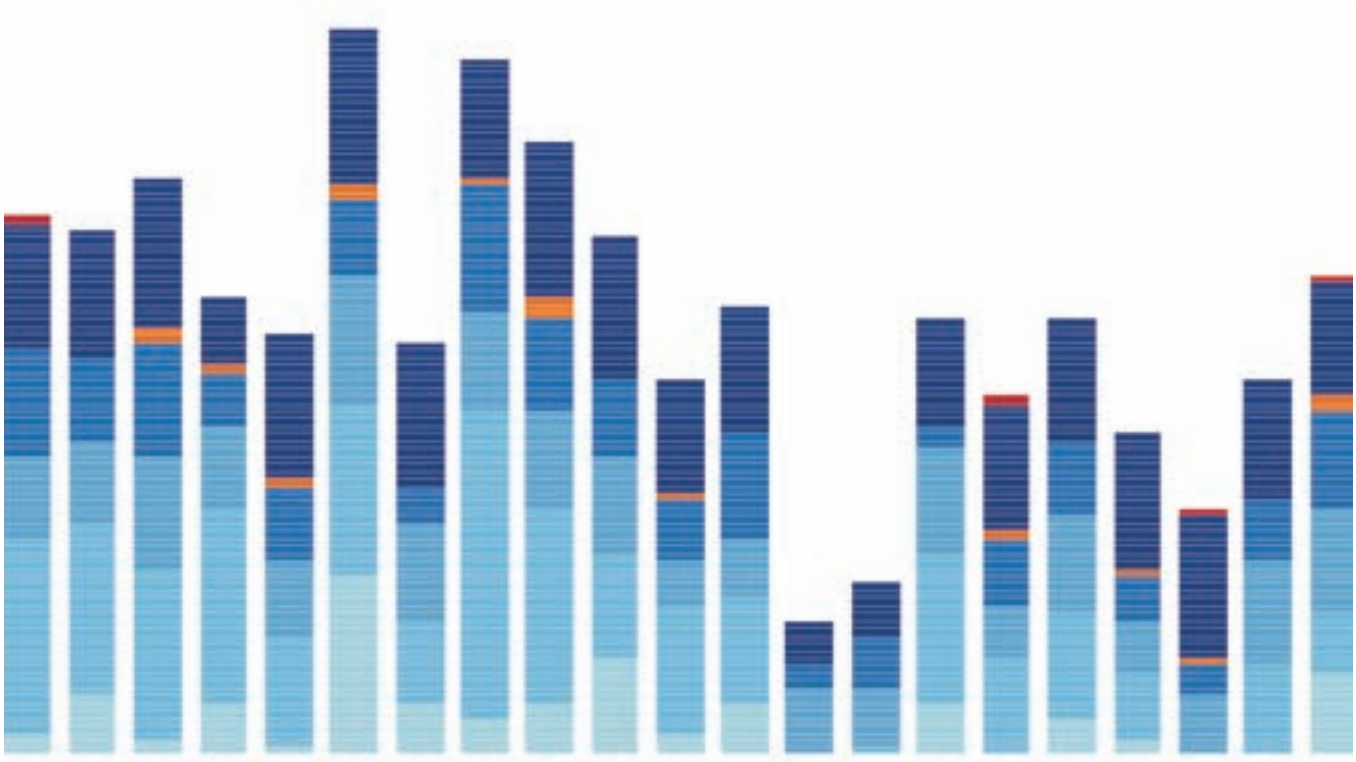
govEAconference.com/west
USE PRIORITY CODE: EAW15

PRESENTING PARTNERS
FEAC Institute · Zachman International Enterprise Architecture

SPONSORS
PHASEONE · PrinterLogic

PARTNERING MEDIA
Defense Systems · FCW · GCN · Washington Technology · OMG

PRODUCED BY Public Sector Events Group



Where Data Meets Transparency

With Tableau, government agency users can see and understand data from any source with fast, easy, drag-and-drop technology.

Tableau will help your agency:

- Harness visual analytics for self-service problem-solving
- Make fact-based decisions that impact legislation
- Increase citizen collaboration and transparency
- Work toward goals 10–100x faster than other BI tools
- Free IT resources to focus on maintaining security

For a free trial visit, www.tableau.com/government

tableau