

government
technology™



Solutions for
state and local
government.

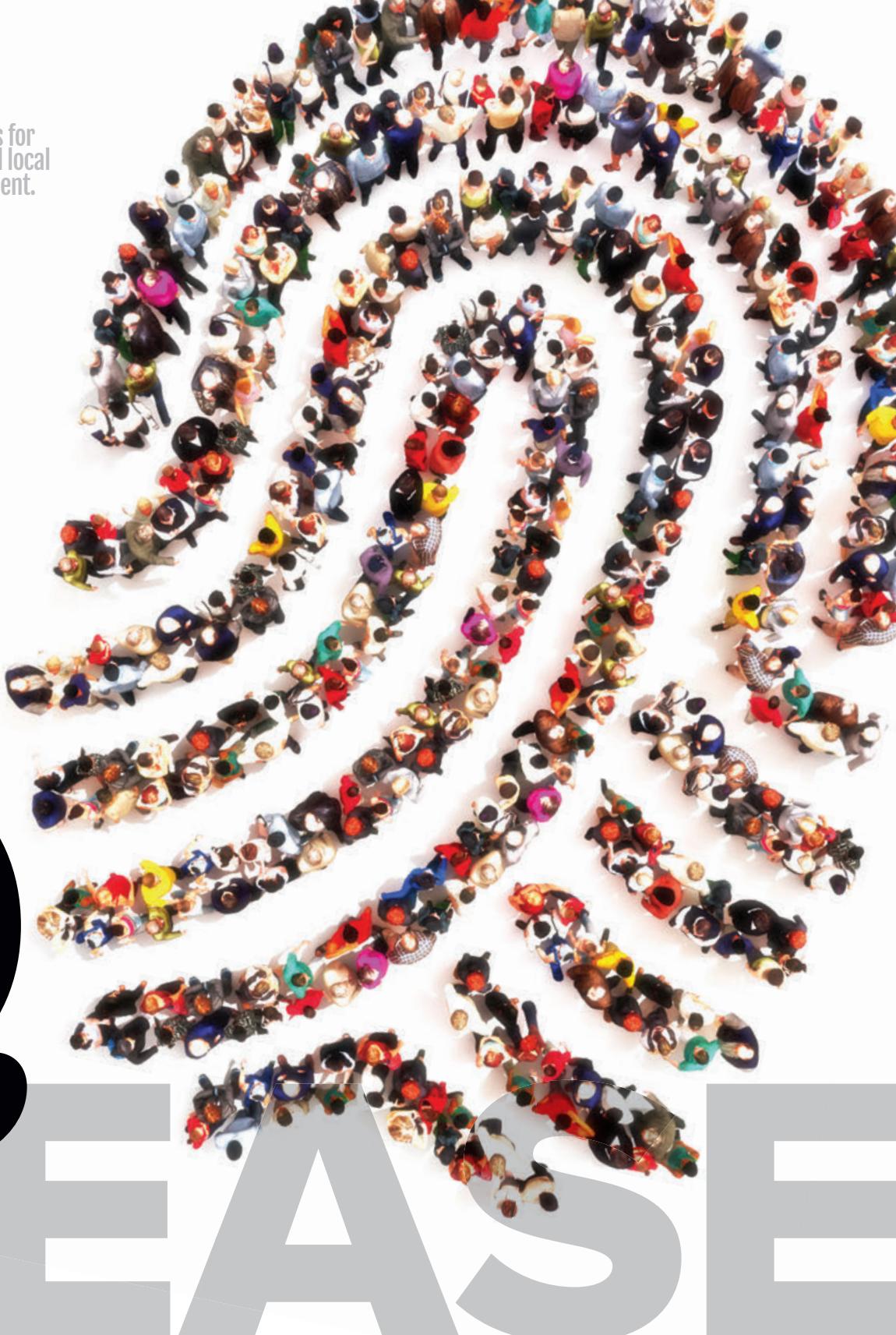
MARCH 2019

PLUS:

A License for Services

We look at cities issuing ID cards to connect non-drivers with government programs.

ID PLEASE



The quest for a
unified solution to
identity and access.



“Disaster response is not just about helping communities get their systems back up, it’s about the whole ecosystem.”

STACY SCHWARTZ

Vice President, AT&T Public Safety

Government agencies on the front lines need a trusted ally that can help manage all aspects of an emergency.

Read the study at

bit.ly/HurricaneResponse



An Ecosystem Approach to Disaster Response

Government agencies on the front lines need a trusted ally that can help manage all aspects of an emergency.

COMMUNICATION IS CRITICAL before, during and after a disaster. Providing information, so protecting or restoring communications infrastructure is always a priority. But considering a disaster as a whole system promotes broader planning and better cooperation among different groups. Protecting and restoring communications infrastructure quickly requires a network of logistics support, emergency planning and experience.

“Disaster response is not just about helping communities get their systems back up, it’s about the whole ecosystem,” says Stacy Schwartz, vice president, AT&T Public Safety. “It’s about supporting first responders in every way possible so they can help citizens.”

The following are recent examples of how AT&T is uniquely supporting disaster response efforts side by side with first responders at the state, local and federal levels:

Bouncing Back from Irma

As of September 2017 Monroe County, Fla., hadn’t been affected by a major hurricane in 2 years. But it was about to get hit by a whisper in the form of Hurricane Irma.

The most powerful Atlantic hurricane in recorded history—sustaining 185-mile-per-hour winds for 37 hours—Irma made landfall in Florida on September 10, a Sunday morning. On Monday morning, first responders turned to assess the damage and assist residents. The Monroe County Emergency Operations Center (EOC), located in Marathon, was directly in the path of Irma. Fortunately, the EOC building sustained only minor damage. But its fiber network was down, crippling the County’s emergency communication capabilities. Satellite helped serve as a backup, but connections were limited.

On Wednesday, AT&T National Disaster Recovery crews arrived in Monroe County, with Cell on Light Trucks (COLTs) units are mobile units equipped with high-capacity antennas. The COLTs provided County officials and emergency responders with cell phone connectivity to help in their disaster response efforts. By Wednesday night, AT&T had restored cellular service at the Marathon EOC and at three emergency resource locations in Key West.

“It was a game-changer,” says Alan MacEachern, director of information technology for Monroe County. “All of a sudden we had voice, text and data capabilities. That was huge from

“Disaster response is not just about helping communities get their systems back up, it’s about the whole ecosystem.”

STACY SCHWARTZ, VICE PRESIDENT, AT&T PUBLIC SAFETY

CONTENTS

Vol 32 | Issue 2



COVER STORY

14 / Identity & Access Management Today

The little-known world of IAM receives scant attention — but security and services can't move forward without it.

By Tod Newcombe

20 / States of Identity

Grappling with security and data access, here's how four states are working toward a single log-in credential.

By David Raths

26 / Turning ID Inside Out

How emerging technologies are poised to disrupt the way we identify ourselves online.

By Adam Stone



11

Laurel Caldwell,
IT director,
Latah County,
Idaho

DAVID KIDD

DEPARTMENTS

32 / Muni ID Cards on the Rise
Cities across the country are issuing residents IDs so they can access benefits and other services.

34 / A Mobile Identity
Louisiana's launch of a digital driver's license puts it ahead of other states working to get government IDs on smartphones.



IN OUR NEXT ISSUE:

Gov Tech in Profile

Up close with our Top 25 Doers, Dreamers and Drivers of 2019.

COLUMNS

6 Point of View

New headquarters bring new ways to innovate in Alameda County, Calif.

10 Data Points

Bans on e-scooters hint at where cities stand on innovation.

11 Four Questions

In Latah County, Idaho, Laurel Caldwell is doing big work in a small jurisdiction.

42 GovGirl on Social

Social media is an essential part of emergency management.

NEWS

8 govtech.com/extra

Updates from *Government Technology's* daily online news service.

12 Big Picture

An abandoned prison in York, Pa., is getting a high-tech makeover.

36 Spectrum

More research, more science, more technology.

37 Products

Dell 75 4K Interactive Touch Monitor, HP Spectre Folio PC, InFocus ScreenPlay projector.

38 CIO Central

Career changes across tech-driven roles in government.

FOLLOW US ON [Twitter](#) [Facebook](#) [YouTube](#) [Google+](#)

WWW.GOVTECH.COM

Connected Governors

Highlights from this year's State of the State addresses.

Publisher: [Alanc@erepublic.com](#)

EDITORIAL

Editor: [Noelle Knell](#), [nknell@govtech.com](#)
Managing Editor: [Lauren Harrison](#), [lharrison@govtech.com](#)
Web Editor & Photographer: [Eyragon Eidam](#), [eeidam@govtech.com](#)
Chief Copy Editor: [Miriam Jones](#), [mjones@govtech.com](#)
Copy Editor: [Kate Albrecht](#), [kalbrecht@govtech.com](#)
Senior Editor: [Tod Newcombe](#), [tnewcombe@govtech.com](#)
Associate Editor, Data & Business: [Ben Miller](#), [bMiller@govtech.com](#)
Staff Writers: [Skip Descant](#), [sdescant@govtech.com](#)
[Zack Quaintance](#), [zquaintance@govtech.com](#)
[Lucas Ropke](#), [lropke@govtech.com](#)
[Andrew Westrope](#), [awestrope@govtech.com](#)

Contributing Writers: [David Raths](#), [Adam Stone](#)
Editorial Assistant: [Moriah Sollie](#), [msollie@govtech.com](#)

DESIGN

Chief Design Officer: [Kelly Martinelli](#), [kmartinelli@govtech.com](#)
Graphic Designer Pubs: [Kale Mendonca](#), [kmendonca@govtech.com](#)
Senior Designer Custom: [Crystal Hopson](#), [chopson@govtech.com](#)
Production Director: [Stephan Widmaier](#), [swidm@govtech.com](#)
Production Manager: [production@govtech.com](#)

PUBLISHING

SENIOR VP OF STRATEGIC ACCOUNTS: [Stacy Ward-Probst](#), [swprobst@govtech.com](#)

VPS OF STRATEGIC ACCOUNTS: [Kim Frame](#), [kframe@govtech.com](#)

Shelley Ballard, [sballard@govtech.com](#)

SALES DIRECTORS:

[Melissa Sellers](#), [msellers@govtech.com](#)

[Karen Hardison](#), [khardison@govtech.com](#)

[Lara Roebelen](#), [lroebelen@govtech.com](#)

[Carmen Besirevic](#), [cbesirevic@govtech.com](#)

[Lynn Gallagher](#), [lgallagher@govtech.com](#)

[Kelly Schieding](#), [kschieding@govtech.com](#)

ACCOUNT EXECUTIVES:

[Rebecca Regrut](#), [rregrut@govtech.com](#)

[Kathryn Nichols](#), [knichols@govtech.com](#)

[Joelle Tell](#), [jtell@govtech.com](#)

[Lisa Blakie](#), [lblackie@govtech.com](#)

[Kristi Leko](#), [kleko@govtech.com](#)

[Justin Windus](#), [jwindus@govtech.com](#)

BUS. DEV. MANAGER:

[Nick Pedersen](#), [npedersen@govtech.com](#)

[Shane Prince](#), [sprince@govtech.com](#)

[Sheryl Winter](#), [swinter@govtech.com](#)

INSIDE SALES:

[Paul Dangberg](#), [pauld@govtech.com](#)

[Katrina Wheeler](#), [kwheeler@govtech.com](#)

[Dana Kansa](#), [dkansa@govtech.com](#)

SALES ADMINISTRATORS:

[Jane Mandel](#), [jmandel@govtech.com](#)

[Lien Largent](#), [llargent@govtech.com](#)

[Tina Faragia](#), [tfaragia@erepublic.com](#)

[Sharon Penny](#), [spenny@govtech.com](#)

[Tara Holm](#), [tholm@erepublic.com](#)

Sr. Dir. of Sales Operations: [Andrea Kleinhardt](#), [akleinhardt@govtech.com](#)

Event Sales Operations Mgr: [Alison Del Real](#), [adelreal@govtech.com](#)

Chief Customer

Success Officer

Dir. of Content Studio:

Dir. of Digital Marketing:

Web Advertising Mgr:

Subscription Coord.:

Arlene Boeger, [aboeger@govtech.com](#)

Jeanne Bigham, [jbigham@govtech.com](#)

Lisa Harney, [lharney@govtech.com](#)

Paul Harney, [pharney@govtech.com](#)

Alan Cox, [alanc@govtech.com](#)

Paul Taylor, [ptaylor@govtech.com](#)

Steve Towns, [stowns@govtech.com](#)

Joe Morris, [jmorris@govtech.com](#)

Dennis McKenna, [dmckenna@govtech.com](#)

Cathilea Robnett, [crobnett@govtech.com](#)

Lisa Harney, [lharney@govtech.com](#)

Paul Harney, [pharney@govtech.com](#)

Executive VP:

Chief Content Officer:

Dep. Chief Content Ofc.:

VP Research:

Government Technology is published by e.Republic Inc. Copyright 2019 by e.Republic Inc. All rights reserved. Government Technology is a registered trademark of e.Republic Inc. Opinions expressed by writers are not necessarily those of the publisher or editors.

Article submissions should be sent to the attention of the Managing Editor. Reprints of all articles in this issue and past issues are available (\$50 minimum). Please direct inquiries for reprints and licensing to Wright's Media: (877) 652-5295, sales@wrightsmedia.com.

Subscription Information: Requests for subscriptions may be directed to Subscription Coordinator by phone or fax to the numbers below. You can also subscribe online at [www.govtech.com](#).

100 Blue Ravine Rd. Folsom, CA 95630
Phone: (916) 932-1300 Fax: (916) 932-1470

Printed in the USA.

e.Republic

BPA
WORLDWIDE



SAVE THE DATE

JUNE 5-6, 2019
MINNEAPOLIS, MN

SUMMIT ON GOVERNMENT PERFORMANCE & INNOVATION 2019

Governing and Living Cities cordially invite you to our 5th Annual Summit on Government Performance & Innovation. This national Summit brings together innovators, disrupters, and civic entrepreneurs — and all those interested in making government work better for local communities. A must-attend event for those who want to stay on top of the latest trends and meet the dreamers and doers of government performance and innovation.

JOIN THE INNOVATION IN MINNEAPOLIS – JUNE 5-6, 2019

Visit our website for hotel and registration information!
Registration is complimentary for public sector.

FOR MORE INFORMATION, VISIT:
www.governing.com/events/gpi





New Headquarters, New Ways to Innovate

The former Crocker National Bank Building in downtown Oakland, Calif., had been empty for a long time. In the historic registry, the red granite and terra cotta tile building's art deco style made it a noteworthy structure in the business district since its construction in the 1950s.

Owned by the county, the building had housed the Child Support Services Department until it outgrew the space about a decade ago. Since then, two other agencies have looked at moving in, but couldn't find a way to make it work to serve their needs.

Enter Alameda County Chief Information Officer Tim Dupuis. Central IT added new areas of responsibility over the past few years, and new staff to go along with it. Now in charge of county communications as well as the IT functions for the social services agency, Dupuis found himself with a fragmented workforce in four different locations.

"Everything was becoming very siloed and we were running out of space," he said.

The bank building would save on leasing costs, since it was an existing county asset. In addition, it freed up 35,000 square feet of office space in county facilities that could help meet the growth needs of other departments.

But the Information Technology Department (ITD) had its work cut out for it in preparing the space for its technology workforce. Once the plans were approved, Dupuis expected about a nine-month construction timeline, but all told, the

project took about three years. The county took great pains to ensure standards for spending were followed and that the building's historic character was preserved.

"A lot of the challenges had to do with looking at the design, making sure we were value engineering what we were doing to stay within the county remodel budget," Dupuis explained.

All told, the total project budget was \$20 million — well within remodeling cost expectations for a project in the Bay Area. And in the end, it came in \$1.5 million below original estimates. Staying within those parameters, the county also achieved a "Gold" LEED certification with the building, exceeding the county's Silver standard.

A parallel challenge Dupuis faced was managing the massive cultural change the new space would represent.

"We were looking at a very different way of running a government IT shop in a building like this," he said. The new design is an activity-based workspace — a concept making a bit of headway in government, but more common to technology offices in the private sector. For Alameda County, it meant trimming the county standard for square feet per employee by about a third. This meant physical changes like fewer offices for management, sit-stand benching systems and many shared spaces intended to encourage collaboration and a whole new style of work. Communication and negotiation behind the scenes to foster buy-in for these dramatic changes was a huge part of Dupuis' focus.

Every employee, even traditionally PC-bound programmers, now has a laptop. And staff in the new facility don't have desk phones, but rather a "soft" phone on their laptop, paired with their choice of headphones or ear buds. The new office forced a massive decluttering effort, as there are no file cabinets. Each employee was granted two banker's boxes to transport their belongings for the move. Everything else was scanned and/or purged, in coordination with legal officials.

"All of the different things that we went through were things that we wanted to address anyway," said Dupuis, noting that the IT department can now help other agencies transition from paper-based to electronic processes with a newfound authority. Likewise, they already live in a world free of desk phones should other agencies want to forgo that cost as well.

Being in the same physical space has already proven a major benefit. A recent system outage at one of the departments was resolved in just 20 minutes — an outcome enabled by all the problem-solvers being in the same space. Prior to the move, a similar problem would've taken a couple days to fix.

Located near Silicon Valley, Dupuis is all too familiar with the challenges of recruiting top technology talent into government service. But the new space definitely helps.

"We may not be able to compete with Silicon Valley salaries, stock options and things of that nature, but we can rival the space and the innovation," he said. "We want to make sure people recognize that their skills aren't going to languish; this isn't old school. This is equally as advanced as what they're seeing in the private sector."

For more on ITD's new headquarters, visit <https://youtu.be/SwPdRxJRqUU>.

“...A PODCAST ALL CITY-GOVERNMENT
CHANGE-MAKERS SHOULD ADD TO
THEIR PLAYLIST.

— *A Bloomberg Cities selection*



HOSTED BY **CATHILEA ROBINETT**
PRESIDENT, GOVERNING

IN THE ARENA

A new podcast from Governing featuring conversations about courage, compassion and creativity in public leadership with those who serve in the arena today.



MAYOR NAN WHALEY
DAYTON, OH



MAYOR STEVE BENJAMIN
COLUMBIA, SC



GOVERNOR DOUG BURGUM
STATE OF NORTH DAKOTA



KRISTEN COX
EXECUTIVE DIRECTOR, OMB,
STATE OF UTAH



MAYOR GREG FISCHER
LOUISVILLE, KY



MAYOR ERIC GARCETTI
LOS ANGELES, CA

Available on Apple Podcasts, Stitcher and governing.com

Beating Blight

Part of a trend of cities exploring storytelling through data and analytics, **St. Petersburg, Fla.**, is building performance dashboards for all its departments, including one aimed at reducing blight. The city's open data and accountability platform, StPeteStat, is using a product called Socrata Perspectives to help the Codes Compliance Assistance Department enforce city codes and identify violations. City technologists used the software to map areas with high code violations, as well as where code investigators were being under- or overworked.

The project fostered buy-in from officials, and district lines were redrawn to be more equitable and instances of blight were reduced.



Southern Smarts

Major hubs like New York, Chicago and Las Vegas grab headlines for their cutting-edge smart cities work, but quieter names are also getting in on the action. A public-private partnership among **Montgomery, Ala.**, its chamber of commerce, Alabama Power and others is developing a smart cities lab to pilot trends those larger municipalities have used, like intelligent parking and free Wi-Fi. The nine-block area will stretch from the Montgomery Biscuits' Riverwalk Stadium to the Alabama statehouse and will be anchored by fiber-optic cables. The first phase of free Wi-Fi access went live in January.

Flickr/Broderick

Biz Beat

State and local gov tech stalwart **Tyler Technologies** is moving further in a new, federal direction. Tyler has previously focused on providing ready-made software to cities, counties and states, and has recently completed several major mergers and acquisitions, including with Socrata and CaseloadPRO, among others. But in January, the company made the second-largest buy-out in its history with the acquisition of MicroPact, a platform that does half its business with the federal government, developing apps for business process and case management. Some of MicroPact's existing state and local customers include the California Department of Consumer Affairs and the Tennessee Department of Health.

WHO SAYS?

"The transformation that's happening — no matter whether you have a title for it or not — is that cities are realizing they're part of the innovation process."

govtech.com/quoteMarch2019

MOST READ STORIES ONLINE:

Louisiana Enters the Era of the Digital Driver's License

6,448 VIEWS

AAA Acquires Largest Autonomous Vehicle Test Site in the Country

2,330 VIEWS

Former FEMA Admin.: AI Can Marry Urban Planning and Disaster Response

1,833 VIEWS

How Is the Federal Shutdown Affecting State and Local Tech?

1,623 VIEWS

Real-Time Data Analytics Aims to Reduce Traffic Fatalities

1,535 VIEWS

Court Rules in Favor of FCC 5G Regulatory Rollbacks

1,346 VIEWS

\$90K

The amount of incentive funding Smart Columbus has for ride-hailing drivers who trade gas-powered cars for electric vehicles.

75%



The proportion of Charleston, S.C., residents who live in a designated flood zone; the city is using predictive analytics to alert them to an emergency.

3.5K

The number of local government customers served by CivicPlus, a builder of websites and integrated communications software.

\$499

The base price for an electronic license plate from Reviver; the technology is currently being piloted in Arizona and California.

Why Security Doesn't Have to be a Barrier to Government Cloud Adoption

Cloud access security brokers can strengthen cloud security and enforce compliance and governance policies.



State and local governments are adopting cloud to support digital transformation and innovation.

Infrastructure as a Service (IaaS) is expanding at a compound average growth rate north of 30 percent, while Software as a Service (SaaS) is increasing by more than 20 percent each year. As government agencies adopt the cloud, security remains a priority.

In this Q&A with *Government Technology*, **Daniel Tang**, cloud solutions architect at McAfee, discusses how cloud access security brokers (CASB) can help government agencies bolster cloud security and enforce compliance and governance policies.

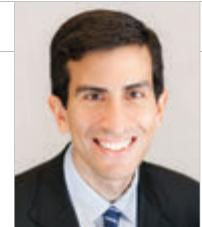
How can government agencies adopt cloud securely without losing control from a compliance and regulatory perspective? Over the past few years, CASB have become an essential element of any cloud security strategy. CASB are on-premises or cloud-hosted software that act as a security control point between users and cloud services to enforce security, compliance and governance policies and help organizations extend the security controls of their on-premises infrastructure to the cloud.

Are there challenges to CASB adoption in the public sector? The common challenge public sector organizations face is bringing out-of-the-box comprehensive CASB support for enterprise cloud services beyond the standard software like Office 365, Box, Salesforce, AWS and more. There are many other cloud applications that may be critical to an agency's mission, yet not used widely enough to get the attention of CASB vendors. Customers are not always able to find off-the-shelf CASB support for a cloud application they want to secure.

How can public sector agencies solve that issue? McAfee's Security Innovation Alliance has a rich history of creating open technologies that allow vendors and customers

to break down barriers in security operations — technologies like OpenDXL and TIE, for example. Earlier this year we announced a capability for cloud delivered applications, called CASB Connect, to simplify CASB support in the cloud.

How has CASB Connect enhanced your offerings? CASB Connect is an open API adapter framework that enables cloud vendors to build and maintain a simple file that allows their cloud service offerings to take advantage of the visibility, threat protection, compliance and data security capabilities offered by McAfee's MVision Cloud CASB service. In other words, CASB Connect enables any cloud service provider or partner to rapidly build lightweight API connectors to McAfee Skyhigh Security Cloud to secure any cloud service, without writing a single line of code. McAfee CASB Connect prevents unauthorized sensitive data from being stored in cloud collaboration, file-sharing or storage services, captures a complete audit trail of all user activity for post-incident forensic investigations and detects compromised accounts, insider threats and privileged access misuse, and malware infections across all cloud services. In a nutshell, it minimizes time spent managing multiple security consoles and accelerates secure cloud adoption.



Rolling in the Street

Bans on e-scooters show that cities have much to learn about embracing innovation.

Among many technology milestones last year, one of them was certainly that 2018 was the first year that e-scooters became a fixture in many major U.S. cities. Adoption has grown quickly, with e-scooter rider growth exceeding similar first-year adoption rates of other mobility services, such as bike-sharing, car-sharing and ride-hailing apps. Unfortunately, this rapid growth could run head-first into a brick wall as a number of state and local governments start passing laws and regulations that either ban or undermine the viability of e-scooters.

One reason e-scooters have gained many converts is because they are so easy to ride. But while motorized electric scooters have existed as a product for a few years, the costs and practicalities of owning one did not make sense for most people. To address these hurdles, a flood of startups have begun offering app-enabled e-scooter rental services.

Scooters offer many benefits to city dwellers. On foot, pedestrians have a limited range — many people are not willing to walk further than a quarter-mile because of various factors including health, climate and available time. But with

scooters, a person's range increases substantially. In Santa Monica, Calif., the first city where e-scooter company Bird launched its operations, the average ride length was 1.6 miles. This expanded range not only makes it possible for individuals to live, work and play in more areas, but it also makes parts of the city that

can only be reached by car, such as because of a lack of crosswalks or sidewalks, more accessible to those without vehicles.

Unfortunately, while some have given this new mobility option an enthusiastic reception, others have bemoaned incidents of scooters blocking sidewalks, breaking traffic ordinances and causing accidents. In response, a number of cities, from West Hollywood, Calif., to Winston-Salem, N.C., are simply banning the scooters once they arrive. Others have proactively blocked scooter companies from introducing the service, such as Columbia, S.C., which enacted a one-year ban on the vehicles in January. And still others have started enacting a hodge-podge of regulations that put these vehicles at a relative disadvantage, such as allowing 16-year-olds to drive cars, but not scooters, or allowing scooter owners to ride at night, but not those using a scooter-sharing app.

There likely is a need for some new laws to address legitimate concerns, but it is unclear what those are. Rather than creating new rules unsupported by any evidence, a better approach is to establish a regulatory sandbox for e-scooters, an idea that has grown in popularity for addressing emerging technologies in other industries, such as financial services. Much like parents allow children to safely learn and explore in a controlled environment, the idea of a regulatory sandbox is to create a testing ground for businesses to experiment with new technologies or business models where existing regulations may be inappropriate or incomplete. This environment allows businesses to learn quickly and solve problems as they arise without responding

to artificial constraints. It also allows regulators to collect data so that they can make more informed decisions about what problems need to be addressed and which interventions are most useful.

Using a regulatory sandbox would not mean that states could not set safety rules for the scooters, such as braking distance requirements, or the riders, such as helmet and licensing requirements, but it would seek to minimize those rules and only create ones backed by solid evidence. Neither would it prohibit local governments from enforcing traffic laws and fining those who violate them, such as riding without helmets where required by law. And local governments that want to be proactive, rather than banning scooters, can work cooperatively with companies to address problems unique to scooters as a service, such as the issue of where riders should leave them once they are done riding. Scooter companies can also work together to come up with common rules for riders, like penalizing within the app those who block bike paths or wheelchair ramps.

Given the many benefits of e-scooters, it is unfortunate that the trend in many cities seems to be banning or overregulating them. However, it is not surprising. When automobiles were first invented, many reacted with similar outrage at the seemingly "noisier, dirtier and more dangerous" vehicles, with Vermont even passing a law requiring someone to walk in front of a car waving a red flag at all times, and many cities banning the vehicles altogether.

More than a century later, it's time we do better. 

Daniel Castro is the vice president of the Information Technology and Innovation Foundation (ITIF) and director of the Center for Data Innovation. Before joining ITIF, he worked at the Government Accountability Office where he audited IT security and management controls.



Laurel Caldwell

IT director, Latah County, Idaho

Latah County, Idaho, IT Director Laurel Caldwell has spent a decade charting a technology path for this relatively small jurisdiction with a population of about 39,000. Despite limited resources, she has managed to deliver a full suite of online services, while also working to build stronger cooperative efforts between county agencies, as well as among the state's other county technology chiefs.

1 You recently helped launch a statewide County CIO Forum. What do you hope to achieve? That started from attending a National Association of Counties conference where Iowa presented on its county association, and we wondered whether we could do that in Idaho. It's about county IT leaders coming together to work on similar initiatives. It happens that 35 of the 44 counties use the same vendor for a lot of their software, so there's a lot we can do to compare and to help each other.

We had our first meeting last year and we are trying to meet three times a year. At our next meeting, we plan to talk about how to handle forensic evidence when we have a cybersecurity breach. We're going to have someone from the state presenting on how we can work together, especially around cybersecurity issues. For me, it's all about having a bigger set of IT people to bounce ideas off of.

2 Latah is a small county. What challenges does that present? For our state, Latah County is more of a medium-sized county. We have a small staff, about four people, but other counties have just one or two people. But we have

the same problems as bigger places, especially around cybersecurity. We still have to secure the network and there's never enough money, never enough expertise and never enough time in the day to get it all done. The smaller tax base obviously is an added limitation to how fast we can move on things.

We prioritize based on what the county wants to move forward with, and we move through those methodically — sometimes the answer is no, we can't do it this year. From my perspective, the top priority is cybersecurity, getting solutions in place to protect the network and data, and doing end-user training on cybersecurity. But that means that when the sheriff's office asked for a new evidence server solution, we just don't have the funding for that this year.

3 What's your biggest recent accomplishment? We did a major overhaul on our county website and did that in-house, which required a lot of resources. We had an older website, built around 2007, and it needed to accommodate the ADA requirements and to work on other devices like tablets and cellphones. It took a lot of dedicated staff time, and there were challenges in getting updated information

from each department. The result is a big improvement from where we were, and it's still a work in progress. There are always things we can make better with the website.

4 You've been in this role for 10 years. What's changed? In government, things are always changing. Whenever you have new elected officials who cycle through, you get different requests for what the network should do. And the technology itself has changed considerably in 10 years. We've tried to take advantage of all the training that is available to keep up with the technology options, especially the emergence of cloud.

I also see that a lot of the public agencies are more willing to share information and collaborate. When I first started, things were siloed, you were on your own. Today when we see that county and city issues overlap, people will compare what they're doing, what software they're using. There's a lot more open discussion now, and that helps a lot. It gives us more options for how we can solve any given problem when people aren't limited to their own networks. When neighboring cities and counties collaborate, everyone benefits. **gt**

— Adam Stone, Contributing Writer

Break Out

An abandoned prison in York, Pa., is getting a high-tech facelift. Built in 1842, the York County Prison was in use until 1979, when its inmates were moved to a new facility in Springettsbury Township just one city over. In 1982, the property was sold for \$51,500 to a local couple who envisioned turning the site into a restaurant complex that never came to fruition. Now, 40 years since the prison was vacated, the cell blocks have been demolished and all that remains is the 30,000-square-foot front building. The property has been valued at \$1.25 million, and local dark fiber startup United Fiber and Data plans to turn the facility into a data center that will be part of a rural fiber-optic backbone that the company is building from New York City to Ashburn, Va.

Sources: *York Daily Record*, City of York





IDENTITY & ACCESS MANAGEMENT TODAY



The little-known world of IAM receives scant attention — but security and services can't move forward without it. **BY TOD NEWCOMBE**



Everybody did it, whether they worked in city, county or state government. Staff would put up little Post-it notes on the edge of the PC monitor with passwords to the different applications they had to access. It could be particularly bad in county government, where one worker may have to access multiple state-run applications to manage human service clients, for example.

Should that worker resign from the agency, all those passwords would have to be stripped out of each individual system. But it didn't always happen in a systematic, orderly way. Not every agency had a reliable vetting system for onboarding and offboarding new and old employees. Old passwords would remain active, creating a potential security nightmare.

Welcome to the decidedly unflashy world of identity and access management (IAM), a back-end operation that gets little attention but has become increasingly important in state and local government, where sharing information is a growing priority, but where managing identity in pursuit of better security has failed to keep abreast with change. Simply put, IAM defines and manages the roles and access privileges of users, who can be government workers, businesses or individual citizens. The goal of IAM is to give one digital identity to a user. Once that identity has been established, it must be maintained, modified and monitored throughout each user's access life cycle, according to Identity Management Solutions Review.

With the growth in security risks in recent years, IAM has become a more important tool to allow the right people to have access to the right information at the right time. But other reasons are driving the need for IAM. Government has many more systems and software applications than ever. Those applications are for new customer services as well as worker tools that didn't exist in the past. Government also has more of these applications in the cloud and allows for more applications to run on mobile devices. It adds up to an online environment that increasingly mirrors the private sector in terms of choices and services that exist entirely online.

Yet, government remains federated, which creates a challenge to the goal of having some kind of single sign-on and enterprise IAM, according to Andras Cser, vice president and principal analyst at Forrester, the IT research firm. "You're seeing some centralization, but single systems for single purposes still predominate," he said. "Most departments just want to manage their own users at this time."

The Struggle for Enterprise IAM

In 2012, IAM received attention from NASCIO, the state CIO organization, when it issued a call to action about the necessity for mature IAM in state government. The organization followed this up with a State Identity and Credential Access Management (SICAM) Guidance and

Roadmap document that provided a vision for IAM architecture as well as steps on how to address trust, security, interoperability and process improvement. While states and localities have taken advantage of IAM platforms from IBM, Oracle, Microsoft and other vendors, IAM remains a work in progress. Enterprise IAM is a struggle for most CIOs. Worse, too many agencies and governments still have a paper-based process in place to create, maintain and disable user accounts, resulting in improper access rights. Lack of investments in core IAM tools, systems and platforms will continue to stymie growth in enterprise IAM and single sign-on.

Another challenge is the surge in cloud computing activity. State and local governments are shifting to the cloud in order to deploy online services more rapidly without the traditional infrastructure costs that go along with the construction of on-premise IT systems. While there are clear benefits to using the cloud, there are also drawbacks. The cloud can aggravate the "challenge of verifying identities and managing access to applications and data by consumers, employees and business partners," explained George Moraetes, in the article *Meeting Identity and Access Management Challenges in the Era of Mobile and Cloud*.

Henry Bagdasarian, founder of the Identity Management Institute, a membership organization that provides IAM training and certification for its members across the globe, also sees the cloud as reshuffling the IAM landscape. "It's changed everything related to IAM," he said. "In the past, everyone had to move through the corporate network. Now, we have cloud applications accessible through the Web, bypassing network security, which used to be the focal point of security."

The result is a heterogeneous environment where on-premises applications require one set of access controls while cloud applications require something different, creating a daunting level of complexity, according to Moraetes. Governments, as well as other organizations, now struggle to manage identities and access requests because the data resides in various locations and business units.

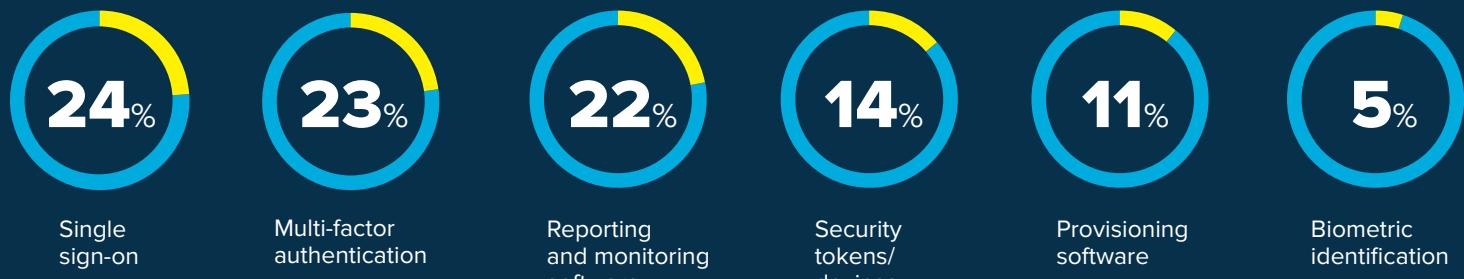
BY 2020, EVERY PERSON
ONLINE WILL CREATE ROUGHLY
**1.7 MEGABYTES OF NEW
DATA EVERY SECOND.**

Source: Identity Management Institute

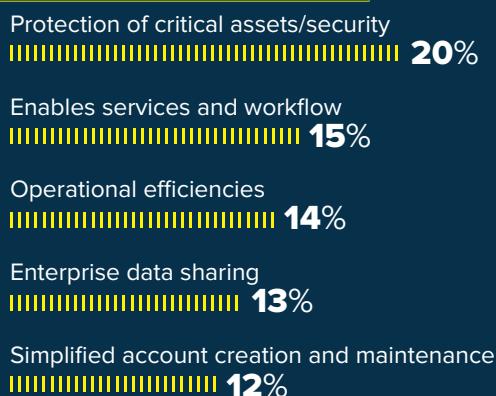
IAM BY THE NUMBERS

The Center for Digital Government* surveyed state and local gov tech leaders on the status of identity access management efforts in their jurisdictions. Here are some of the findings.

MOST COMMONLY USED IAM TECHNOLOGIES:



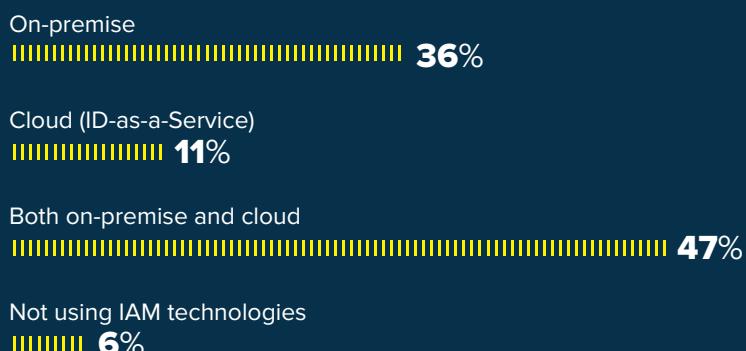
WHY USE IAM?



BIGGEST ROADBLOCKS: WHAT STANDS IN THE WAY OF IMPLEMENTING IAM?



CLOUD OR NOT? WHERE DO IAM TECHNOLOGIES RESIDE?



ROLE OF THE CISO

Sixty-eight percent of respondents report having a chief information security officer. Here's how those with a CISO characterize their role relative to IAM:



The growth in mobile technology has also complicated the adoption of IAM. “People use their mobile devices to access corporate systems and so there needs to be some segregation between the corporate data and personal on the mobile devices,” said Bagdasarian. As governments initiate more BYOD policies, the issues around identity and access management across multiple devices must be addressed early on to avoid problems down the road.

But the problem with IAM isn’t just one of rapid and continuous technological change. It’s also a governance issue. “Organizations lack centralized identity governance,” said Bagdasarian. “This is causing a delay in consolidation of identity directories.” That delay can be tied back to the fact that people will use the same credentials, such as email passwords, to access different standalone systems. Trying to track, monitor and update all those passwords for so many systems has become a daunting task.

Moraetes points to the lack of centralized access management solutions, such as enterprise directories and single sign-on, as key impediments to IAM solutions, along with the ongoing issue of outdated provisioning processes that are manual and inconsistent between business units or agencies, in the case of government. Inadequate provisioning and manual user certification and accreditation operations can slow down and impede how well users can access useful information and, in worst cases, lead to security problems.

Pulling IAM Together

One of the biggest security threats to government is credential harvesting, where hackers use phishing scams to obtain a user’s password or identity credentials and gain access to important data. The first line of defense against this problem is the use of multi-factor identification, which can keep hackers and data thieves from gaining access to cloud applications and other systems, said Bagdasarian.

Another strategy is to create a holistic IAM solution within government. A white paper, *The Challenges and Benefits of Identity and Access Management*, published by F5 Networks, points out that

WITHOUT A RIGOROUS PROCESS IN PLACE, ORGANIZATIONS RUN THE RISK OF TAKING A USER OFF OF ONE SYSTEM BUT NOT ANOTHER WHEN THEY LEAVE, CREATING A SECURITY PROBLEM.

comprehensive IAM includes “centralized access management, automation, reporting and contextual application of security policies” as the key ingredients to meeting today’s IAM needs. That means an end to silos for data, regulatory compliance and information security. Patchwork approaches are no longer acceptable if enterprise IAM is to take root.

An important element to making this happen is the role of the chief information security officer. Moraetes said that the CISO and his or her team can “vet identities, approve appropriate access entitlements, and grant or revoke user identities, access and entitlements in a timely manner,” while enforcing compliance within an organization’s IAM policy. Forrester’s Andras Cser said the role of the CISO has become pivotal as far as IAM is concerned, given how security continues to be a high priority. “They have to pull all of this together for centralized control in IAM.”

Advances in technology also promise to make IAM an easier lift than it has been in the past. For example, Microsoft’s Office 365 offers dual-factor identification. But the new trend is in middleware companies that offer solutions to centralize identity directories, which can facilitate single sign-on and multi-factor authentication across all systems, according to Bagdasarian.

These firms, such as OneLogin, Okta and Ping Identity as well as familiar names such as IBM Cloudant, Oracle Identity and Microsoft’s Azure Active Directory, are identity-as-a-service platforms that simplify the tedious work of onboarding and offboarding users. This process has become more important as new compliance regulations require organizations to certify how they provide access to their systems on a quarterly basis, said Bagdasarian. “Without a rigorous process in place, organizations run the risk of taking a user off of one system but not another when they leave, creating a security problem,” he said.

Make that Robust IAM

By 2020, every person online will create roughly 1.7 megabytes of new data every second, according to the Identity Management Institute. Meanwhile, the number of Internet of Things devices is expected to reach 31 billion in the same year and rise to 75 billion by 2025. By 2020, 83 percent of enterprise workloads will be in the cloud, while on-premises computer work will shrink to just 27 percent.

The environment in which state and local governments operate will mirror those trends. In addition, the amount of data sharing will increase as policymakers see the value in providing cost-effective, integrated applications that serve the public good. A shrinking government workforce will mean a single worker using tools that holistically draw data from shared resources and can handle multiple tasks that used to require many workers. But this requires a robust IAM.

The bottom line is that identity and access management will be essential to the future of how government operates. A well-designed, well-managed IAM will reduce friction when it comes to data sharing while helping to provide the level of security that is now mandatory. An inadequate and balkanized IAM operation will slow down and impede the progress. The public won’t realize this and policymakers will not understand the reason behind the problem, but CIOs and their peers will be on the hook if IAM isn’t modernized and made workable at the enterprise level. 

tnewcombe@govtech.com



SPECIAL
DISTRICTS
PROGRAM



Creating Better Communities.

Special Districts are driving smart tech and innovation across the country. Read their stories, get the stats & connect with the community.

Download the guide:
govtech.com/districts



AN AT&T
PROGRAM

government
technology



STATES OF IDENTITY



Grappling with security and data access, here's how four states are working toward a single log-in credential.

BY DAVID RATHS

When it comes to identity and access management (IAM), state IT executives want to emulate the solutions developed by retail giants such as Amazon. “Think about how citizens access their favorite retail website,” said Erik Avakian, chief information security officer of Pennsylvania. “They can go to different areas of the site and buy what they need with one unified credential.”

Modeling itself on today’s digital retail world, the Keystone state is integrating identity proofing, social media log-ins

and password strength meters. “These are things people expect when they go to other major websites, so we are trying to bring that type of experience to government,” he added. “Regardless of the agency they are doing business with, citizens will have a unified credential they can use across multiple applications.”

To some people, IAM might seem like a technical security issue about back-end authentication between systems. But it also serves as a cornerstone of digital business. Without an enterprise-level IAM strategy, state agencies will

continue to operate in a siloed fashion, and each application will require its own password system and identity-proofing solution.

“As more states move to implement digital government strategies, identity comes into play, because it is part of securing those types of transactions and enabling the digital experience,” said Avakian. But what is the best approach? Four states have tackled IAM at the enterprise level, creating laboratories for possible success elsewhere. Here are their stories.

Utah: IAM Veteran

Some state governments have been working on single-sign-on (SSO) capabilities for years, while others are planning their first pilot projects. But executives have come to accept that IAM is less of a one-time project and more of a discipline. "Like security, IAM is a lifestyle," said Gartner analyst Kevin Kampman. "It is not going to go away. The objectives change, the terrain is changing, the needs are changing, and you need to be able to adapt to that."

Dave Fletcher, Utah's chief technology officer, noted that IAM is tied to security, and the threat environment is always changing. Adapting to that reality requires adding new features such as multi-factor authentication. "We also need to be able to integrate a growing number of cloud services with our sign-on solution," he said. "It is a constantly moving target."

Utah has been working on SSO capabilities since 2002, primarily focused on provisioning and deprovisioning employees

"Like security, IAM is a lifestyle. It is not going to go away."

— Kevin Kampman, Gartner

and enabling access to the applications they need for their jobs, Fletcher said. Utah ID provides access to about 900 different applications and services. Now the state is applying that approach to business- and citizen-facing applications as well. Utah provides more than 1,300 online services, and more than half provide services to businesses.

In 2016, legislation was passed that requires the Department of Technology Services (DTS) to create a single-sign-on business portal. With a budget of \$1.3 million annually, the first phase of the portal is expected to be completed in July 2019. The new portal works primarily with four agencies: Tax Commission, Department

of Workforce Services, Labor Commission and Department of Commerce. Business owners will be able to sign up for notifications, such as a tax payment deadline; and service providers, including accountants and attorneys, will have the opportunity to manage multiple businesses.

Utah is not stopping with business owners. DTS is working with the state Medicaid agency to integrate its applications into the SSO effort. "The thing that initiated the business single sign-on was that some legislators wanted to extend that type of service to the citizens at large," Fletcher explained, "so this business portal is just the first step."

Fletcher explained that the portal will become a common eligibility system that cuts across all of the health and human services departments as well as unemployment, making them fully integrated and easier to use. Eventually DTS wants to take it beyond state agencies to local governments as well.

**Dave Fletcher,
CTO, Utah**



Michigan: Impressive Progress

The state of Michigan is another example that shows you are never really done with IAM. It has been working on its MILogin enterprise IAM solution for more than five years, with different use cases for employees, businesses and individual citizens. Citizens can use MILogin to renew their driver's license, hunting license or fishing license. Employees across all agencies now use MILogin to access the statewide enterprise and resource planning system called SIGMA, said David DeVries, who recently left the position of CIO and director of the Department of Technology, Management and Budget.

By almost any measure, the state has made impressive progress. Almost 230 Web and mobile applications are integrated behind MILogin, and more than 4 million Michigan citizens have logins. "We have an established program here," DeVries said. "Our challenge has been, and still is, to keep up with the technology because it is constantly changing."

DeVries established a policy that all new software programs and all major rewrites or upgrades will have MILogin as their front-end identity piece. Several systems are going live with the SSO log-in in 2019.



**David DeVries, former
CIO, Michigan**

DeVries pointed to the state's new vehicle registration system that will be using the MILogin, which he anticipated going live in February. "Our main requirement was that the vendor was not going to bring his own log-in system to use. They were going to incorporate ours. We are forcing that through the other programs. That is another challenge: how to encourage that, enforce it, and then keep the cost down."

Pennsylvania: Helping Agencies Modernize IAM

In 2013, the National Institute of Standards and Technology awarded grants to Michigan and Pennsylvania to pilot identity management solutions. That started the conversation in Pennsylvania on how to streamline the citizen experience and enhance security and has led to the Keystone Login SSO initiative. "We want to get to a unified credential that is secure and provides different levels of assurance depending on the type of transaction the citizen is trying to do," said CISO Erik Avakian.

If a citizen is applying for benefits, that may require identity proofing, he explained. Here is how that works: A user can provide information from their driver's license or state ID card, which is then verified by the Department of Transportation based on an exact match of the information provided. Or the person can undertake a knowledge-based authentication, which is currently provided as a service by Experian. The constituent is asked for identifying information (name, address and other optional pieces of information). Experian matches the user against its data system and returns a series of multiple-choice questions that the constituent should be able to correctly answer. A score is then returned based on the responses and other criteria such as the vendor's fraud alert system.

Pennsylvania is seeking to move beyond siloed applications that require citizens to have user logins and passwords for multiple sites. "All these different user names and passwords are frustrating to the citizen and less secure because they have to remember all of them," Avakian said. "The experience is disjointed. Keystone Login gets us beyond that."



**Erik Avakian, CISO,
Pennsylvania**

One application that has gone live with Keystone Login is a financial disclosure application used by more than 10,000 current and former employees to file annual Statements of Financial Interest under the State Ethics Act and/or Governor's Code of Conduct (an executive order). Approximately 30 applications are scheduled to go live in 2019, including the voter services portal, business registration and professional licensing and an enterprise grants portal.

Pennsylvania's Office of Information Technology is trying to get agencies to see Keystone Login as part of their legacy modernization process. "As agencies modernize or move to a new version, we say as part of this version, let's migrate you to Keystone Login instead of using your own directory," Avakian said. "We have APIs to help agencies come on board; there is an onboarding guide, and a communications plan put into effect. We have been working hand in hand with the agencies and have an applications team available to help them. It is definitely something the agencies need help with. But we didn't do it in a silo; we are all moving together."

Indiana: Creating a Holistic View of Citizens

Indiana expects several agencies to go live with its Access Indiana SSO solution in 2019. The state's Office of Technology and Management Performance Hub have been working since 2017 with four of the state's largest citizen-facing applications from the Bureau of Motor Vehicles (BMV), Health and Human Services, Workforce Development and the Department of Revenue.

Graig Lubsen, communications and marketing director at Indiana's Office of Technology, sits on three of the four working committees involving Access Indiana. He said Indiana sees SSO as a first step toward the state taking a more holistic view of citizens and the services they access by creating a single client account across agencies. "If you don't have everybody using the same credential, you can't have a singular view of a person or citizen from the state government's perspective," Lubsen said. "We had to tackle single sign-on first."

Better understanding citizen interactions with state government could lead to the state being able to recommend services that they would either qualify for or could be interested in, according to Dewand Neely, the state's chief information officer. "The state could maybe utilize the citizen information to save money, such as on mailing costs by being able to centrally verify a person's

address. We can also develop a central portal for a citizen to manage their experience with state government, customizing the design to show things the user interacts with or messages that are of interest."

The state chose to work with NIC subsidiary Indiana Interactive to build the solution. "Initially we were using another off-the-shelf product from a major technology company, which we had in place for INBiz, our business one-stop portal," Lubsen explained. "But as we developed the requirements, we found that there were too many restrictions on what we could do with that solution, so we chose to build our own." (For instance, adding multi-factor authentication would have been too expensive using the previous solution, he said.) "We have saved a bunch of money and were able to add flexibility in terms of password requirements and the user flow and experience."

Like other state IT execs, Neely and Lubsen have found that legacy system integration is a more involved process: "Our Department of Homeland Security has a public safety portal that is being built from scratch," Lubsen said. "We were able to add the sign-on component with only 10 hours of development work. With the BMV, their system is older and it took them weeks to do."

Neely explained that from discussions with agencies early in the development

process, his team is aware that each new agency will have unique needs. "This has shown itself from various password complexity requirements or even the password history. It's important that we have phases where we bring in agencies over time and not bite off everything at once. This means Access Indiana must be resilient, scalable and flexible to meet these demands."

Integration work for the BMV and Department of Revenue is already done, but the state may wait until other agencies are ready to make a "bigger bang" as they all go live with Access Indiana together, Lubsen said.

Indiana has found that good governance is a key part of the IAM process. The work is led by an executive committee made up of the heads of all participating agencies and the governor's office. There also is an advisory committee of the IT directors and a marketing committee made up of communications directors from each of the agencies. A call center committee was established to determine how the state was going to handle calls about creating an account. They chose to outsource that work to a third party. "We didn't want to throw that onto the agencies, and we need to have 24/7 support," Lubsen said. "We tried to look at it from all the angles and make sure these committees are composed of subject matter experts to drive the process forward."

Through Indiana's governance structure, the IAM team accepts feature requests from all project partners and then each partner rates how high a request is ranked. "There are currently 16 items in our backlog, such as strengthening confidence in user identities, which are being sorted by order of importance, based on agency votes."

Gartner's Kevin Kampman encourages IT leaders to see IAM as an evolution as they work with agency partners. "It doesn't take long before you realize that, like security, identity touches every activity you do, so you need a comprehensive approach to identity in order to succeed," he said. "Otherwise, it is just like driving on a rocky road: You are going to have bumps all the way. You want to be able to smooth that out by having a consistent and shared view of how you deal with identity in different contexts." 

DAVID KIDD



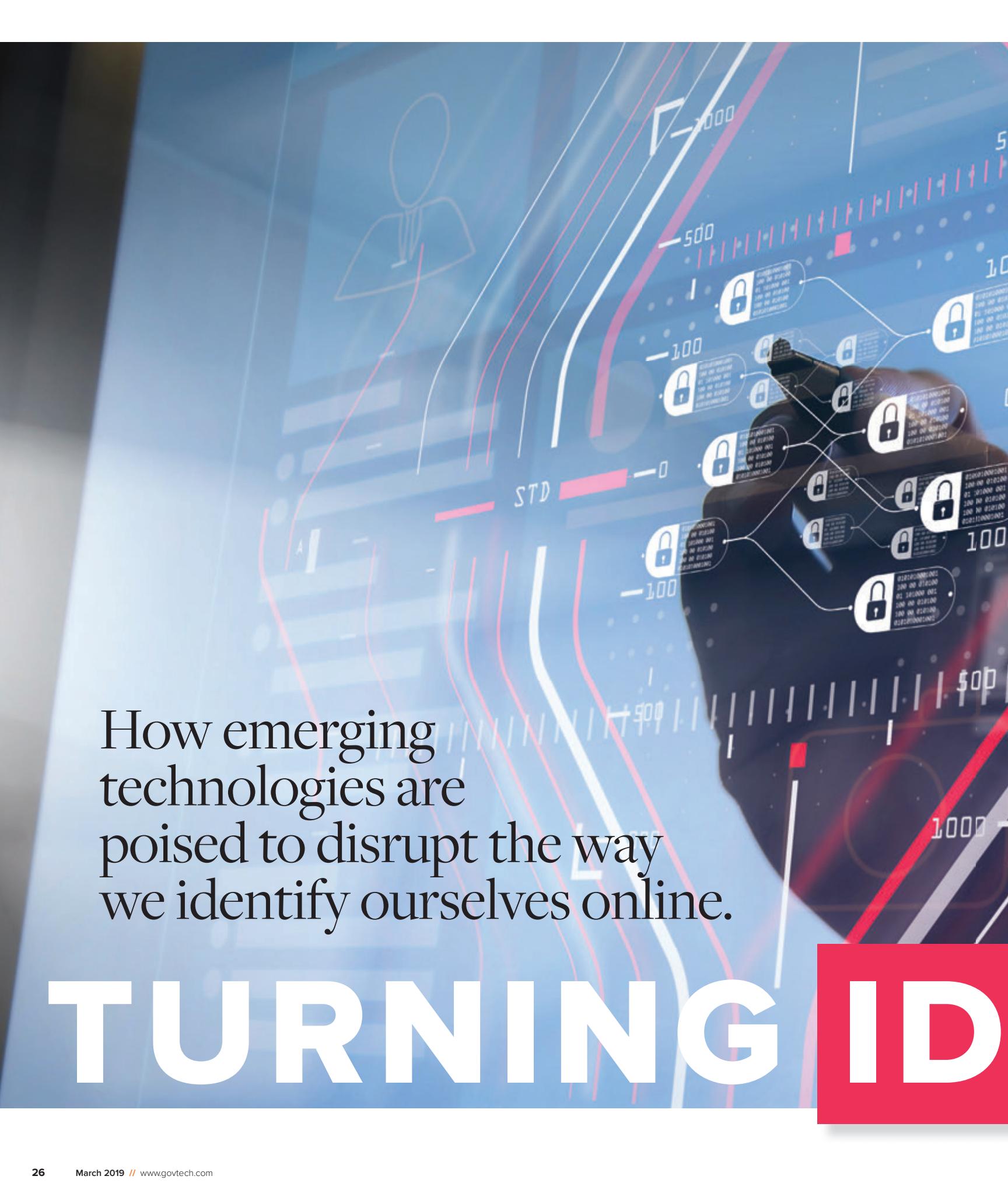
**Dewand Neely,
CIO, Indiana**

Stay up to date on the latest trends and gain insights into some of your most pressing challenges.



Visit our website for some of our most recent work!
www.govtech.com/library

government
technology



How emerging technologies are poised to disrupt the way we identify ourselves online.

TURNING ID



BY ADAM STONE

INSIDE OUT

SHUTTERSTOCK.COM

As a technology innovation leader in the Illinois Department of Commerce, Jennifer M. O'Rourke struggled with the sheer volume and complexity of identity and access management, or IAM.

"As we looked to provide a particular organization with a tax credit, there were audit points that included other organizations, but we kept those resources in isolated, segmented, disparate systems," said O'Rourke, now co-founder and president of identity technology firm Attest. "There was no efficient, portfolio-level way in which a given individual or organization could engage with the department."

Across government, technology leaders and business-line managers rank IAM as a foremost concern: In 2018 the National Association of State Chief Information Officers (NASCIO) included identity on its top 10 list of state tech priorities for the first time. A number of factors have come together to make IAM a pressing issue:

- Citizen access is expanding, with taxpayers logging into a variety of state and local systems. Loose control over IAM leads to fragmentation and excessive complexity, not to mention a poor citizen experience.
- The rise of cloud technologies creates a range of new access points for government employees, whose identity must be verified and validated across both legacy and emerging platforms.
- Rising mobile access among both citizens and government workers creates an additional vector for IAM.
- Regulatory and compliance constraints put added pressure on government to ensure proper management of beneficiary identity and other aspects of IAM.

Biometrics and multifactor authentication have helped validate user identities, but these tend to be tech-heavy solutions and



they aren't always user-friendly. IT leaders are looking toward the next iteration.

The vendor community is eager to assist: Grand View Research sees the IAM market reaching \$22.68 billion by 2025. Before the spending starts, it's worth looking at some of the main tools currently emerging on the IAM landscape, including cloud-based controls, artificial intelligence and blockchain.

CLOUD-BASED MANAGEMENT

The rise of cloud computing creates new challenges around IAM, but also offers new solutions.

Move to the cloud and IAM leaves the familiar (if clunky) confines of your legacy environment. You may work with multiple cloud providers, each with its own unique security controls. This creates the potential for confusion and complication. But cloud also brings its own remedies.

Cloud providers and third parties may offer identity as a service, or identity as a platform. "These tools create a central identity database that integrates with your internal directory. Through that they manage a single sign-on and multi-factor authentication, and they can identity life cycle management," said Henry Bagdasarian, executive director of the Identity Management Institute.

"SAY SOMEONE PUTS THEIR INITIALS INSTEAD OF THEIR FULL NAME, BUT EVERYTHING ELSE SEEMS TO MATCH. MACHINE LEARNING COULD HELP YOU TO CONSOLIDATE THOSE RECORDS ON A LARGE SCALE."



Google, for instance, boasts that its Cloud Identity tool “makes it easy to provision and manage users and groups, set up single sign-on, and configure multi-factor authentication” directly from a central console. All the major cloud providers claim similar capabilities. Some will also offer identity governance services, helping to create policies for identity management, while others may deliver authentication services in support of multi-factor authentication.

Centralization is the key asset here. By leveraging the cloud to create a central directory, IT leaders can gain a global view of IAM, integrating their legacy and cloud iterations in a common touchpoint. “You want to centralize and automate as much as possible. You don’t want your system admin to have to go one by one removing and adding people,” Bagdasarian said.

When Jennifer O’Rourke was innovation leader at the Illinois Department of Commerce, she encountered the complex problem of identity management. Now as co-founder and president of Attest, she and her team are using blockchain to consolidate and track citizen IDs.

AI AND MACHINE LEARNING

In the big picture, IAM seeks to manage identity, ensuring that those who interact with government systems are who they claim to be. In a more granular sense, though, IAM puts the emphasis on access — it’s about limiting who gets in, and where.

Some experts point to rising capabilities around machine learning and artificial intelligence as a potential boon to access management. AI can see into the inner workings of a system with a speed and volume unmatched by human senses.

“Imagine I’m looking at a dashboard showing how many logins I had today, how many people requested access to a system, how much traffic we are seeing,” said Sarah Squire, co-author of the 2017 NIST Digital Identity Guidelines.

“AI can look for those same types of things and it can crunch way more data,” said Squire, now senior technical architect at IAM solutions firm Ping Identity. “It can also see much more subtle patterns. It can find anomalies: No one has ever logged into your government system at 3 a.m. from China before. That’s weird. Let’s tell someone or block that access.”

An instructor with the SANS Technology Institute, Kenneth G. Hartman says this kind of access control could be the low-hanging fruit for AI. “The simplest examples are when I am known to be in San Francisco and someone is using my identity in China. That automatically triggers an alarm,” he said. “What’s interesting about AI is that it can detect even more subtle patterns, things we as humans might

not notice. I normally log in at 9 a.m. and then I start coming in at 7 a.m. and maybe there are algorithms that pick up on that.”

AI and machine learning could help on the identity management side as well, for instance by cross-checking the veracity of citizen data across multiple fragmented databases. “Suppose you have data that isn’t consolidated and there is a discrepancy,” said Gartner Senior Analyst Kevin Kampman. “You might be able to use machine learning to spot that. Say someone puts their initials instead of their full name, but everything else seems to match. Machine learning could help you to consolidate those records on a large scale.”

BLOCKCHAIN

On the cutting edge of IAM, there’s blockchain, the shared immutable ledger technology best known as the infrastructure that supports bitcoin and other cryptocurrencies. Those key descriptors — shared, immutable, ledger — make some believe that blockchain could serve as a formidable new implement in the IAM toolkit.

At Attest, O’Rourke and her team have a product in beta (due for a Q1 2019 release) that includes a “wallet” wherein citizens can digitally establish their identity on blockchain, and a pair of APIs that government could use to connect with citizens seeking to authenticate themselves in this way.

One advantage here lies in the validity of the credential. A physical driver’s license can be altered, whereas with a cryptographically endorsed digital credential, “it is immutably

clear that the driver's license has in fact been issued by the DMV," O'Rourke said.

Moreover, the identity rests in the hands of the citizen, potentially freeing government from the laborious upkeep of those many, fragmented IAM repositories. "For the first time, a user can have a natively digital attribute, something about themselves, and they can be the holder of that, as opposed to the current state where all the different government departments are the authors or writers of this information and the holders of this information," she said.

Former Utah state CIO Phillip Windley chairs the Sovrin Foundation, a nonprofit that is using blockchain to back up identity. In Canada the organization has worked with banks and employers to launch initial forays into what it calls "self-sovereign identity," the idea of a decentralized identity that is more about who you are and less about who issued the credential.

"We don't want government to be the central identity player and we certainly don't want Google or Facebook to do that either," Windley said. "So we create a decentralized network where the parties issue

be used to identify constituents who could benefit from that and who haven't signed up for some reason," Kampman said.

This example highlights the potential for IAM to make government more user-friendly, but it also highlights the inherent risk in any new IAM evolution: When you tinker with identity, you skirt the edge of privacy.

"You have to be careful when there is sensitivity around personal data," Kampman said. Whether it's AI or any identity-related effort, "you need governance over this to be clear about what can be used and what can't be used for a given purpose. You are a custodian of data and when you aggregate that data your responsibilities increase exponentially."

Broadly, the looking-before-leaping paradigm is in full force here. As government IT leaders and their business-line peers seek to better manage access and identity in an emerging cloud-driven enterprise, they'll need to be thoughtful not just about the how, but about the why behind their efforts.

"There needs to be a strategy," Kampman said. "What is the outcome going to be? The technology world can solve these problems but it needs to be done with a viewpoint toward how it will appear to the end user. You want to have control over the technologies but you also want all the stakeholders to have an opportunity to contribute toward governance."

Some, meanwhile are looking over the horizon to an IAM end game in which all these pesky log-ins and multiple identities and siloed access management apparatus just ... go away. They envision a world where people simply are who they say they are.

Some describe it as contextual identity. You typically log in from this device, in this place, at this time. You type this fast, using these keys, with a browser configured in this or that way. Taken together and smashed through appropriate algorithms, this data could serve to identify a user with little to no further fuss.

"We want a situation where our security is so good, we can tell whether you are an attacker or a valid user just through your traffic," Squire said. "Our holy grail is zero log-in." 



17% OF SURVEYED STATE AND LOCAL GOVERNMENT LEADERS SAY THEY WOULD CONSIDER USING BLOCKCHAIN FOR IAM. ANOTHER 36% SAID THEY MIGHT.

SOURCE: CENTER FOR DIGITAL GOVERNMENT

Blockchain credentials would have the advantage of being sharable across all government offices. In the absence of a central identity database — which many citizens would find more than a little creepy — government could leverage blockchain as a way to consolidate its IAM needs.

"In the ecosystem today, there is no one single entity that has certificate authority. There is no central place where all the participants can consistently go to in order to validate a document or a relationship between an individual and, say, the department of motor vehicles," O'Rourke said. Blockchain could deliver that central touchpoint, without the Orwellian overtones of a central ID database.

In fact, some say the greatest value of blockchain lies in the possibility that it could get the government out of the identity business entirely.

credentials about whatever they know about. The bank issues a credential saying that I am a customer. My employer issues me a credential saying that I work in a certain place."

The idea is nascent, but it has its supporters: IBM has partnered with Sovrin and has even produced a GitHub tutorial on self-sovereign identity.

BEYOND ACCESS

If government were to pursue these emerging IAM methodologies, some say, it could reap added benefits, beyond just access control.

Take AI for instance. The immediate benefit is clear: Let's stop those 3 a.m. logins from China. But AI could have broader applications across identity management as well. "Say the county is trying to act as a buyer for electrical power and they want to give constituents a discount. AI could



SPECIAL
DISTRICTS
PROGRAM

Join us at the Summit.

With five regional events and an awards program designed for you, it's never been easier for Special Districts to connect and celebrate innovation.

Register. Nominate. Participate.
govtech.com/districts



AN AT&T
PROGRAM

government
technology

Muni ID Cards on the Rise

States issue valid identification in the form of drivers' licenses and other IDs, and the federal government issues official documents like passports and Social Security cards. But over the last decade, a new way residents can present themselves for official purposes has been on the rise: the municipal ID card. Cities — and a handful of counties — have begun to issue ID cards that let residents who do not hold a driver's license access benefits specific to their jurisdiction. The cards are often promoted to young people, the elderly, homeless residents and immigrants. They can be used to access food assistance, library services and discounts at local businesses. Here's a look at a sample of the nearly 20 cities large and small that *GT* found running municipal ID programs. 

Oakland, Calif.

Name: Oakland City ID

Agency: Oakland City ID

Date Launched:

February 2013

Services Available: Proof of ID to local police and other authorities; access to homeless services; open a bank account; access food assistance

San Francisco

Name: SF City ID Card

Agency: Office of the County Clerk

Date Launched:

January 2009

Services Available: Medical and allergy information on the cardholder; ID for opening a checking account; public library card; local discounts

Richmond, Calif.

Name: Richmond City ID

Agency: Richmond City ID

Date Launched: October 2014

Services Available: Prepaid debit card; proof of ID to local police and other authorities; valid for use at community college; food assistance programs







A Mobile Identity

Louisiana's launch of a digital driver's license puts it ahead of other states working to get government IDs on smartphones.

By Skip Descant / Staff Writer

Drivers in Louisiana may want to leave their driver's license at home, as long as they remember to take along their phone as they head out the door.

The state has recently introduced a digital driver's license that resides on smartphones, making Louisiana an early adopter of technology that moves one of the most ubiquitous pieces of government documentation and identification from wallets to mobile devices.

"I'm all for technology," remarked Rep. Ted James, a state legislator from Baton Rouge, who introduced the bill in 2016 to allow for a digital driver's license. James' interest in technology seemed to gel with the state's commissioner of motor vehicles who was also interested in exploring technology improvements around drivers' licenses.

The bill was passed about two years ago. It then took another year for Envoc, a private software development firm based in Louisiana, to develop the app. The digital license, sometimes referred to as a DDL, officially launched in July 2018.

"The first thing is folks want to be able to use it for everything," said James. "I still encourage people to have a physical driver's license, because it's not mandated that other entities accept it, outside of law enforcement," he added.

The digital driver's license, which resides on a driver's smartphone, is acceptable by law enforcement in the state. It has also recently been given the green light by the Louisiana Office of Alcohol and Tobacco Control, which means the "digital credential" — in the parlance of technologists and state officials — is acceptable identification for the purchase of alcohol and tobacco.

"But of course the holy grail is TSA — to be able to use it at the airport," said Calvin Fabre, founder and president of Envoc. "We are talking with them."

Some retailers will recognize and accept the digital driver's license, but many are still in the dark as to the app's legitimacy, said James.

"A store may ask that you produce a physical license. So I encourage people to have both," he added.

To get a digital driver's license, Louisiana motorists need to first download the free LA Wallet app, which then sets up the process to get their virtual license, which costs \$5.99. So far, about 77,000 people have downloaded the app, with about 41,000, or between 2 and 3 percent of the driving population, who have activated the purchase of the license.



"Now, this is before any major marketing," said Fabre. "We will be starting a big campaign in 2019 to build awareness."

Louisiana seems to be ahead of the curve on a trend toward developing digital drivers' licenses. Several states are in various stages of development.

Iowa is one of the states developing a DDL. "Most recently, we have exited the planning stage of the project and are excited to now begin undertaking the development stages of the project," said Mindi Nguyen, project coordinator and liaison for the Iowa mobile drivers license project. "For the current schedule, we're looking at an anticipated go-live, or public release, in early spring 2020."

Other states like Colorado, Idaho and Maryland, along with the District of Columbia, have piloted digital driver's license projects; however, a statewide

rollout of those programs has not yet occurred.

The digital driver's license in Louisiana has the potential to serve other purposes beyond simply standing in for the physical document, say Envoc officials. The app includes a feature known as VerifyYou, which allows it to verify the validity of another LA Wallet digital license or physical driver's license. So for example, a bouncer outside a bar could conduct a real-time check of a patron's digital driver's license with the DMV.

"The app will also do that with a physical printed license, which means that I can now scan a physical hard license with my app, and that can go back to the DMV, and verify you in real time," Fabre explained. "So now we're doing real-time identity verification, using the app, even with the old-school license. It could also

be used to verify someone who shows up at your house to perform a service," he added.

A next step will be to work out the reciprocity agreements for other states to both develop digital licenses and accept those from Louisiana. Also, the ability to easily verify the validity of a digital driver's license could make the delivery of age-verified products like alcohol purchases easier.

"We think that this is going to help us pioneer alcohol delivery with Waitr and Uber Eats," said Fabre, calling to mind a common restaurant delivery service in the southeastern U.S. "So imagine you're ordering a pizza to be delivered to your house, maybe through Domino's or Waitr or Uber Eats. And you want a bottle of wine to go with it." **gt**

sdescant@govtech.com



Safety First

Following stories like the December 2018 incident in which an Amazon robot sprayed two dozen workers with bear spray, the e-commerce giant is taking steps to protect warehouse employees from their AI counterparts. The Robotic Test Vest, designed by Amazon engineers, is a worker safety wearable that alerts worker-bots to a human's presence when they enter an area to repair or otherwise work around the bot. The idea is that the bot will work together with the human to avoid collisions. The vest has been rolled out to more than 25 sites. SOURCE: TECHCRUNCH



JUMPING IN: In the push to get more kids involved in STEM education, Microsoft has expanded its software that teaches visually impaired students basic coding skills. Launched in the UK in 2017 under the name Project Torino, and now called Code Jumper, the project is expanding to the U.S. Microsoft gave all the technology and research that went into the software to the nonprofit American Printing House for the Blind, who will also work to bring Code Jumper not only to the U.S. but also to Canada, Australia and India by the end of 2019. Rather than the drag-and-drop tools students often use to learn to code, Code Jumper has kids physically connect plastic pods together with their hands to create programs, a big leap forward for tech education accessibility. SOURCE: GIZMODO

\$57M

IN JANUARY, privacy regulators in France fined Google \$56.8 million for not getting proper user consent before showing targeted ads online and for making their privacy disclosures too difficult to access, violating the General Data Protection Regulation (GDPR) laws that went into effect across Europe last year. Google claims it gets consumer consent, but French watchdog group CNIL found the company's process to be unsatisfactory. Among other issues, the group wrote, "the information communicated is not clear enough so that the user can understand that the legal basis of processing operations for the ads personalization is the consent, and not the legitimate interest of the company." This was France's first enforcement of GDPR regulations. SOURCE: GIZMODO





◀ Contact Work

The new Dell 75 4K Interactive Touch Monitor (C7520QT) lets users write or draw in real time with virtually no lag on the monitor's 20-point multi-touch InGlass screen using their fingers, palm or styluses — all at the same time. Optimized fonts ensure consistently sharp visuals and vivid colors from virtually anywhere in the room thanks to the wide viewing angle enabled by IPS technology. Whether people are viewing the screen under natural or fluorescent light, they'll experience consistent onscreen clarity with anti-glare and anti-smudge coating. Buttons at the side of the panel enable users to lower the displayed image to three different height settings. www.dell.com

Unveiling Productivity ▶

HP has released the Spectre Folio, a convertible PC made with 100 percent real leather. The device contains an 8th-generation Intel Core i5 or i7 (Y-series) processor and its battery lasts up to 19 hours. The computer moves easily from a traditional laptop position to a tent position that neatly tucks away the keyboard for sturdier support on the lap, to a tablet position with a built-in tilt — all made possible by strategically placed magnets and the unique flexibility of leather to act as a natural hinge. Other features include up to 16 GB of memory and up to 2 TB of SSD storage. www.hp.com



◀ Brilliant Display

InFocus Corp. re-introduced the ScreenPlay projector line with two models — the SP2080HD, which provides bright, 4,000-lumen images in full 1920 x 1080 HD resolution, and a high 32,000:1 contrast ratio for sharpness and depth; and the SP1081HD, also in full 1080p resolution, which has 3,800 lumens and 28,500:1 contrast. Users can add either projector to almost any space; InFocus BrilliantColor technology enables the units to project vivid, accurate colors on many surfaces and in virtually any light. Powered by the latest DLP technology, the SP1081HD and SP2080HD can accept content from various sources and can display 3-D content from PCs, Blu-rays, game consoles and more with 144Hz DLP Link 3D glasses (sold separately). www.infocus.com



For more product news, log on to explore *Government Technology's* Product Source. govtech.com/products

Read full reports and breaking news about career changes across tech-driven roles in government at govtech.com/people.



Todd Nacapuy

CIO Transition in Hawaii

At the start of the new year, **Todd Nacapuy** stepped down as Hawaii CIO to return to the private sector to work for Hawaii Employers' Mutual Insurance Company. He served in the position since 2014. Gov. David Ige named **Douglas Murdock**, a former state comptroller and vice president of fiscal affairs for the state tourism agency, to head the Hawaii Office of Enterprise Technology Services.

New Vermont CISO

Vermont tapped **Nicholas Andersen** to be its new chief information security officer in December. Andersen brings 12 years of cyberexperience to the role, including work with U.S. military organizations, including the FAA, Department of Homeland Security and the U.S. Marine Corps Cyber Command.



David DeVries



Tricia L. Foster

Tech Turnover in Michigan

Michigan CIO and Director of the Department of Technology, Management and Budget (DTMB) **David DeVries** stepped down ahead of the new governor, Gretchen Whitmer, taking office at the start of the year. He was appointed by former Gov. Rick Snyder in August 2017. Whitmer named **Tricia L. Foster** to take over as director of DTMB; as of press time the state had not named a new CIO. In February the state announced **Chris DeRusha** as its new chief security officer. DeRusha was previously deputy CSO for DTMB, and held security roles with the U.S. Department of Homeland Security and the Obama administration.

Innovative Changes in South Bend

After more than five years serving as CIO of South Bend, Ind., **Santiago Garces** resigned to become director of Pittsburgh's Department of Innovation and Performance. At the end of January, the city named **Denise Linn Riedl** to fill the role. Riedl previously held positions with the City Tech Collaborative in Chicago, the Smart Chicago Collaborative and the Federal Communications Commission.

New Tech Secretary for New Mexico

Ahead of her inauguration Jan. 1, New Mexico Gov. Michelle Lujan Grisham announced **Vincent Martinez** would be taking the lead as secretary of the Department of Information Technology and state CIO. Martinez brings both public- and private-sector experience to the position, having most recently served as the state's managing director of cloud and communications.

Several Illinois IT Leaders Depart

Illinois saw a brisk turnaround of IT leadership as the governor's office changed hands. Following the retirement of Kirk Lonbom in December, outgoing Gov. Bruce Rauner named CTO **Jack King** as Illinois' interim CIO just before the inauguration of new Gov. J.B. Pritzker; about one month later, King and CISO **Chris Hill** announced they would return to the tech sector. The Department of Information Technology's Chief Strategy Officer **Shanna Rahming** and Chief of Staff Tyler Clark departed in February.

Washington, D.C., Names Acting CTO

Lindsey Parker was appointed by Washington, D.C., Mayor Muriel Bowser to the post of acting CTO, taking over from Barney Krukoff, who had served as interim CTO for the previous year. Parker was previously deputy chief of staff in Bowser's office and brings tech leadership experience from her work at Symantec.

The Survivors

These state IT leaders held on to their positions despite governor transitions.



**Lee Allen,
Kansas**



**David Cagigal,
Wisconsin**



**Stephanie
Dedmon,
Tennessee**



**Michael
Dietrich,
Nevada**



**Greg Zickau,
Idaho**

Minnesota CIO Steps Down

After nearly a year in the position, **Johanna Clyborne** stepped aside as lead of Minnesota Information Technology Services in early January, ahead of incoming Gov. Tim Walz appointing new cabinet officials. As of press time she had not announced her next move.



Johanna Clyborne

Permanent CISO in Washington State

In January, Washington state announced **Ronald Buchanan** as its new chief information security officer. Prior to the appointment he served as chief information risk officer and IT director of the Information Security and Privacy office for the Oregon Health Authority and Department of Human Services. Washington's acting CISO ahead of Buchanan was Scott Bream, although the role was previously filled by Agnes Kirk, who retired in June 2018.

Colorado Names New CIO

Among the first round of cabinet appointments under new Colorado Gov. Jared Polis, **Theresa Szczeruk** was named state CIO. Szczeruk is the co-founder and CEO of tech communications company Radish Systems, and takes over from Suma Nallapati, who stepped down following Polis' election.

Shreveport, La., Hires First CTO

The newly elected mayor of Louisiana's third-largest city, Adrian Perkins, appointed **Keith Hanson** to serve as the city's first chief technology officer. Hanson is a Shreveport native and comes from the private sector.

cio central

Read full reports and breaking news about career changes across tech-driven roles in government at govtech.com/people.



Robert von Wolffradt

Longtime Iowa CIO Steps Down

Iowa CIO **Robert von Wolffradt** left his position as Iowa CIO after more than six years. He was previously CIO for Wyoming from 2007 to 2011. Von Wolffradt was replaced in an interim capacity by **Jeff Franklin**, a veteran of Iowa IT service.

Dallas Names First Chief Innovation Officer

Appointed by the Dallas city manager, **Laila Alequresh** is the city's first chief innovation officer and will head the newly created Office of Innovation. Alequresh already has a well-established career in gov tech, including innovation work in Los Angeles and Philadelphia.

Randy Cole Leaves Ohio Turnpike for Blockchain Startup

Longtime Executive Director of the Ohio Turnpike and Infrastructure Commission **Randy Cole** in January announced that he was joining Cleveland-based startup Ownum, which aims to use blockchain to make government more efficient. The move comes after more than 10 years in public-sector service, including positions with the Ohio Controlling Board and on the advisory board of DriveOhio.

Oklahoma Hires Digital Transformation Secretary

New Oklahoma Gov. Kevin Stitt appointed entrepreneur **David Ostrowe** to be the state's first secretary of digital transformation and administration, a new role aimed at creating efficiencies across the enterprise. While Ostrowe will not have direct oversight of state IT, he'll be working with CIO Bo Reese and John Budd, secretary of agency accountability, who heads the tech agency.



Charleston, S.C., Gets Its First CINO

Tracy McKee started work as Charleston, S.C.'s first chief innovation officer in November. She served as GIS director for Charleston from 1999 to early 2018, and most recently was chief data officer for Baltimore for 10 months.



New CIO in Charlotte, N.C.

Reenie Askew, formerly the deputy CIO of Houston, was named CIO in Charlotte, N.C. Her experience also includes more than 20 years as senior director of business technology at Sysco Corp. The position in Charlotte had been vacant since longtime CIO Jeff Stovall left city service in September.



Eric Larson

Larson Out at Florida AST

Amid the departure of Gov. Rick Scott and the arrival of newly elected Gov.

Ron DeSantis, Florida CIO

Eric Larson left his work with the Agency for State Technology. Larson had served in the position since March 2017. As of press time the state had not yet named a successor.

Atlanta Appoints New CISO

Veteran security and risk management professional

William Wade III was in February appointed CISO of the Atlanta Information Management Department. His previous experience includes more than five years as senior information security officer at VeriFone and manager of cybersecurity at travel tech firm Travelport.



Fulton County, Ga., Appoints New CIO

The most populous county in Georgia and home to the state capital of Atlanta, Fulton County, Ga., tapped

Nicole Keaton Hart as its next CIO. Hart was previously deputy CIO for the county, and her career includes 25 years in public- and private-sector IT. She takes over from Sallie Wright, who left the role in August.



New Leadership in Alaska

At the end of 2018, **Peter Zuyus** was named Alaska state CIO, an appointment that lasted just two months. In early February, the state's website listed attorney **Paula Vrana** as acting CIO. The transition follows a series of recent leadership changes in the Department of Administration, which oversees Alaska's Office of Information Technology.

Cincinnati Data Leader Leaves for NYC Parks

Cincinnati's Chief Performance Officer **Leigh Tami**, who for the last four years has helped stand up the city's data and analytics program, announced in February she had accepted a position as director of data analytics for New York City Parks and Recreation. **Nicollette Staton**, analytics and innovation manager in Cincinnati, has replaced Tami in an interim capacity.



Preparing for Crisis

Crafting a solid social media strategy is an essential part of emergency management.

Social media communications during a crisis situation can come from any number of agencies, not just police, fire or emergency management as you might expect. In some instances, these communications originate from the city or county manager's office, department of transportation, public works or water services — it all depends on the manner of crisis and the size of the agency's social media presence. It's crucial for all types of agencies and major departments to incorporate social media into crisis planning exercises.

When your agency gets together to plan response to high-risk emergency scenarios, make sure your social media coordinator has a seat at the table. At the same time, social media professionals should remember to reach out to their local emergency manager in exercises that involve planning social media messaging for crisis situations.

Crisis Strategy Planning Exercises

There are many ways to incorporate social media in your crisis planning exercises. One basic activity is to organize all of your social media contributors and other stakeholders in a room to plan messages and tactics for specific emergencies.

Start by brainstorming the top five to 10 high-risk crisis scenarios that have the potential to impact your agency. This could be a

flood, tornado, active shooter situation, mass casualty incident, school bus crash, polar vortex — you name it.

For each of these crises, begin to craft some of the generic social media messages that should be shared during these emergency situations. Type up what the potential crisis scenario might be, then draft several social messages that you'd most likely need to share if the situation were to unfold.

Your messages could include anything from preparedness information (what citizens can do before this crisis hits) to the first message you'll want to share immediately after you get the word. There will be a lot of details you don't know yet, but use blanks for the specifics. The goal is to have some content ready, no matter the situation. Timing is critical.

When I teach social media crisis planning, we don't stop here. It's just as important for the agency to talk about strategies for handling all the other things that happen during a crisis that may impact social media. Some questions to ponder during your planning exercises:

- There's a disruptive rumor spreading on social media while you're managing the crisis. How can your team address it?
- You have zero new information about the crisis, and it's going on 20 minutes since your last tweet. What is acceptable filler?
- At the start of the emergency, you forgot to unschedule a

lighthearted or humorous Facebook post. It's getting backlash for inappropriate timing. How do you handle it?

- People start tweeting that they're trapped and need help. What's your social media protocol?

Not in My Backyard

What if the emergency isn't actually in your jurisdiction, but you want to be ready to support other agencies with your messages on social media? Establish your strategy for supporting the lead agency if the crisis does not fall within your area, and "stay in your lane" while continuing to share their communications and contribute in a helpful way.

Remember, planning shouldn't be the sole responsibility of those involved in crafting the social media plan. I highly recommend developing a crisis communications strategy and protocols in tandem with local and regional emergency management and public safety officials. Don't forget to ensure that your procedures align with broader plans. 



Kristy is known as "GovGirl" in the government technology industry. A former city government Web manager with a passion for social media, technology and the lighter side of government life, Kristy is the CEO of Government Social Media.

Government Technology's Top 25
are innovators, collaborators,
and transformers driven to improve
state and local government.

A blurred background image showing the silhouettes of many people in what appears to be a large, modern office or lobby with large windows and architectural glass walls.

government
technology

Meet our
**2019 Top 25 Doers,
Dreamers and Drivers**
in the April issue.

TOP
25
DOERS,
DREAMERS
&DRIVERS

Fast is a network
that connects citizens and
government agencies.

Beyond Fast is the network that optimizes government performance.

There was a time when megabits per second was all that really mattered. Which is why Comcast built the nation's largest Gig-speed network to deliver unrelenting speed to more organizations in more places.

Now we're going **beyond**.

Beyond pure speed. To optimizing network performance by helping government agencies upgrade legacy systems and applications.

Beyond basic offerings. To deep, proven experience with government networks and Schedule 70-approved products.

Beyond one-size-fits-all. To customized networks that are cost efficient, secure and reliable.

We're taking our relentless speed and adding smart technologies and advanced applications that can deliver easy access to information across fragmented legacy systems—at speeds you never thought possible.

Take your government agency **beyond**.

ComcastBusiness.com/publicsector

COMCAST
BUSINESS
BEYOND FAST

Restrictions apply. Not available in all areas.
Maximum download 940 Mbps when hardwired via
Ethernet. Actual speeds vary and are not guaranteed.
©2019 Comcast. All rights reserved.