FEBRUARY 2017

techwire

New Protocol Helps California Local Law Enforcement Implement Cloud Services

By Maggie Cabrey

In collaboration with the private sector, the California Department of Justice (CalDOJ) is going forward with implementing a new protocol designed to support local law enforcement agencies in deploying cloud solutions for criminal justice data.

Under state government code, CADOJ is mandated to maintain a network backbone for use by law enforcement agencies. Supporting this responsibility, the department created the California Law Enforcement Telecommunications System (CLETS) and the CLETS Advisory Committee (CAC).

The need for a group like CAC trickles down from the FBI, which has a group called the Advisory Policy Board. It's the responsibility of the board to provide national standards for agencies across the U.S. to access Criminal Justice Information Services or national criminal justice data. In California, CAC is charged with ensuring data being sent across local, state and federal agencies meets those FBI requirements.

However, technology has come leaps and bounds since CLETS became operational in the 1960s, when it primarily applied to securing data running on dedicated lines via one-way, text-based machines. Following the request of one local police department, DOJ and CAC have been making moves to ensure it keeps up with modern advancements, particularly in the area of cloud technology.

FACEBOOK

CAC counsels the California Attorney General on the appropriate methods of collecting, storing and disseminating CLETS data. When a local law enforcement entity wishes to implement technology not already approved by the committee, it must first go through an application process explaining how the solution meets security requirements. A CLETS auditor is then assigned to the application, who decides whether the technology is legitimate.

Last year, when the Chula Vista, Calif., Police Department requested approval to deploy Microsoft Office 365 and Azure, the agency's technology manager, Eric Wood, found a missing piece in the CLETS approval processes. He also learned that there were several neighboring agencies that had submitted requests to deploy cloud services a year prior to his application, all of which never received a response from CAC.

"We discovered that the CLETS agency did not have a protocol to follow on how to authorize a law enforcement agency in the state to use Office 365, Azure or any cloud

CONTINUED ON PAGE 6

INSIDE:

NEWS BRIEFS

Department of Social Services to Award $10 Million Contract for Case Management System

The California Department of Social Services announced in February that the bid for its new Appeals Case Management System (ACMS) will be awarded to Visionary Integration Professionals (VIP LLC).

Under the more than $10 million contract, VIP will support the creation of a "single case management database to combine intake, scheduling and reporting functionalities into a single workflow."


SHUTTERSTOCK

The work will consolidate the existing four-decade-old mainframe database housed at the Office of Technology Services, and more than 20 ad-hoc applications. ACMS will be a public-facing system and replace the current State Hearings System built in the 1970s.

Seven vendors bid on the RFP, which was initially issued in December 2015. The contract term will be four years, the final two years of which will include maintenance and operation activities.

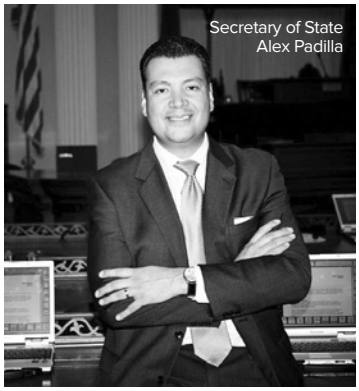
VIP is based in Reston, Va., with a West Coast office in Folsom, Calif.

Private Sector Weighs in on Cal-Access Replacement Project

The California Secretary of State's Office is gathering input from stakeholders about the replacement of the state's campaign and lobbying database, Cal-Access.

Last fall, Gov. Jerry Brown signed SB 1349, requiring a complete rebuild of Cal-Access into a database where campaign contributions and lobbying expenditures will be made public. Since the measure was approved, Secretary of State Alex Padilla has been working to ensure the system fits the needs of all those involved.

In February, Padilla held a public meeting in Sacramento, where members of the public were given an opportunity to share their thoughts about desired features of the new Cal-Access solution. Many of the attendees commented on the need to make the system more adaptable as technology continues to evolve. Skippy Williams, product manager for Berkeley-based MapLight, recommended the new system be released in an open source license. If the system were to be built using an open source solution, Williams said vendors would be allowed to freely review and modify the system.


Secretary of State Alex Padilla
JESSICA MULHOLLAND

TechWire Introducing News Section for Career Moves

Has your company or government department hired new staff members? If so, we want to hear about them.

Our Insider community is thriving, and there are more people than ever going to work for local tech companies and public-sector agencies. We want to give our readers the latest scoop on who's going where.

If you would like to see a new hire, promotion or retirement mentioned on *TechWire,* email Editor Matt Williams at matt@techwire.net.

Please include the person's name, their position, a brief bio and, if you want, a photo of him or her. We'll include them in our newsletter.

New IT Compliance Policies for California State Government

The Department of General Services and Department of Technology summarize revisions to IT compliance policies in a recent joint memo.

Among the significant changes: The new policy requires oversight and certification of compliance with IT policies by CIOs for IT acquisitions of more than $5,000. (The previous threshold was $100,000.)

Under the new policy, departments also can self-certify that their IT procurement is within their Department of General Services-delegated procurement authority limit or within their California Department of Technology-delegated Project Approval Authority.

NEWS BRIEFS

The TechWire Industry Briefing hosted a panel of leaders from the California Department of Technology, including (from left to right) Deputy State CIO Chris Cruz; Peter Liebert, California's chief information security officer and director of the Office of Information Security; Ben Word, the chief state enterprise architect; and CalCloud project director Scott MacDonald.

TECHWIRE.NET

State Making Moves to Bolster Cyberdefense

The California Department of Technology (CDT) is making moves to develop a Security Operations Center (SOC) in partnership with the Office of Emergency Services' California Cybersecurity Integration Center (Cal-CSIC), Military Department and California Highway Patrol.

At the TechWire Insider Industry Briefing, state Chief Information Security Officer Peter Liebert spoke about the work being done to create the SOC and the agencies involved in the initiative, referred to by officials as the "four amigos."

Each agency has its own wheelhouse in terms of cyber, according to Liebert. Under government code, CHP has the authority to go out and conduct investigations in events where a state agency is victimized. While patrol is charged with the enforcement, CDT runs network analysis, Cal-CSIC facilitates interagency communication and the Military Department primarily manages assessment services necessary to support critical network infrastructure. Liebert explained how each of these agency functions will integrate with the SOC.

"The vast majority of the traffic that's traveling on our state networks comes through [the CDT] building," Liebert said. "It only makes sense that we centralize protection and analysis as much as possible to utilize that central gateway aspect and provide value from a 24/7 SOC that will be looking at malicious traffic, analyzing that traffic and then responding accordingly."

CDT will focus on the data that comes across the state network and work with Cal-CSIC, which will act at the primary coordinating body. If a threat is found as CDT oversees detection and analysis, the Cal-CSIC will be brought in to organize response. In order to ensure that the "hand-in-hand" relationship between the agencies continues, Liebert said there will be a representative from CDT in the Cal-CSIC SOC on a 24/7 basis.

The "four amigos" have been meeting multiple times a week to determine the procedures they will use to tackle potential network hazards and issues. Liebert said the goal is to develop a comprehensive communications plan that will show how managing an event escalates, starting from either third-party notifications or a customer agency, all the way up to the Governor's Office if necessary.

Deputy State CIO Discusses Strategic Objectives for 2017

Deputy state CIO Chris Cruz outlined the California Department of Technology's core strategic objectives for 2017 and beyond during a TechWire Industry Briefing in Sacramento.

The objectives include continued focus on statewide information security and procurement modernization, Cruz said, along with efforts to update the department's website, develop proof-of-concepts in partnership with vendors within the department's innovation lab, and better integrate enterprise architecture into the state's IT project delivery process.

Cruz mentioned some initiatives that could be of interest to IT suppliers:

- The Department of Technology is going to be developing a Security Operations Center (SOC) in partnership with the Office of Emergency Services, Military Department and CHP. As part of standing up that SOC, the department will be integrating the state data center into the California Cybersecurity Integration Center (Cal-CSIC) program, Cruz said.
- During 2017, in partnership with the Department of General Services, the Department of Technology will continue to work on streamlining the contracting process for both vendors and customers, and plans to modify its service-level catalog. "By brokering services through the Department, we feel this is the right way to go, and enhances our information security if we standardize our hardware and software," Cruz said.
- CDT also is working to integrate Enterprise Architecture into the early stages of project planning and procurement. Cruz said this focus should lead to bids that have more accurate requirements and scope. "We're hoping that simplicity, not only from a state, but also from the vendor side, will lead to better outcomes."

IN THE SPOTLIGHT: CANNABIS

SHUTTERSTOCK

California State CIO Discusses Cannabis Licensing Software at Oversight Hearing

The state of California will use a product from Accela for a licensing system that that will be deployed for the medical and recreational cannabis industry.

State CIO Amy Tong told a legislative panel that the software was chosen via a competitive price quote and selected in part because of its ease of use and flexibility as California approaches a mandated Jan. 1, 2018 go-live deadline.

"We decided to choose that product based on its track record being used in both the industry for licensing as well as other state entities that have chosen this particular product to implement a licensing capability," Tong said.

The Department of Technology was in negotiations, as of February, with a systems integrator that will come aboard to install the software, Tong said. The contract with is Accela is about $3.5 million.

The new IT systems for the cannabis industry — licensing and "track and trace" — are required by statute under the Medical Cannabis Regulation and Safety Act (MCRSA) of 2015. Officials also plan to build additional functionality within the licensing system to implement Prop 64, legalizing recreational use of marijuana by adults. California voters approved that measure in November. The MCRSA legislation set an aggressive Jan. 1, 2018, date to launch the licensing system.

State Sen. Jerry Hill said the deadline is swiftly approaching and he noted there are a number of differences in the two laws.

"Frankly, I have to say there's a fair amount of skepticism, actually, from some up here," Hill said, referencing his colleagues, "about us meeting that deadline."

Tong and Lori Ajax, chief of the Bureau of Medical Cannabis Regulation, explained that the software that will launch in January 2018 likely will not include all functionality, such as renewals. Tong said the goal is to have the capability by Jan. 1 to accept applications for licenses through a Web portal. But processing them could take longer.

Law Enforcement Turns to Tech to Help Regulate Cannabis Industry

California's path to govern medical and recreational cannabis is shaping up to be a sophisticated one — from testing drugged drivers to tracking a packaged marijuana product back to the farm that cultivated the plant.

Officials across state government in February discussed how they plan to use technology to regulate the industry, protect public health and deter impaired drivers from getting behind the wheel.

As part of new license regulations, an IT system — known as "track and trace" — will be implemented so that regulators can follow a marijuana plant from a seed to the dispensary. Law enforcement told lawmakers,that they hope the system will be provided to them in a useful format.

For example, CHP officers responding to a collision would want to verify a truck's marijuana load was coming from a licensed facility, Richard Desmond, legislation coordinator at the California Highway Patrol, told lawmakers.

With the legalization of recreational cannabis has come the growing concern, several lawmakers said, of more drugged drivers on the roads and the limitation of law enforcement to identify and arrest impaired drivers. That's in large part because measuring a marijuana user's impairment is far more difficult than a simple breathalyzer or blood test currently administered to drivers suspected to be under the influence of alcohol.

"There's a lot of new technology out there, and we don't necessarily know what this technology is capable of and how feasible or logistical it is to use on the side of the road," Desmond said.

The CHP hopes to use the $3 million set aside in Proposition 64 to vet some of those technologies, Desmond said.

BUSINESS NEWS

Folsom-Based PowerSchool Acquires Public-Sector Software Company for $850 Million

Folsom-based PowerSchool announced it has acquired SunGard K-12 business from FIS, a financial services technology provider.

The acquisition was made by Vista Equity Partners for $850 million. Vista has been expanding PowerSchool's software suite since it originally purchased the company in 2015 for $350 million. In its deal with FIS, Vista will now be able to combine SunGard K-12's enterprise resource system with PowerSchool's Unified Classroom platform.

PowerSchool headquarters in Folsom

POWERSCHOOL GROUP

How Will Changes to California's 'Tech Transfer' Statute Impact Businesses?

The evolving relationship between state taxation and the digital economy was the topic of a recent California State Assembly Committee on Revenue and Taxation hearing.

Discussion at the meeting centered around a Technology Transfer Agreement (TTA) statute, a type of arrangement involving a sale of tangible and intangible personal property. A case settled last year between the state and Lucent Technologies Inc. has spurred recent conversation among lawmakers regarding the Court of Appeals' interpretation of the agreement's statutes and its far-reaching revenue implications for California.

In order to qualify as a TTA, the seller must hold a patent or copyright interest and license the right to make or sell a product to the buyer, subject to the patent or copyright held by the seller. Under a TTA, Sales and Use Tax is applicable to tangible property and not to intangible property.

In the case with Lucent, the Court of Appeals claimed the Board of Equalization (BOE) had improperly assessed sales tax on the manufacturer when it asserted that copies of Lucent's telecommunications software made on magnetic tapes and CDs transferred to nine different telephone companies qualified as tangible property. As a result, the court ordered the BOE to pay Lucent a sales tax refund of more than $24.5 million.

Although the dispute involving the BOE and Lucent was settled, questions still remain regarding the definition of "tangible" versus "intangible" in transactions where software is involved.

"The court's view is because these were magnetic tapes, after the telephone companies purchased the tapes from the manufacturer, they can throw the tapes away because now it's loaded onto the digital switches," said Robert Lambert, assistant chief counsel of the BOE's Litigation Division at the meeting. "Therefore it's merely a convenient medium of transfer that is not needed to implement the intellectual property rights after the date of sale."

Sacramento Startup Streamlines Access to Public Records

A local startup is looking to help open up public records and make government more transparent.

The company, called Vigilant, provides users with a research and intelligence tool that's designed to help streamline access to public records. Those who sign up for the service can utilize Vigilant's search engine, which includes state, county and city data, such as property records, business filings, licenses and contracts.

TWITTER/LAURA GOOD

Co-founder **Mike Phillips** talked about the Vigilant solution during a presentation in February. Phillips explained how Vigilant works and how his experience in public affairs inspired him, along with co-founder Zac Palin, to create the service.

"I used to run a public affairs consulting firm and do a lot of competitive intelligence and research for folks," Phillips said. "I hired a lot of researchers and they'd spend the vast majority of their time going out to load databases, searching those databases, pulling together records from those databases. Basically spending their time doing what robots could do."

In addition to manual searches, customers can sign up for alerts to receive information on a schedule. Vigilant also offers a lobby intelligence program that enables users to review up-to-the-minute lobbying data from all states, federal government, and major cities and counties.

TechWire welcomes your feedback. Contact Editor Matt Williams at (916) 932-1310 or matt@techwire.net.

CONTINUED FROM FRONT PAGE

service for that matter," Woods said in an interview with *TechWire*. "They had not gone through and approved it for any agency because they didn't know how without a protocol."

Recognizing the potential impacts his discovery could have on the private sector, Wood engaged with Microsoft to explain how the missing protocol was likely a significant reason why law enforcement agencies in California weren't deploying the company's cloud services. Prompted by Wood's application, the company began assessing how to remedy the issue.

Microsoft had begun working with CalDOJ more than five years prior to Wood's discovery, looking to ensure that CLETS and agencies at both a state and national level understood where the evolution of technology is and where it's going, an effort Stuart McKee, Microsoft's chief technology officer of state and local government, was heavily involved in.

"Although CLETS historically was developed for teletypes, we have a fiduciary responsibility to embrace it and work through it in such a way that you mitigate the risk for all the parties involved," McKee said.

At the time Wood submitted his application for cloud services, Microsoft already had a contractual commitment to CalDOJ in place since 2013, stating the company would provide a level of access to auditing of environments used by agencies, as well as fingerprint-based background checks of employees involved in the development and deployment of those solutions. However, without a CLETS procedure in place to approve Microsoft cloud technology, Wood referred to the agreement as more of an "empty nod of approval."

Beginning in March 2016, CalDOJ CLETS auditors and engineers held conference calls on a near weekly basis with Microsoft for more than six

Stuart McKee, Microsoft's chief technology officer of state and local government

LINKEDIN

months, during which the group worked through a list of roles, requirements and responsibilities that would go into law enforcement deploying Microsoft cloud solutions. McKee said the conversations primarily revolved around education.

"Most of the work that went on, from Microsoft's standpoint, was about trying to get educated and understand CLETS, its history, policies and processes, [as well as] understand Eric [Wood], Chula Vista, their requirements and how they operate as an organization," McKee said. "Then trying to reconcile that, very often, with what other organizations across California are doing to create some consistency, if you will."

Conference calls between CalDOJ and Microsoft closed in October. The end product of the collaboration is a security matrix that gives CLETS auditors a framework to review how security issues involving Microsoft Office 365 and Azure would be managed.

"Once the security matrix was established, they agreed that it encompassed essentially A to Z of everything we need to be covered," Wood said. "Then [CAC] can provide that to an agency who wants to apply and say, 'In your application complete this security matrix.' That was the missing piece."

Agencies that had previously requested to implement Microsoft cloud products were asked to re-submit their applications. Following evaluation from CLETS auditors, the Chula Vista Police Department's updated proposal was approved by CAC on Dec. 14. Wood said they contracted with Winbourne Consulting to help develop the submission.

In this day and age, many public sector agencies are strapped for resources and funding, a concept that the Chula Vista PD hasn't been immune to. However, with the protocol to approve cloud resources now in place with CLETS, Wood's department and other law enforcements organizations in California have the ability shift their attention away from specific activities, such as racking on-premise servers.

"Me and my staff are now freed up to really focus on the particular needs of our agency, not just the foundational plumbing of having documents flowing and where are they stored on a file server," Wood elucidated on how the changes have helped his department. "You can now enable your people to really keep up with a smaller, more manageable set of compliance"

As for the private sector, McKee gave insight on how he thinks the CLETS process and the approval for Chula Vista PD is going to impact the market.

"Getting this milestone completed is going to release a lot of pent up demand. Most of these agencies have already embraced the technology, but they now have an additional level of confidence that what they're doing is right. At a national level, it really acknowledges California's leadership and how it is continuing to evolve and embrace emerging technologies responsibly."

SHUTTERSTOCK

6 State Agencies Planning Cybersecurity Improvements

Several California agencies are looking to make improvements to their information security operations in the upcoming budget year.

Following the recent release of Gov. Jerry Brown's budget address, state departments are in the process of submitting 2017-18 funding requests. While submissions cover a range of topics, some requests suggest there may be a movement among state agencies to invest more in cybersecurity. Here's a quick look at six funding proposals that reflect this potential trend:

1 The California Department of Transportation requested more that $4 million for consultant contracts, one-time and ongoing software and hardware purchases, six permanent positions, and ongoing training expenses. Funding will also support Caltrans in developing its Enterprise IT Security Program Roadmap.

2 The California Department of Corrections and Rehabilitation (CDCR) proposed to spend $1.5 million on hardware, software and vendor services. These components will support CDCR in opening its own security operations center.

3 With the goal of developing and running an effective information security and risk management program, the Department of Rehabilitation (DOR) asked for $281,000 from the General Fund for a systems software specialist and staff information systems analyst specialist. The two full-time employees will work under the DOR's Information Security Office, helping safeguard the data of more than 100,000 individuals.

4 The Department of Alcoholic Beverage Control (ABC), looking to establish its own Information Security Office (ISO), has asked for $278,000 in 2017-18 and $274,000 in 2018-19. The funding will be used to make the data processing manager and systems analyst positions permanent within the ISO.

5 A $303,000 budget change was proposed by the State Treasurer's Office to provide support to the cyber-risk management program managed by its Information Technology Division. According to the submission, the recommended expenditure would permit "acquisition of vulnerability assessment, continuous network monitoring and log management security products," as well as a full-time systems software specialist.

6 The Public Utilities Commission proposed spending $665,000 to establish a cybersecurity regulatory group. Made up of four highly technical analysts, the group will be charged with myriad tasks, including examining new policy debates, and evaluating proposed frameworks and best practices. Money would come from the PUC Utilities Reimbursement Account funded by user fees.

Workers' Compensation Claims in CA Could Get Electronic Boost

California is taking first steps toward implementing electronic systems for workers' compensation injury reports and what's called the "utilization review" process.

The systems are mandated by legislation passed in 2016. The bill's author, state Sen. Tony Mendoza, called SB 1160 "an important reform measure that will improve data collection and medical treatment delivery for California's injured workers."

Specifically, the Department of Industrial Relations (DIR) has been tasked with creating an electronic system that can accept Doctors' First Report of Injury documents. California's labor code "requires a physician who treats an injured employee to file a 'Doctor's First Report of Injury' (DFR) with the claims administrator for every work illness or injury, even first-aid cases where there is no lost time from work."

DIR's Division of Workers' Compensation also proposes to to develop a system for electronic reporting of documents related for the utilization review process, which, according to a legislative summary, is the "review process for medical treatment recommendations by physicians to see if the request for medical treatment is medically necessary. The full UR process varies by vendor, but it generally involves initial review by a non-physician, with higher level review(s) being conducted by a physician or physicians."

Both projects — the utilization review database and the electronic form for the Doctor's First Report of Injury — are subject to the Department of Technology's planning process before final approval.

When a Data Breach Happens, Will California Pay for Identity Protection?


Assemblyman Matt Dababneh, D-Encino

MATT DABABNEH

The chairman of the Assembly's Banking and Finance Committee is proposing that in the event of a breach of government data, California state and local agencies would be required to provide identity theft protection or mitigation services at no cost to constituents whose personal data may have been compromised.

The idea is the central purpose of the reintroduced legislation (AB 241) put forward by Assemblyman Matt Dababneh, D-Encino. State law already extends the same requirements to businesses or individuals. Under Dababneh's bill, the free identity theft protection would be offered for a period of at least 12 months.

Analysis

The legislation would potentially impact hundreds of thousands of records and millions of Californians in future years. Between 2012 and 2015, the state Attorney General said it received reports of 657 data breaches that involved the personal information of more than 500 California residents, according to the California Department of Justice's 2016 data breach report. Government accounted for 5 percent of those breaches and 2 percent of total records breaches between 2012-15, the report said.

For big breaches, offering identity theft protection is costly. In 2015, the federal government spent a reported $133 million to provide ID theft protection services to an estimated 21.5 million people whose personal information was stolen in the much-publicized hacking of the Office of Personnel Management. In a separate incident, Utah spent millions of dollars for two years' worth of ID protection when Security Security numbers were stolen from the state's health department.

Dababneh introduced legislation nearly identical to AB 241 in 2015. That bill (AB 259) stalled in Appropriations. A committee analysis found Dababneh's legislation in 2015 would incur "potential major costs in the tens to hundreds of millions of dollars, depending on the scope of a data breach to any of various state agencies." Further findings from that analysis:

Even one event affecting 100,000 individuals could result in potential costs of $12 million to $36 million (General Fund) to provide credit monitoring services for one year.

Based on information surveyed from credit monitoring services, bulk enrollment costs for credit monitoring services in which the vendor is provided with a complete list of individuals at once from the breached entity generally range from $10 to $30 per month per person ($120 to $360 per year per person), depending on the type of monitoring package offered by the vendor.

The five biggest breaches (by number of records) reported to the California Attorney General 2012-15:

ANTHEM, INC.	10.4M
TARGET	7.5M
LIVING SOCIAL	7.5M
UCLA HEALTH	4.5M
PNI DIGITAL MEDIA (COSTCO/RIATEAID/CVS)	2.8M
T-MOBILE USA, INC. (EXPERIAN)	2.1M

Source: California Attorney General

The U.S. market for identity theft protection services is $3 billion to $4 billion, according to one research firm. "Identity theft protection firms use software to track unauthorized use of credit and other personal information," IBIS World reported in 2013. "[By] 2018, this industry is forecast to increase at an annualized rate of 2.1 percent to $3.8 billion."

SHUTTERSTOCK

California's Enterprise Migration to Cloud Email Continues Forward

California is inching closer to achieving a single system for email and productivity tools across the state government.

By the end of 2017, officials say the vast majority of email accounts kept by California's state government — perhaps 90 percent or more — will be hosted off-premises in Microsoft's government cloud.

That will be the end result after the California retires its on-premise CA.Mail system and its off-premise California Email Service (CES). CA.Mail is going offline Dec. 31. 2017, and the CES contract expires in October. So state customers are migrating en masse to Office 365 in the cloud.

"The state and Department of Technology is committed to working with government to define some enterprise standards for technology, and this [email system] is one of the first ones out of the gate: We have a common framework now for how we manage, maintain and secure email," Department of Technology chief deputy director Chris Cruz said.

The migration is well underway. The Department of Technology provided some statistics to TechWire on the progress so far, current as of February:

- 27 departments (24 CES, 3 CA.Mail) have completed their migration so far, totaling 84,000 mailboxes.
- 72 departments in all will migrate to Office 365 by December 2017. Of these, there are 170,000 mailboxes (CES: 99,000 and CA.Mail 71,000)
- 10 additional departments that host their own email are interested in migrating. This would add another 15,000 mailboxes.

These numbers indicate approximately 185,000 mailboxes could be in Office 365 by the conclusion of 2017.

For state customers using the CES system, transition services are being provided for free by Microsoft, via Planet Technologies or other resellers. CA.Mail customers are hiring outside consultants to help with their migration. ENS-Inc., based in the Sacramento area, also is providing services.

There could be several advantages to widespread adoption of Office 365. One is that licensing and renewals for the email and productivity suite will be centrally managed at the Department of Technology; previously, departments agreed to licenses individually and one-by-one. Another benefit should be the features that Office 365 brings the state workforce, such as 50-gigabyte mailboxes, online versions of Office and SharePoint, Skype for Business, 1 terabyte of storage per user, and more.

The common platform also should help standardize California's cybersecurity. Office 365 is compliant with several major security standards — FedRAMP, FIPS, HIPAA, IRS 1075 and will enable two-factor authentication, single sign-on and mobile device management capabilities.

"This is obviously very significant because it gets the state to a single statewide email system and platform, which allows us to secure our data in a much more up-to-date-fashion that meets all the highest levels of security compliance," Cruz said.

So far, California has spent about $35 million to date on Office 365 licenses and renewals for this project, covering 85 percent of the departments that will be migrating.

MARKET ANALYSIS

Security Operations Centers Are a Government Trend in 2017

The California Department of Corrections and Rehabilitation (CDCR) plans to open its own information security operations center to protect internal IT systems and thwart illicit communication and other damaging behaviors among inmates.

Pending approval by the Legislature of a $2.6 million budget request, CDCR information security officer Vitaliy Panych said he intends to move as quickly as possible to recruit and hire eight staff and get the new SOC up and running sometime in fall 2017.

"One of the main challenges will be finding the people. The information security job market is pretty scarce," Panych told TechWire. "We'll have positions at both the entry level and the senior level. It's really a matter of getting qualified people; I'm going to be recruiting the heck out of people."

Panych said the SOC will have dedicated office space within the CDCR, likely at CDCR's Aerojet campus in Rancho Cordova or at an existing communications center the department operates in downtown Sacramento.

One of the main duties of the new cyberteam will be to proactively hook into CDCR's systems and hunt for unusual behavior, malicious abuse and insider threats.

"Corrections is a big place, there's a lot of employees. We deal with inmates and technology is being extended to them," Panych said. "With the passage of Prop 57, there are a lot of education and rehabilitation efforts being driven to inmates. ... For us, what that means for security is that anytime we provision any kind of access to systems or technology, there's a likelihood it will get abused and be used in a malicious manner."

CDCR

The corrections department's security operations center will be linked to a broader SOC the California Department of Technology plans to build itself, as well as the California Cybersecurity Integration Center (Cal-SIC), in order to share data and threat intelligence.

"In short, we are building our own, but it will be 'wired' to the Department of Technology/CalSIC. Kind of a first-layer and second-layer approach. We will be at a more granular level, but feeding the state SOC with our info," CDCR chief information officer Russ Nichols explained via email.

Market Analysis

The build-out of Security Operations Centers within California state government looks like a trend in the making. The California Department of Motor Vehicles opened its own SOC in late 2015, and TechWire toured the facility. Now the California Department of Technology said it will build its own too. That's on top of the California Cybersecurity Integration Center (Cal-CSIC) that makes its debut in 2016.

There's a market opportunity in each of these new facilities. CDCR proposed to spend $1.5 million on hardware, software and vendor services for its SOC, according to budget documents.

FEDERAL NEWS

What Does a New FCC Chairman Mean for California?

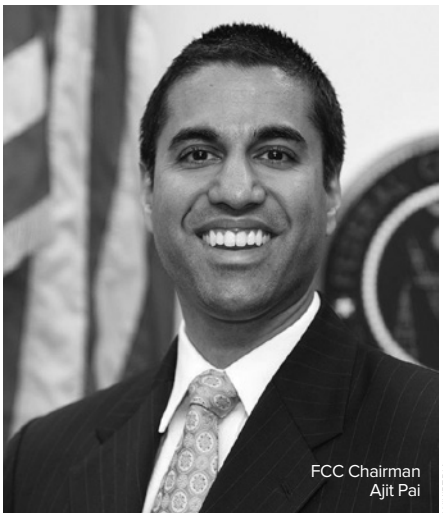
Many are wondering if the influence of Ajit Pai, whom President Trump promoted to chairman of the FCC, might substantially change the landscape for telecommunications companies, broadband service providers and emerging technologies.

Some critics note that Pai opposes net neutrality rules, and he took heat for a recent decision revoking an order that added nine telecom providers to the Lifeline program, which subsidizes phone and Internet service for low-income citizens. He has been called a "proponent of limited government and a free-market approach to regulations." One observer called him someone who "never met a mega-merger he didn't like."

Meanwhile, many industry leaders have lauded Trump's elevation of the 44-year-old Pai, a Republican and Kansas-raised lawyer whom President Obama named to the commission in 2012. USTelecom CEO Jonathan Spalter, for example, said "we share Commissioner Pai's vision for a 'Broadband First' future based on a bold but pragmatic strategy to erase the many regulatory barriers impeding the expansion of our nation's communications infrastructure." Comcast's chief diversity officer said, "This is a terrific appointment for the American consumer and the companies the FCC regulates."

What could Pai's leadership mean for California? It's hard to say for certain, but a quick review of some of Pai's correspondence with California state government and his comments in front of the private sector in California do shed a small measure of light on the matter:

- In July 2016, Pai sent a letter to the California Public Utilities Commission asking for its help and advice in combating fraud waste and abuse within the Lifeline program. Pai noted that California is one of four states that maintain their own Lifeline accountability databases.
- In 2012, Pai complimented Gov. Jerry Brown for signing into law the California Internet-Protocol deregulation bill, calling the legislation "bipartisan work at its best" that avoids "intrusive government regulations." Pai said California's bill would "prevent the application of legacy economic regulations to IP services while preserving consumer protections like E911."
- During a FCC field hearing in 2013 at Moffett Federal Airfield in Santa Clara, Pai said he wanted to learn how California is preparing its communications systems with the knowledge that the next big earthquake will inevitably hit. "So it's important, as we think about how to keep our communications networks running during emergencies, to consider our country's complexities before seizing any one-size-fits-all solutions," Pai said in those remarks.
- At a San Diego Conference of CTIA - The Wireless Association, Pai credited the federal government's "deregulatory approach from the beginning" for the growth of the wireless industry, and he called regulation "pervasive, and it's not pretty." He continued, "In my view, our deregulatory approach to wireless has been a success. The market is highly competitive. Almost all consumers can choose from at least four facilities-based wireless providers. There are also many wireless resellers that cater to consumers who traditionally have been underserved. Prices have consistently fallen."
- In 2016, Pai proposed a Digital Empowerment Agenda in which he proposed the creation of Gigabit Opportunity Zones, build-out of broadband in rural America, removing regulatory barriers to broadband deployment, and promoting entrepreneurship and innovation.
- In February, Pai penned a blog post in which he defended his commitment to closing the digital divide, and he cited a visit to a Los Angeles community as part of his work on the issue. He said the FCC is scheduled later this month to work on proposals to put billions of dollars toward bringing 4G coverage to all parts of the country. Pai said on the controversial decision about the Lifeline program has been "sensationalized."



FCC Chairman Ajit Pai

WIKIPEDIA