

~~RECEIVED~~
~~JAN 25 2017~~

INTERIM REPORT

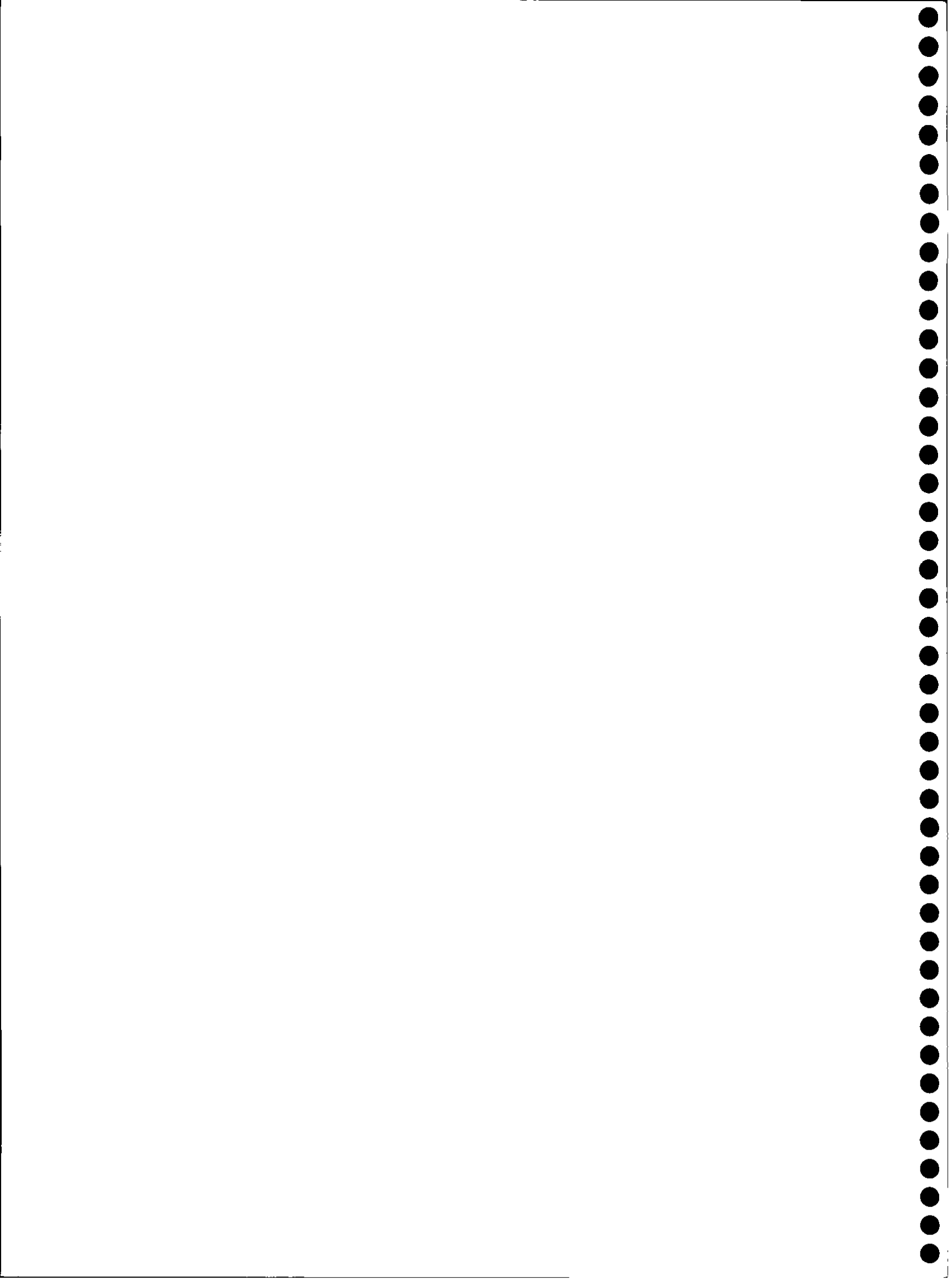
to the 85th Texas Legislature



HOUSE COMMITTEE ON
GOVERNMENT TRANSPARENCY & OPERATION



JANUARY 2017



**HOUSE COMMITTEE ON GOVERNMENT TRANSPARENCY & OPERATION
TEXAS HOUSE OF REPRESENTATIVES
INTERIM REPORT 2016**

**A REPORT TO THE
HOUSE OF REPRESENTATIVES
85TH TEXAS LEGISLATURE**

**GARY ELKINS
CHAIRMAN**

**COMMITTEE CLERK
TERI AVERY**





Committee On
Government Transparency & Operation

January 4, 2017

Gary Elkins
Chairman

P.O. Box 2910
Austin, Texas 78768-2910

The Honorable Joe Straus
Speaker, Texas House of Representatives
Members of the Texas House of Representatives
Texas State Capitol, Rm. 2W.13
Austin, Texas 78701

Dear Mr. Speaker and Fellow Members:

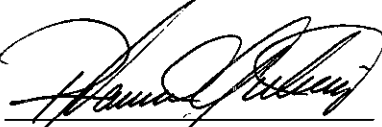
The Committee on Government Transparency & Operation of the Eighty-fourth Legislature hereby submits its interim report including recommendations and drafted legislation for consideration by the Eighty-fifth Legislature.


Respectfully submitted,

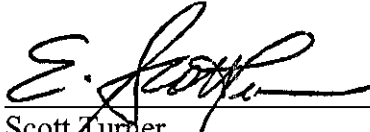

Gary Elkins



Rick Galindo


Larry Gonzales


Roland Gutierrez


Jeff Leach


Scott Turner


Armando Walle

Armando Walle
Vice-Chairman

Members: Rick Galindo, Larry Gonzales, Roland Gutierrez, Jeff Leach, Scott Turner



1

TABLE OF CONTENTS

INTRODUCTION	4
INTERIM STUDY CHARGES.	5
INTERIM CHARGE #1	6
BACKGROUND	7
HEARING.	9
RECOMMENDATIONS.	18
INTERIM CHARGE #2	20
BACKGROUND	21
HEARING.	23
CONCLUSION.	28
INTERIM CHARGE #3	29
BACKGROUND	30
HEARING.	32
RECOMMENDATIONS.	40
INTERIM CHARGE #4	40
BACKGROUND	41
HEARING.	46
RECOMMENDATIONS.	52
INTERIM CHARGE #5	53
BACKGROUND	54
HEARING.	57
RECOMMENDATIONS.	61
INTERIM CHARGE #6	62
BACKGROUND	63
HEARING.	64
RECOMMENDATIONS.	74



INTRODUCTION

At the beginning of the 84th Legislature, the Honorable Joe Straus, Speaker of the Texas House of Representatives, appointed seven members to the House Committee on Government Transparency & Operation. The Committee membership included the following: Gary Elkins, Chairman; Armando Walle, Vice-Chair; Rick Galindo, Larry Gonzales, Roland Gutierrez, Jeff Leach and Scott Turner.

The committee was given jurisdiction over all matters pertaining to:

- (1) the organization, operation, powers, regulations, and management of state departments, agencies, institutions, and advisory committees;
- (2) elimination of inefficiencies in the provision of state services;
- (3) open government matters, including open records and open meetings; [and]
- (4) advances in science and technology, including telecommunications, electronic technology, or automated data processing, by state agencies, including institutions of higher education;
- (5) the promotion within the state of an advance described by Subdivision (4);
- (6) cooperation between the state or a local governmental entity and the scientific and technological community, including private businesses, institutions of higher education, and federal governmental laboratories; and
- (7) the Texas Emerging Technology Advisory Committee and the Sunset Advisory Commission.



INTERIM STUDY CHARGES

1. Identify and address potential gaps in the state's cybersecurity policies and ensure that personal information held by state agencies is secure. Address whether industry-accepted cybersecurity standards have been met by state agencies and state data centers and determine ways to promote a culture of cybersecurity awareness among users of state information resources.
2. Examine purchasing practices by state agencies to ensure such practices are efficient and transparent.
3. Study issues related to access to public information held outside of the custody or control of the governmental body by current or former officers or employees. Assess whether the Public Information Act's procedures for response to repetitious or redundant public information requests adequately protect small governmental bodies from the financial burdens imposed by such requests.
4. Study the use of commercial cloud computing by state agencies and institutions of higher education, including efficiencies surrounding a utility-based model, security impacts of transitioning to cloud computing, and cost-savings achieved by the utilization of commercial cloud computing services.
5. Review the process of dissemination by public entities of criminal records containing incomplete or inaccurate information, assess options for the subjects of such records to correct the misinformation specifically as it interferes with their ability to obtain employment, and determine the need for greater regulations over this process. (Joint charge with the House Committee on Homeland Security & Public Safety)
6. Study the impact of emerging technologies used by law enforcement and issues related to appropriate dissemination of the data provided by those technologies, including the impact of technologies on the operation of law enforcement agencies, the operation of the Public Information Act, and any appropriate safeguards for citizens and law enforcement officers who interact with those technologies or whose data is recorded. (Joint charge with the House Select Committee on Emerging Issues in Texas Law Enforcement)



INTERIM CHARGE #1

Identify and address potential gaps in the state's cybersecurity policies and ensure that personal information held by state agencies is secure. Address whether industry-accepted cybersecurity standards have been met by state agencies and state data centers and determine ways to promote a culture of cybersecurity awareness among users of state information resources.



BACKGROUND

TCEEDC

The Texas Cybersecurity, Education and Economic Development Council (TCEEDC) was statutorily created in 2011 to study and provide recommendations to improve the infrastructure of the state's cyber security operations with existing resources and through partnerships between government, business, and institutions of higher education, and to examine specific actions to accelerate the growth of cyber security as an industry in the state.

The TCEEDC report, *Building a More Secure and Prosperous Texas*, was presented to the Legislature in December 2012. The Report focused on three main areas: Texas' Cybersecurity Infrastructure, the Cybersecurity Industry Within Texas, and the State's Cybersecurity Educational Needs. Among the findings of the TCEEDC were:

- No state-wide coordination of cybersecurity strategy beyond state agencies
- Lack of coordinated cybersecurity effort allows cyber-crime to outpace the development of a cybersecurity infrastructure to effectively counter those activities
- Several examples of innovation and cyber excellence throughout Texas, but mostly localized rather than programs to expand to regional or statewide models
- Lack of qualified cybersecurity workforce is significantly impactful to both economic growth and the protection of the state's cyber infrastructure

Additional Findings and Recommendations Specific to Texas State Agencies included:

- All state agencies are required to maintain security best practices according to Texas Administrative Code (TAC) 202.
- More collaborative efforts within the State strengthen the overall security posture of state agencies
- State agency compliance with TAC 202 requirements form a good foundation for ensuring basic protection of State of Texas information assets.
- Need to increase the number of cybersecurity practitioners throughout the State, not only to provide the expertise needed to grow cyber security investment in Texas, but also to protect the state's cyber assets.

The report contained several recommendations to strengthen Texas' Cyber security that were implemented by the 83rd Legislature.

SB 1597 – Required proactive protection of the state against cybercrime/similar security threats.

SB 1101 – Extended the TCEEDC for an additional 2 years through August 31, 2015.

SB 1102 – Required the Department of Information Resources (DIR) to designate a state Cybersecurity Coordinator and permitted DIR to implement other recommendations from the Council report, including building public/private partnerships between state agencies and industry and coordinating efforts to leverage best practices among organizations throughout the state.

SB 1134 – Required DIR to establish a state framework for cybersecurity.

DIR

The Texas Department of Information Resources (DIR) manages the enterprise security program and coordinates statewide cybersecurity efforts through security services, policy and assurance, risk management, and education and training. DIR has addressed several of the recommendations of the TCEEDC. The following initiatives, explained below, have been implemented to improve the state’s overall cybersecurity posture:

- Offering third party security assessments,
- Developing a unified cybersecurity framework, which is aligned to federal and private sector best practices and standards,
- Offering cybersecurity products and services through the cooperative contracts program,
- Implementing a governance, risk and compliance software platform, and
- Providing numerous training and education opportunities.

HEARING

On April 5, 2016, the House Committee on Government Transparency & Operation met in a public hearing in Austin, Texas, to consider the following charge:

Identify and address potential gaps in the state's cybersecurity policies and ensure that personal information held by state agencies is secure. Address whether industry-accepted cybersecurity standards have been met by state agencies and state data centers and determine ways to promote a culture of cybersecurity awareness among users of state information resources.

The committee heard testimony from the following:

Edward Block, Texas Department of Information Resources (DIR);
Lena Conklin, Legislative Budget Board;
Mary Dickerson, TCEEDC;
John Dickson, The Denim Group;
Brandon Neff, Innové;
Dr. Gregory White, UT-San Antonio (UTSA) and TCEEDC; and
Michael Wyatt, Deloitte & Touche, LLP.

The committee heard from a panel of private sector cyber security professionals. John Dickson, Principal, The Denim Group, relayed to the committee his experience at an IT conference after a statewide public sector security breach. When he asked the IT officials if their chief executive officers had inquired about their susceptibility to a breach, only about a fourth of them had. When asked if any of them had been requested to come up with plans to address security lapses or to come up with resources to address potential security breaches, none had.

At least at that time, those agencies had not truly learned the lessons from known breaches. The heads of the agencies did not consider cyber security as a top concern. Of course, this occurred several years ago. Since then, several well-publicized breaches have occurred in other states and in the federal government.

In his experience, Dickson noted how different agencies have prepared themselves for the increasingly sophisticated cyber security attacks. Whereas there are pockets of security excellence throughout the state in certain agencies where advances in defense protect the sensitive data of citizens to provide self-service capabilities for more open government, there are agencies that are likely woefully unprepared for a sophisticated attack and have sensitive taxpayer information at risk that point to a broader challenge that exists across the state. Dickson believes that cyber security should be a major public policy focus for the state. He fears that unless the state changes its strategy, one of the agencies will likely encounter another breach that will interrupt its ability to govern, prohibit businesses across the state to conduct commerce, and will likely result in a widespread crisis in confidence in state government.

Also on the private sector panel was Mike Wyatt, Director, Deloitte & Touche, LLP. Wyatt presented information in regard to managing state cyber security risks. He pointed out that our

economy and society use platforms designed for sharing information and staying connected, not protecting it. State agencies collect, share and use large volumes of the most comprehensive citizen information. This data makes states an attractive target for both organized cyber criminals and hacktivists. Innovations that drive growth also create cyber risk. As agencies strive to serve their constituents better, they use new technologies such as web-based services, social media, cloud services and mobile applications that could increase risks.

According to Wyatt, perfect security is not feasible. Instead, the state should reduce the impact of cyber incidents by becoming more secure: enabling business innovation by protecting critical assets against known and emerging threats across the ecosystem; more vigilant: gaining visibility and preemptive threat insight to detect both known and unknown adversarial activity; and more resilient: strengthening ability to recover when incidents occur.

A 2014 Deloitte-NASCIO Cybersecurity study found that only 24 percent of Chief Information Security Officers (CISO) versus 60 percent of agency chief executives had confidence in their ability to protect against external cyber attacks. However, both agree that the greatest barriers to cyber security are funding and the increased sophistication of threats.

Cyber strategy cannot be based solely on preventing the most recently publicized attacks. It is important to be secure - having risk-prioritized controls to defend critical assets against known and emerging threats; be vigilant - having threat intelligence and situational awareness to anticipate and identify harmful behavior; and be resilient - being prepared and having the ability to recover from, and minimize the impact of, cyber incidents. The costs and impact of a cyber attack may be more far-reaching than common references would indicate.

Brandon Neff, President, Innové discussed the current cyber threat environment. Like other witnesses, Neff stated that a diverse set of cyber threat actors are targeting public and private entities across the State of Texas. These actors include nation states, organized criminal syndicates, and insider or employee threats. He echoed that risk cannot be eliminated. The state should focus its cyber security spending to reduce risk on the Critical Systems and Data Assets that ensure the safety, security, and privacy of the public, or ensure the operational effectiveness of agencies to accomplish their stated mission in the public interest.

Neff agreed that as agencies embrace new technologies to serve the public - websites and mobile applications - the opportunity for attack increases as well. He stressed that one of the weakest points of entry for hackers is through an organization's personnel, who often unwittingly introduce malicious code by clicking links that appear to be legitimate.

Neff suggested the most immediate step is to conduct independent and regular compromise assessments to expose issues currently found on State systems or networks. A simultaneous next step is to conduct independent and regular perimeter assessments that identify the weak spots where cyber threat actors are most likely to gain entry. Having cooperative Public-Private partnerships among IT professionals will help Texas agencies improve their cyber security. And finally, sound cyber security practices must go beyond regulatory compliance. Cyber Threat Actors innovate faster than governments can regulate. Texas needs to reduce risk of breach for its most critical systems and data assets, not just being compliant with NIST or ISO cyber

security frameworks. In the future, given the speed of innovation among cyber threat actors, fully compliant organizations will still be vulnerable to breach. Compliance is a good step forward, but not sufficient for success.

Following the private sector panel, the committee heard from Edward Block, DIR; Lena Conklin, Legislative Budget Board (LBB); Mary Dickerson, TCEEDC; and Dr. Gregory White, UT-San Antonio (UTSA) and TCEEDC.

Mary Dickerson briefed the committee on the TCEEDC, its work, publication and recommendations. A substantial amount of the background for this charge was taken from her testimony. She informed the committee that efforts have been made towards creating partnerships through the Texas Cybersecurity Council to establish the Business Executives for Texas Security (BETS) partnership to provide a consistent voice for industry regarding cybersecurity policies in order to facilitate communication between the state and industry.

Gregory White, PhD, also a member of the TCEEDC and Director of the University of Texas at San Antonio's Center for Infrastructure Assurance and Security (CIAS), briefed the committee on cyber security threats, emphasized the importance of education and training in developing a culture of security, presented background information, and informed them of UTSA's esteemed cyber security programs. In 2014, UTSA was ranked the #1 Cyber Security Program by The Ponemon Institute. It is the first Texas school designated as a National Security Administration (NSA) / Department of Homeland Security (DHS) Center of Academic Excellence in Information Assurance Education. UTSA has received a number of prestigious designations and has security programs and centers in multiple departments in different colleges.

The UTSA CIAS was founded in the summer of 2001. While making an impact nationally, it has three main focus areas: Cyber Defense Competition Program, Infrastructure Assurance Programs, and Cyber Security Training & Awareness.

According to Dr. White, when a cyber event occurs, states and communities need a response plan. In response to this need, the CIAS has developed the Community Cyber Security Maturity Model (CCSMM). The CCSMM provides a structure which communities and states can use to determine their level of preparedness and to create a plan to improve their security posture and enhance their chances of successfully preventing or detecting and responding to a cyber attack.

When a cyber event occurs, it will not matter to citizens what type of incident it is or whether the state was specifically targeted. What matters to them is that they can still do the things they want to do –the infrastructures they rely on need to be functioning. State and community leaders need to be prepared to respond to a cyber event, no matter what type, in order to maintain the functionality of the cyber infrastructures their citizens rely on.

Edward Block, Department of Information Resources (DIR), updated the committee on the initiatives that DIR has taken, many in response to the TCEEDC's suggestions, and is in the process of implementing those suggestions, to improve cyber security for state agencies, as follows:

Third Party Assessments

DIR has performed security assessments of about 50 state agencies, using a third party vendor, to evaluate their overall cybersecurity stance. Based on these assessments, the following seven trends were identified:

- There are information security and cybersecurity staffing challenges
- There is an absence of secure software development standards
- Security governance and awareness is performed ad-hoc
- Often manual, there are duplicative agency identity and access management solutions
- There is a general lack of 24x7 event monitoring and analysis
- There is little network segmentation to segregate high-value assets
- There is a lack of data classification policies

According to DIR, staffing remains the most difficult issue to address due to negative unemployment rates for cybersecurity professionals. The other issues are being addressed by DIR as follows:

Secure software development: DIR is preparing a request for offer (RFO) to deliver managed application services through the statewide technology center. This would allow agencies to contract for software development.

Standards in security governance and awareness: In 2015, DIR, working with a committee of information security professionals from state agencies, institutions of higher education and the private sector, repealed and replaced Texas Administrative Code Chapter 202, the administrative rule which sets statewide information security standards. The previous version had not had a substantial review for several years. The revised version of TAC Chapter 202 resembles the Federal Information Security Management Act (FISMA), prescribing the roles and responsibilities of state government. Technical controls are incorporated by reference and are not in the rule itself, which allows for greater flexibility in response to changing cyber threats. These technical controls are in the form of a controls standards catalog that is based on the National Institute of Standards (NIST) which represents a strong industry reviewed approach to securing information resources.

Identity and access management standardization: Senate Bill 1878 (84R) authorized DIR to conduct a study on new identification and access technologies that may better protect personal information held by the state. That study is ongoing with a report due to state leadership in November 2016.

Event monitoring and analysis: To provide 24x7x365 monitoring and analysis in a cost effective manner, DIR is preparing a RFO to deliver managed security service providers through the Data Center Services (DCS) program.

Network segmentation: Adequate network segmentation is based on data classification, which must be in place before segmentation decisions can be made. The nature of this type of segmentation is a logical or virtual network segment running on top of an existing physical network.

Data classification: In 2014, DIR published a whitepaper and template that agencies can use to develop a data classification program. Data classification ensures that resources are spent efficiently, protecting information to its requirements, rather than spending resources protecting all information to the same level.

Cybersecurity Framework

The 83rd Legislature tasked DIR with developing a unified Cybersecurity Framework. The elements that comprise the Framework are the TAC 202 revision and the Agency Security Plan template.

- **TAC 202:** In 2015, a revised Texas Administrative Code, Chapter 202, was adopted. (as mentioned above). The revised TAC 202 covers agency responsibilities and includes a Control Standards Catalog. It specifies the minimum information security requirements that agencies must employ to provide the appropriate level of security relevant to level of risk. Additionally, it contains a Control Crosswalk. The crosswalk maps TAC 202 to industry standards, regulatory requirements and compliance mandates. It allows agencies to consolidate a lot of steps. For instance, many agencies must meet state requirements, federal requirements and certain industry-specific requirements. With the Control Crosswalk, agencies can see at a glance how those requirements intersect and begin to prioritize efforts.

- **Agency Security Plan:** The Agency Security Plan template uses a common language to address and manage cybersecurity risk in a cost-effective way, based on business needs, without placing additional regulatory requirements on agencies. The template is divided into five concurrent and continuous functions, which are the same as NIST: Identify, Protect, Detect, Respond and Recover. The plan includes a Vendor Alignment Tool that enables vendors of security products and services to align their offerings to the Cybersecurity Framework, and Guidelines and Whitepapers to provide more resources and insights to help agencies manage the complexities of information security.

Cybersecurity Products and Services through the Cooperative Contracts Program

DIR offers cybersecurity products and services through the cooperative contracts program. Among the products and services offered are network security monitoring, alerting, and analysis services to provide early warning for attempted intrusions and cyber-attacks, as well as alerts to authorities that facilitate appropriate countermeasures; network intrusion prevention service to proactively identify and block known threats to network security; and testing services offered by DIR at no cost that include controlled penetration testing and web application vulnerability scanning.

The Archer GRC Portal

To tie together the overall state security program, DIR has implemented a governance, risk and compliance (GRC) software platform that is available to all agencies. This system gives each agency a full view of their security posture and provides the state CISO a holistic view of statewide cybersecurity. The GRC portal provides:

- **Incident management:** requires agencies to provide timely reporting of certain types of security incidents to DIR. Timely reporting is required (preferably within 24 hours) for incidents that propagate to other state systems, result in criminal violations, need to be reported to law enforcement, or involve disclosure of confidential data (i.e. sensitive personal data).
- **Analysis and risk assessment analysis:** TAC 202 requires all agencies and institutions of higher education to perform a risk assessment. DIR, through the Archer GRC portal, is providing a standardized method for performing these assessments. The portal offers agencies an application to prepare and submit their Security Plans, a dashboard that allows them to see their organization's security stance, comparison statistics for incident management and response, and applications for agencies to perform risk assessments, manage policies and policy exceptions.

Education and Training

In its 2015 Data Breach Investigations Report, Verizon stated that “more than two-thirds of incidents that comprised the Cyber-Espionage pattern have featured phishing.” Phishing is a form of attack that uses emails to trick victims into downloading malicious code, visiting a malicious website, or entering their credentials. In 2012, South Carolina's Department of Revenue was the victim of a phishing attack, resulting in the loss of personally identifying information of 80 percent of its citizens and costing the state more than \$15 million. Most phishing attempts are not detected by standard Anti-virus. The best method to prevent this type of attack is through user education and training.

There are a variety of educational and training opportunities for state agencies. DIR offers security training classes (both in-person and online) tailored to the needs of Information Security Officers within state agencies. They provide end-user level security awareness training online to agencies that request it and offer monthly tabletop security exercises in partnership with the University of Texas at San Antonio's Center for Infrastructure Assurance and Security (CIAS). These exercises are free for agencies. DIR publishes monthly newsletters covering security topics and outlining ways to improve individual security programs. The Statewide Information Security Advisory Committee (SISAC) is made up of Information Security Officers from state and local government as well as representatives from private industry. Its purpose is to cross-pollinate ideas and best practices among members as well as make recommendations to DIR with regard to information security operations.

Lena Conklin, Legislative Budget Board (LBB), clarified the two provisions contained in the 2016-17 General Appropriations Act (GAA) pertaining to cybersecurity projects. The provisions were added as a result of several security and modernization-related project requests made by state agencies in their 2016-17 Legislative Appropriations Requests (LARs). The reports

required by these provisions will provide DIR's assessment of 2018-19 biennial requests and inform LBB recommendations. Several of the requesting agencies cited DIR initiatives, such as security assessments and the legacy systems study, in their 2016-17 LARs as an informing factor in making the requests.

The 2016-17 State of Texas Budget included the following budget riders:

Sec. 9.10. Prioritization of Cybersecurity and Legacy System Projects.

Out of funds appropriated elsewhere in this Act and in accordance with Government Code, Chapter 2054, the Department of Information Resources (department) shall submit a prioritization of state agencies' cybersecurity projects and projects to modernize or replace legacy systems, as defined in the October 2014 Legacy Systems Study, to be considered for funding to the Legislative Budget Board by October 1, 2016. Agencies shall coordinate and cooperate with the department for implementation of this provision.

This provision directs DIR to submit to the LBB, by October 1, 2016, a prioritization of state agencies' cybersecurity projects and projects to modernize or replace legacy systems for funding consideration. Agencies are directed to coordinate and cooperate with DIR for this purpose.

In preparation for the report, the agency is currently in the process of surveying agencies for information on upcoming requests for the 2018-19 LARs. The survey gathers information on identifying risks being addressed by agencies' requests, along with information on their probability and impact.

Sec. 9.11. Cybersecurity Initiatives.

(a) Out of funds appropriated elsewhere in this Act to agencies listed in subsection (d) for cybersecurity initiatives, agencies shall coordinate with the Department of Information Resources "department" to ensure security standards promulgated by the department in accordance with Government Code, §2054.059 are met.

(b) In accordance with Sections 2157.006 and 2157.068, Government Code, the Department of Information Resources may require the state agencies identified in subsection (d) of this section with plans to purchase network security hardware and software, out of funds appropriated elsewhere in this Act, to coordinate such purchases with the department to achieve additional cost savings through a coordinated bulk purchasing effort. Agencies identified in subsection (d) of this section shall cooperate with the department's requirements. Other state agencies and institutions of higher education receiving an appropriation by this Act for network security hardware and software, may also coordinate with the department through a coordinated bulk purchasing effort.

(c) In accordance with Government Code, Section 2054.003, any cybersecurity initiative may be considered a major information resources project and may be subject to review by the Quality Assurance Team.

(d) Agency:

- (1) Department of Aging and Disability Services;
- (2) Department of Assistive and Rehabilitative Services;
- (3) Department of Family and Protective Services;
- (4) Department of State Health Services;
- (5) Health and Human Services Commission;
- (6) Higher Education Coordinating Board;
- (7) Office of Court Administration;
- (8) Parks and Wildlife Department;
- (9) Department of Insurance; and
- (10) Department of Licensing and Regulation.

(e) By October 1, 2016, the Department of Information Resources shall report to the Legislative Budget Board on the status of the cybersecurity initiatives and bulk purchasing efforts for the agencies listed in subsection (d) in this section, including the progress made in meeting the cybersecurity framework in Government Code, §2054.059 and the cost savings realized through the coordinated bulk purchasing effort required under subsection (b) of this section.

Sec. 9.11 identifies ten agencies with funding for cybersecurity initiatives and directs the agencies to coordinate with DIR to ensure security standards promulgated by DIR are met; authorizes DIR to conduct a bulk purchase of network security hardware and software and requires the identified agencies to coordinate such purchases through DIR (other state agencies and institutions of higher education (IHEs) may also participate in the bulk purchasing effort); authorizes cybersecurity initiatives to be considered a major information resources project for review by the Quality Assurance Team (QAT); and requires DIR to submit a report by October 1, 2016, to the LBB on the status of cybersecurity initiatives and bulk purchasing efforts. The report must include the progress made in meeting the cybersecurity framework developed by DIR and any cost savings of the bulk purchasing initiative.

Ms. Conklin explained that funding for IT security services at DIR is primarily contained in the following three strategies:

Strategy A.1.3, Statewide Security funding provides DIR with resources to implement statewide information technology security policies, procedures, standards, and guidelines to state agencies and IHEs. For 2016-17, \$0.7 million was appropriated for this strategy.

Strategy B.3.1, Statewide Cyber Security Services funding provides risk management tools, such as incidence and compliance reporting, access to security research and advisory materials, and training. In fiscal years 2014 and 2015, 124 and 304 agencies and IHEs, respectively, participated in DIR provided training offerings; 150 agencies and IHEs are expected to participate in the trainings in each fiscal year of the 2016-17 biennium. Additionally, funding provides security assessments conducted by a third-party vendor (currently NTT Data and previously Gartner) which evaluates agencies and IHEs overall security postures and identifies areas for improvement. Agencies and IHEs are selected to receive security assessments based on

various risk factors, as well as agency size and budget. An agency may volunteer or request to have an assessment. During the 2014-15 biennium, 26 security assessments were performed; 30 assessments are expected in the 2016-17 biennium. For 2016-17, \$11.5 million was appropriated for this strategy.

Strategy C.2.2. Network and Telecommunications Security Services funding provides for operation of the Network and Security Operations Center (NSOC) which delivers enhanced statewide network communications services. The program provides network security services, including incident monitoring and response and various network testing services to participating state agencies and IHEs. Among testing services provided are controlled penetration tests (CPTs) which identifies network and system vulnerabilities by attempting a mock-attack on agencies networks. According to the agency, 50 CPTs were performed in fiscal year 2014 and 48 in fiscal year 2015; 50 CPTs are expected to be performed in fiscal year 2016.

Services are provided to state agencies and institutions of higher education at no direct cost. Programs are funded through the administrative fee charged to purchases made through the Cooperative Contracts program deposited to the Clearing Fund and administrative fees and charges made through the Capital Complex Telephone System and Texas Agency Network (TEX-AN) programs deposited to the Telecommunications Revolving Fund. For the 2016-17 biennium, \$0.7 million was appropriated for Strategy C.2.2.

6



RECOMMENDATIONS

Require Executive Director, Commissioner, CEO level approval for annual agency cyber security risk report

Texas' cybersecurity approach needs to evolve. In the private sector, boards increasingly view cyber risk as a first order business risk. A sound cyber risk program is not simply a cost to the business – It is an integral aspect of achieving business success.

Cyber security risk is a policy-level issue to be handled at the elected and appointed official level, not just administratively at an agency or within information technology departments at agencies. In the private sector, cyber security risk has been elevated to a Board of Directors and CEO issue. The equivalent should happen within the State of Texas, from the Governor's office, to the Legislature, and at the appointed policy level within state agencies.

Other states, including Utah and South Carolina, have already experienced major cyber security breaches. As mentioned, states like South Carolina and Utah have experienced major security breaches that involved spending millions of dollars to restore citizen trust. In South Carolina, cyber security remediation remains front and center as a public policy discussion.

Per TAC 202.23.a.2, the agency head is given an annual, comprehensive risk evaluation report that is prepared by the agency ISO. The report can be kept on file for future reference or provided to leadership if requested. The agency head should be required to approve the report.

Increase the number of cybersecurity practitioners in Texas to provide the expertise needed to grow cybersecurity investment and to protect the cyber assets of the state

Nationwide, there is a shortfall of trained cybersecurity professionals. In some areas there is a negative unemployment rate (meaning there are more jobs available than job seekers.) Recruiting and retaining a qualified IT workforce for the public sector continues to be a challenge. The state should continue to invest in higher education cybersecurity programs in order to attract students to the cybersecurity field, spur research and development, and encourage institutions of higher education to become leaders in cybersecurity within their own communities. Additionally, increased innovative efforts, which have shown promise, should be encouraged. One such effort is to work with federal and state military representatives regarding transition plans for veterans.

Central Legislative Committee Responsible for Cyber Security Risks

The Texas House of Representatives, through its House Resolution that adopts the permanent House Rules of the 85th Legislature, should select one standing committee to have jurisdiction over cybersecurity policies.

Funding to Replace Legacy Systems

“Legacy Systems” are information resources that are no longer supported by the manufacturer. These systems may seem to function correctly, but security patches and fixes are no longer available from the manufacturer, which creates vulnerability in the statewide network. Without the funding to continually refresh information resources, the technology debt continues to build.

Information Sharing and Collaboration

As a federated form of government, each agency and institution of higher education has their own security function. Many of these agencies have tools and technologies to counter cyber-threats. Through information sharing and collaboration among entities the benefits from these tools is multiplied. The committee suggests the implementation of the recommendations of the Interagency Data Transparency Commission (IDTC) report.

In 2015, the Interagency Data Transparency Commission (IDTC) was established to conduct a study of current data structure, classification, sharing, and reporting protocols for the state. Their report, published on September 1, 2016, made several recommendations. Among them are establishing a focus within larger agencies that oversees Enterprise Information Management (EIM) functions; establishing EIM best practices and training program; designating the Texas Open Data Portal as the preferred location for all public data; and establishing Open Data best practices and training program. The Commission also recommends creating a centralized data-sharing portal for interagency data sharing; establishing interagency data sharing best practices and an aligned training program;

Commercialization of University Technology

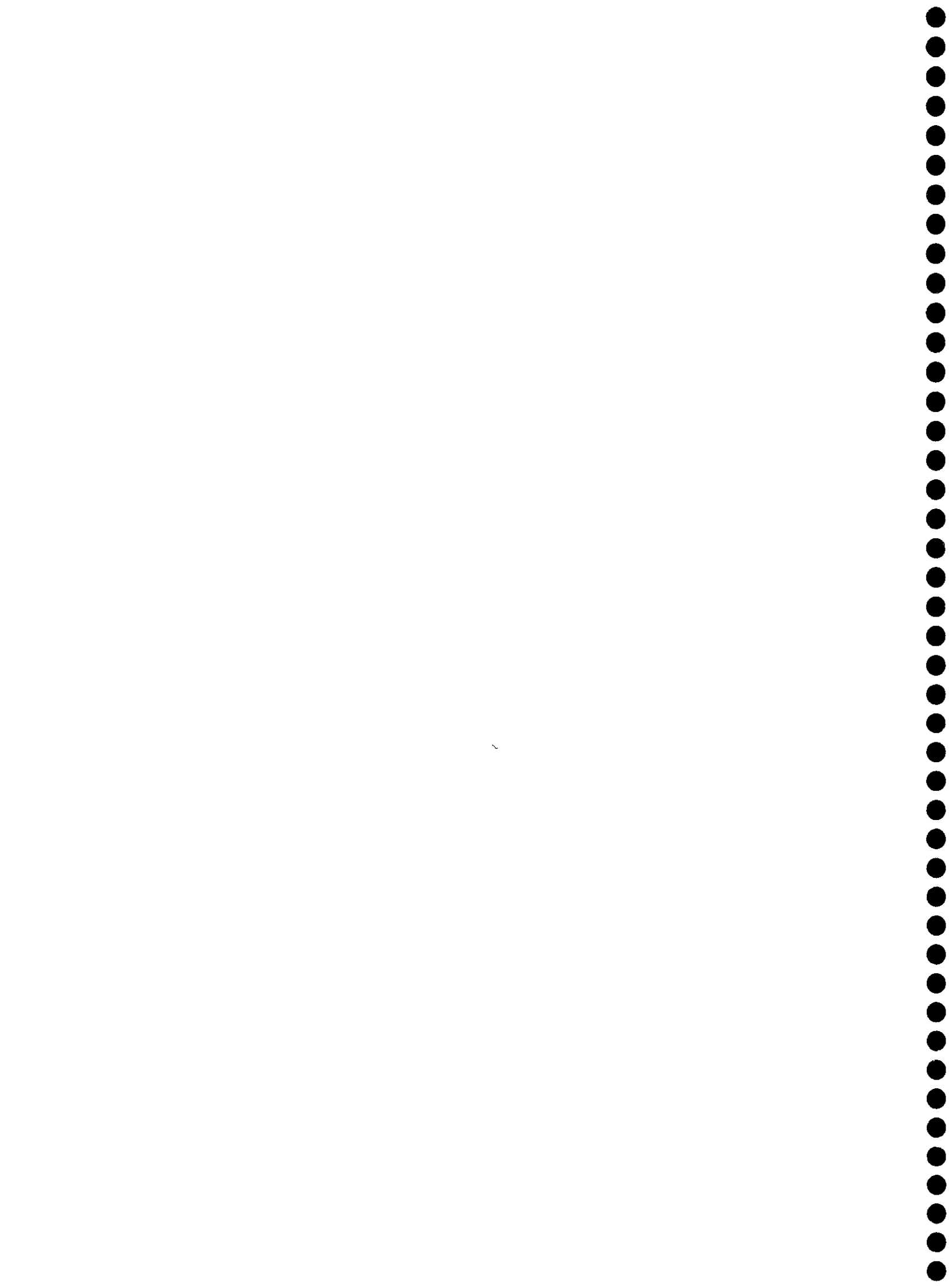
The state should consider promoting collaboration, innovation, and entrepreneurship in cyber security to facilitate the commercialization of university research and development and encourage the development of new businesses with innovative products and services in cybersecurity.

Increase the leadership role of DIR in establishing a sustainable Cybersecurity Awareness Program for all Texans.

The Texas CISO is currently serving dual roles as both the state Cybersecurity Coordinator and Chair of Texas Cybersecurity Council. There needs to be an increase in the full-time staff and additional funding allocated to state cyber security coordination and state awareness efforts. Current awareness efforts include an electronic newsletter and partnership with DHS for National Cybersecurity Month events.

INTERIM CHARGE #2

Examine purchasing practices by state agencies to ensure such practices are efficient and transparent.



BACKGROUND

According to some researchers, one-third of all government spending goes towards purchasing goods to provide services and execute government missions. Improving the efficiency of these transactions could lead to budgetary savings. The vastness and complexities of this budgetary spending, however, is often mired in old technology. Texas is striving to make statutory and technological improvements which should lead to efficiencies - cost savings - and transparency.

In Texas, there has been a shift from directly delivering services to contracting for the delivery of many of those services. There are concerns that adequate accountability and transparency mechanisms have not been put in place to monitor these contracts.

Recent news coverage and reports from various state agencies have outlined many problems with the way state government contracts for goods and services, highlighting the need for improved contract management practices and reporting of the contracts across state government agencies. In response, the Legislature enacted a number of reforms to the contracting and purchasing statutes at state agencies during the 84th Legislature. However, more than one report from the State Auditor's Office has a quote similar to the following:

The Commission had adequate controls over its purchasing process; however, it did not consistently (1) follow its processes related to obtaining required signatures and approvals and (2) retain required documentation to support compliance with purchasing requirements. In addition, the Commission had not fully documented its purchasing processes.

Although procurement authority is delegated to each state agency, state law provides the structure for and mandates the use of a centralized purchasing system by state agencies. The centralized statewide procurement system was created for the purpose of supporting state operations and shortening the procurement cycle for agency purchasers. Centralization of purchasing also allows for the state to benefit from potential economies of scale from bulk purchases and helps reduce redundant staff work across all state government purchasing offices. Over the past 20 years, the state has encouraged a centralized system for cooperative contracts so the state may take advantage of cost savings and increased effectiveness. These efforts have allowed the state to consolidate information technology services shared by state entities, increase volume purchasing of services, and improve management of major information projects—which all represent a significant cost savings as well as increased efficiency and accountability in state and local contracts. The authority to make purchases on behalf of state agencies is granted to the Comptroller of Public Accounts (CPA) for most purchases and to the Texas Department of Information Resources (DIR) for telecommunications and information resources purchases.

DIR's Cooperative Contracts program was created with the passage of HB 1516 (79R). The legislation requires state agencies to buy commodity items via DIR Master Contracts, unless the agency obtains an exemption from DIR. DIR offers more than 750 technology Master Contracts for products and services such as computers, software, security hardware and services, networking equipment, telecommunications equipment, IT staffing services and technology-

based training. The contracts were used for more than \$2 billion dollars of purchasing activity in FY15, approximately 25% of the purchasing volume was state agencies, excluding higher education. These Master Contracts generate more than \$200 million in annual cost savings for customers, including local governments and independent school districts (ISDs), through negotiated MSRP discounts and by streamlining the procurement process for customers.

Customers place orders directly with the vendors participating in the Cooperative Contracts program. Invoicing and payment transactions occur directly between the agency and the awarded vendor. This program saves DIR customers time, money and resources.

During the 84th Regular Legislative Session, a number of changes were instituted to increase the efficiency and transparency of government purchasing by the State of Texas. Among these, the CPA was charged with determining what state agencies must report or provide in the Centralized Accounting and Payroll/Personnel System (CAPPS) related to purchasing, including contracts and solicitations. CAPPS strives to provide a single financial and human resources (HR)/payroll administration software solution for Texas state agencies. CAPPS seeks to increase efficiency and transparency in the state's purchasing process. It allows aging and inefficient legacy systems to be replaced with an easy-to-use, easy-to-update system that can be scaled to meet the needs of any agency regardless of complexity and size. Reporting is easier and more accurate with CAPPS. Agency functions are recorded in a common data language on an interconnected system that allows financial and HR/payroll departments to exchange information quickly, safely and reliably.

Additionally, the Legislature required the CPA to conduct a study examining the feasibility and practicality of consolidating state purchasing functions into fewer state agencies or one state agency. Further, it required that the study examine the cost savings that may be achieved through abolishing offices or departments of state agencies that have a dedicated office or department for purchasing; and consolidating or reducing the number of vendors authorized to contract with this state to allow this state to better leverage its purchasing power. That study, which will contain a much more in-depth report of this charge, including a report on the process for the legislature or the executive branch to implement the consolidation of state purchasing; and the total cost to this state of the purchasing responsibilities for each state agency, including the dedicated office or department in the agency with purchasing responsibility, will be available on the Comptroller's website, no later than December 31, 2016.

HEARING

On April 5, 2016, the House Committee on Government Transparency & Operation met in a public hearing in Austin, Texas, to consider the following charge:

Examine purchasing practices by state agencies to ensure such practices are efficient and transparent.

The Committee heard testimony from the following:

Dana Collins, Texas Department of information resources;
Bobby Pounds, Texas Comptroller of Public Accounts;
Jacob Pugh, Legislative Budget Board;
Jennifer Saha, Computing Technology Industry Association; and
Sandra Woodruff, Texas Comptroller of Public Accounts.

Jennifer Saha updated the Committee on the Computing Technology Industry Association's (CompTIA) Texas Procurement Committee activities. The group has focused on recent procurement reforms and advocating for efficient and transparent procurements within the state. They have met quarterly and have provided input to the CPA and DIR on procurement best practices.

CompTIA advocates continuing the use of cooperative contracts and other pre-negotiated vehicles. However, recent changes to the cooperative contracting have decreased the purchasing limits, making agencies use them only for smaller contracts. Additionally, according to CompTIA, newly mandated reviews add to procurement timelines and decrease efficiency. CompTIA members have seen negative impacts due to this change. Often seeking the most efficient way to procure goods and services, these changes can be counterproductive to efficiency, but the other side of the argument is that these new measures mitigate risk. This has always been the balance of procurements: a balance of risk and efficiency that produces the most successful goods and services to citizens.

New rules and agency implementation have been carefully observed and watched by many industry eyes during the interim. According to Saha, the most important impact observed relates to communications and transparency. CompTIA's members have experienced first-hand instances where agencies are incorrectly stating that they cannot meet with or talk to any vendors. This has resulted in a slow-down of the procurement process. The technology industry that serves Texas has experienced a concerning firewall from state agencies when it comes to discussing innovative solutions to agency business problems. It seems that new rules relating to procurements have confused agencies and made them averse to dialogue between agency staff and vendors because they are afraid of breaking the new laws. CompTIA's Texas Procurement Committee believes that this lack of communication is one of the largest problems resulting from the recent implementation of new rules and laws. The group is embarking on an initiative to educate agencies about the agencies' authority to communicate with industry. These communications help craft successful, competitive procurements, which ultimately, is in the best interest of the State.

Saha told the Committee that some states have legislated strong definitions of allowable communications in order to clarify precise rules around information sharing. Such rules allow for welcomed clarity as to what is and is not allowable by both state employees and the vendor community. Industry has supported such legislation in the past as it provides clear rules to which vendors and state agencies are equally held accountable.

CompTIA is very interested in the Comptroller's Centralized State Purchasing Study. They have engaged the Comptroller's team in discussing the vendor portion of that study.

The Texas Vendor Performance Tracking System is of specific interest to Texas vendors and nationally. Other states are examining the system. Texas' vendor performance tracking system is online and mandated for widespread use. Vendors appreciate the transparency and accountability that is inherent in a vendor scoring system and CompTIA advocates for fair, efficient and easy-to-use systems when they are examined in Texas and other states.

Dana Collins from the Texas Department of Information Resources (DIR) provided the committee with information on DIR. DIR provides statewide leadership and oversight for management of government information and communications technology. DIR provides technology knowledge, leadership and solutions to state agencies. As part of that mission, a Statement of Work (SOW) is required, from agencies to DIR, for certain IT services over \$50,000. Those services include certain Cloud Services, Deliverables Based Information Technology Services (DBITS), Managed Services for Information Technology, IT Security Services and Comprehensive Web Development. SOWs are not required for IT Staffing Services, Support Agreements, Maintenance Agreements, or Hardware or Software Only Contracts.

DIR reviews the agency SOW to ensure the scope is appropriate for the DIR contract selected and consults with the agency. DIR responds to the agency within 30 working days of submission, and then the agency submits the approved SOW to relevant DIR vendors. The agency evaluates vendor responses, and executes a final version of the SOW. The agency sends the final signed SOW to DIR for approval. DIR reviews, approves, signs and returns the SOW to agency. Finally, the agency issues the purchase order to the selected vendor. Vendors cannot be paid until DIR signs the final SOW. For increased transparency, agencies must post all executed SOWs on their websites.

Bobby Pounds, from the Office of the Texas Comptroller of Public Accounts (CPA), explained to the Committee the CPA Study mandated from the 84th Legislature Session. The Legislature charged the CPA with conducting a study that examines the feasibility and practicality of consolidating state purchasing functions. The CPA has contracted with RSM US LLC to perform data analysis and consulting services in support of the CPA Study.

The study must examine the cost savings to the state that may be achieved through abolishing offices or departments of state agencies that have a dedicated office or department for purchasing; consolidating or reducing the number of vendors authorized to contract with the state to allow the state to better leverage its purchasing power; a detailed projection of expected savings or costs to the state in consolidating state purchasing; a report on the process for the

legislature or the executive branch to implement the consolidation of state purchasing; a list of state agencies, including dedicated offices or departments in those agencies, with purchasing responsibilities; and the total cost to the state of the purchasing responsibilities for each state agency, including the dedicated office or department in the agency with purchasing responsibility.

The RFP was awarded in March 2016. CPA has begun working with the vendor as a liaison between the selected agencies to begin identifying and collecting relevant data pursuant to the purpose of the study. The CPA has determined that 110 state agencies will be studied by analyzing expenditure data for fiscal 2014 and fiscal 2015 obtained from the Uniform Statewide Accounting System (USAS) and, for agencies that employ it, the Centralized Accounting and Payroll/Procurement System (CAPPS). Institutions of higher education will not be studied. RSM developed a survey — that was distributed by the Comptroller to agencies in April — to help determine the number of personnel involved in the purchasing and contracting processes. RSM has analyzed the data and benchmark Texas purchasing to inform the CPA and ultimately the Legislature about how Texas state purchasing practices compare with other public sector and private sector environments.

CPA has proactively initiated a study of the vendor community to address procurement issues at the vendor level to run parallel to the purchasing study. This study consists of a 21-question survey distributed to vendors to obtain feedback as to how to establish efficiencies and transparency in state contracting and realize cost savings from a vendor perspective.

The Comptroller aims to present realistic opportunities for the Legislature to enact effective reforms to the state purchasing process, in light of existing and ongoing efforts such as the consolidation of state agencies that provide health and human services, the ongoing implementation of CAPPS, and statutes that regulate state agency spending and authorize certain delegated spending. At this writing, the CPA is completing its report using the RSM data and analysis. It will be available on the CPA website no later than December 31, 2016.

Sandra Woodruff updated the committee on CAPPS - the Centralized Accounting and Payroll/Personnel System used by the CPA. CAPPS seeks to increase efficiency and transparency in the state's purchasing process. It allows aging and inefficient legacy systems to be replaced with an easy-to-use, easy-to-update system that can be scaled to meet the needs of any agency regardless of complexity and size. Reporting is easier and more accurate with CAPPS. Agency functions are recorded in a common data language on an interconnected system that allows financial and HR/payroll departments to exchange information quickly, safely and reliably.

The 84th Legislature charged the CPA with determining what state agencies must report or provide in CAPPS related to purchasing, including contracts and solicitations. The CPA evaluated options in the CAPPS software and developed a method for electronically storing all of the data noted in SB 20, Section 9 (84R). The CPA developed standards for the entry of procurement and contracting information into CAPPS. The CPA and LBB are working together to develop an automated interface from CAPPS to the LBB's contracts database. Once completed, report development will begin. Additionally, the CPA will be addressing access

needs for Oversight Agency inquiry access to CAPPs. The CPA is creating security roles to allow the LBB and DIR direct access to procurement and contracting information in CAPPs, including the ability to drill down to attachments for each contract or purchase order.

According to Woodruff, CAPPs deployment activity continues as scheduled. 26 additional agencies have deployed CAPPs Human Resources and payroll functions. An additional 11 agencies deployed CAPPs Financials in September 2016. Nine agencies are scheduled to deploy CAPPs HR/Payroll in 2017 and 27 agencies will deploy CAPPs Financials in 2017.

With continued funding, CAPPs deployments will conclude at the end of Fiscal Year 2020. Executive briefings have been held with all agencies not currently on the deployment schedule. The CPA anticipates a deployment plan for all remaining agencies will be created by the end of May 2016.

Jacob Pugh, Legislative Budget Board, presented information to the committee regarding the overview of contract reporting requirements, the contracts database, LBB support to agencies, monitoring risk and reviewing selected contracts. He reminded the committee that two new provisions were adopted by the 84th Legislature in the General Appropriations Act (GAA) that increase transparency in state procurements. GAA Article IX, Section 7.04 requires all contracts over \$50,000 to be reported to the LBB, regardless of funding source. "Contract" is widely construed to include grants, interagency agreements, and any purchase of goods or services. And, GAA Article IX, Section 7.12 requires all contracts over \$10 million to be reported to the LBB, regardless of funding source, as well as emergency and sole-source contracts over \$1 million. Additionally, an attestation letter, or certification, signed by the executive director of the agency must be provided that attests to the procurement's compliance with the State of Texas Contract Management Guide, Procurement Manual, and all applicable statutes, policies, and rules related to procurement.

Several statutory provisions require agencies and institutions of higher education to report other contracts to the LBB. For instance, all contracts over \$50,000, and professional and consulting services contracts over \$14,000, must be reported to the LBB. Exemptions to this requirement include Texas Department of Transportation, Health and Human Service Agencies, and Institutions of Higher Education and System Offices. However, these exemptions do not preclude the LBB from requesting contract documents and other supporting documents from state entities.

The LBB maintains a contract database. The database is a single system for reporting contracts and contract documents to the LBB. It houses data that is publicly available and searchable. Recently, the interface with the CPA was completed, so the LBB database now receives contract data directly from CAPPs. It provides richer data for oversight and improved accuracy for increased transparency. LBB staff review contract data to ensure compliance with reporting requirements and assist agencies in reporting accurate and complete information.

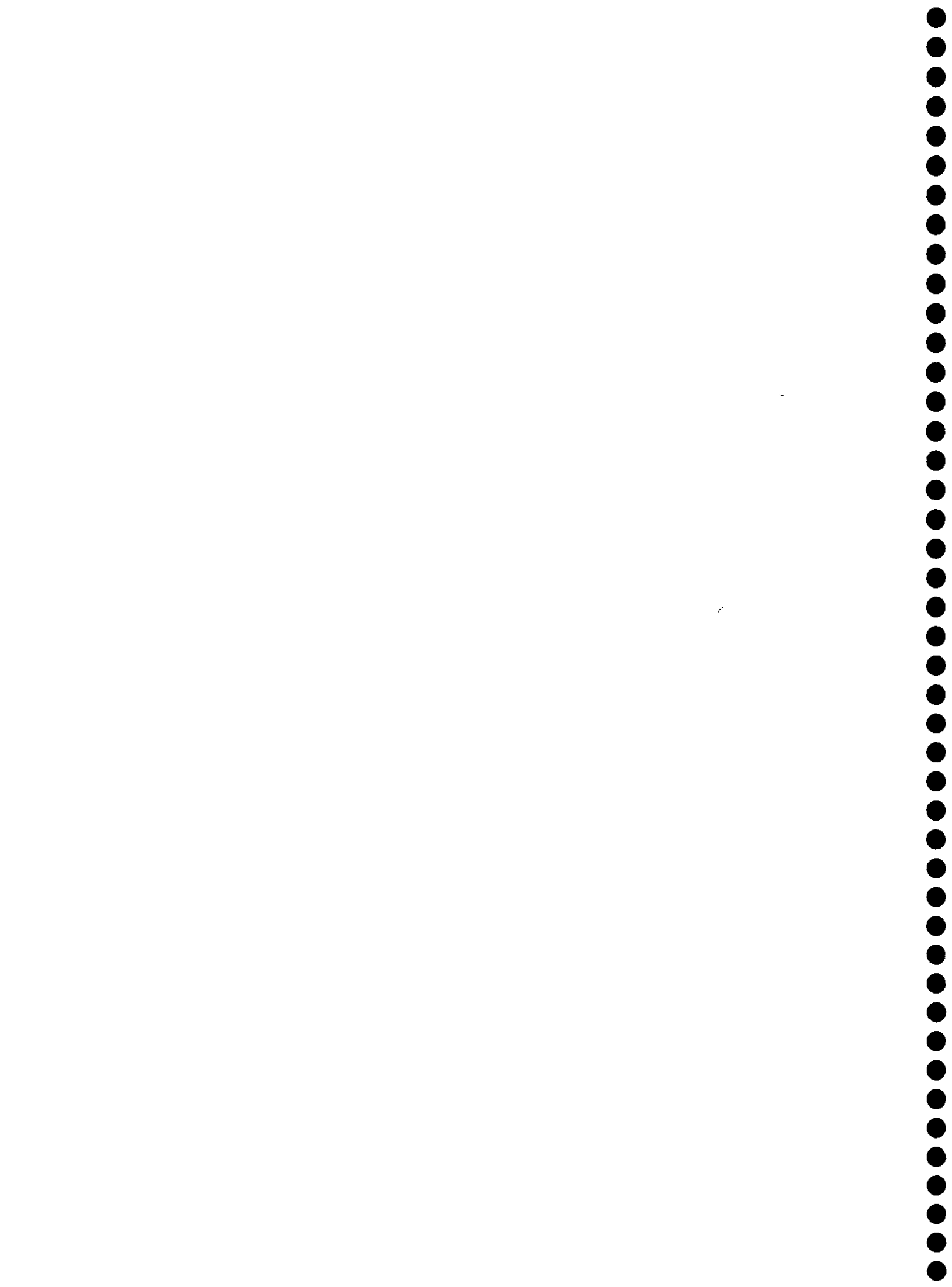
Improvements to the new LBB database include more reportable data fields for a more comprehensive view of contracts, searchable and downloadable data for agency or public use, enhanced data entry controls to reduce duplicate or inaccurate entries, rapid response to information queries and flexible, responsive in-house design and implementation.

The newly established LBB Contracts Oversight Team (COT) maintains the Contracts Database and monitors reported contract information. Initially, LBB is working with high-volume agencies to complete reporting. The COT has prioritized contracts subject to Article IX 7.12 for reporting, followed by remaining current fiscal year contracts and then fiscal year 2015 contracts. To support agency reporting, COT has provided training, both initially upon deployment of the new database and on an ongoing basis as necessary with agencies. COT maintains updated training materials and detailed reporting instructions on its website.

In addition to maintaining the Contracts Database, COT monitors state contracting to identify and mitigate risks. The COT establishes protocols for assessing risk across all procurements submitted to the LBB Contracts Database. A web form for is available for individuals, vendors, or employees to report potential contracting issues. Additionally, the COT conducts in-depth reviews of certain contracts with a goal of working with state entities to help mitigate or remediate risk. COT makes budget and/or policy recommendations to improve the framework and requirements related to procurement or to individual agency's processes for administration and oversight.

Preliminary COT observations following initial contract reviews and interaction with agencies since the implementation of SB 20 include the following:

- Agencies and institutions of higher education sometimes conflate the contract posting requirements of SB 20 with other statutory and GAA contract reporting requirements.
- Agencies do not always have ready access to documentation related to a vendor's selection.
- Risk to the state is often introduced during the solicitation and contract formulation phases of procurement.
- Negotiation with vendors over a contract's terms and conditions can weaken protections for the state.
- Outsourcing a function or system development can limit an agency's flexibility in reallocating resources when priorities shift.



CONCLUSION

The committee heard testimony that the most important impact observed from the recent implementation of new rules and laws relates to a lack of communication and transparency. The technology industry that serves Texas has experienced a concerning firewall from state agencies when it comes to discussing innovative solutions to agency business problems. According to some, it seems that new rules relating to procurements have confused agencies and made them averse to dialogue between agency staff and vendors because agency staff fears breaking the new laws. This could result in a slow-down of the procurement process.

The CPA and DIR have conducted training webinars and provided policy guidance to agencies regarding the new rules. On September 15, DIR published a memo on vendor/agency communications, which is available on their website. The committee encourages the CPA and DIR to continue their efforts to educate agencies about the agencies' authority to communicate with industry. These communications help craft successful, competitive procurements, which ultimately, is in the best interest of the State.

The 84th Legislature tasked the CPA to examine the feasibility and practicality of consolidating state purchasing functions into fewer state agencies or one state agency. Further, it required that the study examine the cost savings that may be achieved through abolishing offices or departments of state agencies that have a dedicated office or department for purchasing; and consolidating or reducing the number of vendors authorized to contract with this state to allow this state to better leverage its purchasing power. That study, which will contain a much more in-depth report of this charge, including a report on the process for the legislature or the executive branch to implement the consolidation of state purchasing; and the total cost to this state of the purchasing responsibilities for each state agency, including the dedicated office or department in the agency with purchasing responsibility, will be available on the Comptroller's website, no later than December 31, 2016.

The Committee looks forward to implementing recommendations from the Comptroller's study. The CPA's study aims to present realistic opportunities for the Legislature to enact effective reforms to the state purchasing process, in light of existing and ongoing efforts such as the consolidation of state agencies that provide health and human services, the ongoing implementation of CAPPs, and statutes that regulate state agency spending and authorize certain delegated spending.



INTERIM CHARGE #3

Study issues related to access to public information held outside of the custody or control of the governmental body by current or former officers or employees. Assess whether the Public Information Act's procedures for response to repetitious or redundant public information requests adequately protect small governmental bodies from the financial burdens imposed by such requests.



BACKGROUND

The Texas Public Information Act (the Act) was first adopted in 1973 following the Sharpstown Scandal. In 1993, it underwent a nonsubstantive revision and was codified as chapter 552 of the Texas Government Code. Citing the fundamental American philosophy of a constitutional form of government of the people, for the people, and by the people, the Act states that it is the policy of this state that each person is entitled to information about the affairs of government and the official acts of public officials and employees. Further, it states that the people, in delegating authority, do not give their public servants the right to decide what is good for the people to know and what is not good for them to know.

The Act provides a method for the public to request public information. The Act is triggered when a person submits a written request for information to a governmental body. If a governmental body wishes to withhold any information, it must generally seek a ruling from the Office of the Attorney General (OAG) within ten business days.¹ The governmental body must explain the basis for withholding the information and provide a copy of the information to the OAG for review within fifteen business days. If a governmental body does not seek to withhold information, it must release the requested information promptly. "Public information" includes any information that is written, produced, created, assembled, or maintained by or for a governmental body. It includes information in the custody of a third party, if that information relates to the transaction of official business. It also includes any electronic communications on any device, even a personal e-mail account or personal cellular telephone, if the communications are in connection with the transaction of official business. The Act also sets out exceptions to the release of public information.

Although "public information" includes any electronic communications on any device, even a personal e-mail account or personal cellular telephone, if the communications are in connection with the transaction of official business. In a recent case, *City of El Paso v. Abbott*, the Third Court of Appeals recognized when information is held by an official or employee of a governmental body outside the custody of the governmental body itself, there is no recourse for a governmental body to compel its own official or employee to turn over that information.

In that case, certain e-mails responsive to a request for information were held in the private e-mail account of a city official. The OAG issued a ruling concluding the e-mails were "public information" subject to the Act because they related to the official business of the city and were held by a public official or employee of the city. Subsequently, the city produced all of the information it was able to identify, locate, and gather that was responsive to the request and that the OAG had determined must be released. Because of the efforts made by the city to locate and compile information contained in the private e-mail accounts, the court concluded the city had not refused to comply with the Act. But it also recognized there were no methods by which the city could compel the disclosure of public-information e-mails located on private e-mail

¹ A governmental body may withhold public information without requesting a decision of the OAG if it is expressly authorized by the Act (e.g. social security numbers) or if it is authorized by a previous determination of the OAG (e.g. personal information of officials and employees requesting that their personal information be kept confidential).

accounts. After *City of El Paso*, the 84th Legislature considered HB 1764 and SB 1087. These bills provided a mechanism for governmental bodies to compel individual holding records to return public information to the governmental body and also broadened the enforcement authority of the OAG. However, neither bill passed the legislature.

The Act provides the procedure for handling repetitious or redundant requests. A governmental body that receives a request for information it determines it has already furnished or made available may certify to the requestor it has already made the information available and specifies requirements of the certification. Further, a governmental body is allowed to recover reasonable costs associated with providing information in response to a request for public information, including, in some cases, costs of making copies and charges for time or labor. Additionally, HB 685 was passed and became effective in 2015. It allows a political subdivision to refer open records requestors to a specific website in response to the request when appropriate.

HEARING

On May 25, 2016, the House Committee on Government Transparency & Operation met in a public hearing in Austin, Texas, to consider the following charge:

Study issues related to access to public information held outside of the custody or control of the governmental body by current or former officers or employees. Assess whether the Public Information Act's procedures for response to repetitious or redundant public information requests adequately protect small governmental bodies from the financial burdens imposed by such requests.

The Committee heard invited testimony from the following:

Bill Aleshire, Attorney;
Chris Cobler, Texas Press Association;
Sherry Cook, Texas Alcoholic Beverage Commission;
Bruce Green, City of Lufkin;
Jim Hemphill, Freedom of Information Foundation;
Justin Gordon, Office of the Attorney General;
Ed Jones, Angelina County;
Kelley Shannon, Freedom of Information Foundation of Texas; and
Wes Suiter, Angelina County.

The charge was divided into two separate, yet related, issues. The first issue addressed in the hearing was access to public information held outside the custody or control of a governmental body. This portion of the charge is a result of the *City of El Paso v. Abbott*.

Bill Aleshire testified that use of personal email accounts to conduct government business is on the rise, no Texas statute prohibits such practice and those records are subject to the Act. If a Texas official operating under Texas law chooses to keep personal emails about official business concealed in personal email accounts—those emails would likely remain undisclosed, on personal servers or simply deleted without prosecution for destroying a government record. If a public information request is received by the state or local agency for emails, that agency would respond with only the information or emails in its possession, not those held by the employee on a personal email account. And if the requestor, and even the agency, knew of the existence of the emails held on a personal account, the Act would not enable the requestor to get a court order requiring the disclosure of those emails.

That hypothetical scenario is the result of the *City of El Paso v. Abbott* case. Public information advocates view this as a gaping hole in the enforceability of the Act. There is no requirement for the collection or disclosure of public information held privately by Texas public servants.

According to Aleshire, although most would agree that privately held emails are “public information” as that term is defined in the Act, as interpreted in *El Paso*, the Act waives sovereign immunity for a records requestor to bring suit only against the governmental body, not against the public servant who actually possesses the emails, and to obtain relief only if the

governmental body “refuses” to supply public information it possesses. Under the Act, if a public servant has government business emails on a personal email account and refuses to give the governmental body the government records and public information, no Texas court has jurisdiction to grant relief to the requestor to obtain the emails.

Chris Cobler related his recent experience with what he views as a loophole in the Act. When reporting on the actions of some Victoria City Council members in May 2013, he focused on the public’s suspicion that four council members had formed a walking quorum and had violated the Texas Open Meetings Act.

His newspaper filed an open records request for written communication among all council members in the days leading up to the meeting in question. Three complied with the request, but four did not. It became clear that the other four council members had written records responsive to the Act request.

After reaching this impasse, the city attorney told the reporter that he had no legal way to compel the council members to release clearly public information in their possession. Thus, the city attorney had to respond to the Texas Attorney General that he had done all he could to comply with the newspaper’s open records request. According to Cobler, the city attorney conceded this was a legal loophole that went against the spirit of the Act, but said his hands were tied.

Cobler told the Committee that the “custodian loophole” prevents the public from getting the full story about its elected officials’ actions.

Justin Gordon from the OAG testified on both parts of the charge. He testified that the Act requires a governmental body to make a good-faith effort to relate a written request to responsive information and to either release the information or seek a ruling from the OAG to determine if the information is excepted from public disclosure. A governmental body that refuses to provide information or to request a ruling may be subject to civil enforcement remedies under the Act. These remedies allow a requestor or the OAG to file suit against a governmental body for refusal to comply with the Act. The requestor also may refer a civil complaint to a local district or county attorney, or to the Travis County District Attorney if the governmental body is a state agency. Additionally, a public information officer may face criminal liability if, with criminal negligence, the officer refuses to provide access to public information. However, the OAG has no authority to enforce the criminal violations within the Act. A decision to prosecute a criminal violation under the Act rests with a local district or county attorney. Additionally, Gordon gave an overview of the *City of El Paso* case.

In summary, the Act provides for civil remedies and criminal penalties when a governmental body fails or refuses to provide public information in response to a request made under the Act. However, there are no statutory mechanisms for a governmental body to compel an individual officer, employee, or third party with personal custody of that information to provide it to the governmental body for release to the requestor.

Gordon then focused on the second part of the charge: Whether the Act's procedures for response to repetitious or redundant public information requests adequately protect small governmental bodies from the financial burdens imposed by such requests.

A governmental body must treat all requests for public information uniformly. An officer for public information may not ask why the requestor wants the information or what use the requestor will make of the information once it is released. Gordon told the Committee that the Act provides a procedure for handling repetitious or redundant requests. A governmental body that receives a request for information it determines it has already furnished or made available may certify to the requestor it has already made the information available and specifies requirements of the certification.

Further, a governmental body is allowed to recover reasonable costs associated with providing information in response to a request for public information. The rules generally allow a governmental body to charge \$0.10 per paper copy and \$15 per hour for personnel labor. However, a governmental body may not charge for labor if there are 50 or fewer paper pages of responsive information. A governmental body also is not allowed to charge the requestor for the time it takes to request a ruling from the OAG. Additionally, if a governmental body estimates the charges will exceed \$40, it must provide the requestor with a written itemized cost estimate before any work is completed. This estimate requires a response from the requestor, which may include modifying the request or narrowing the scope of the request. In certain circumstances, the governmental body may require the requestor to pre-pay a bond or deposit before it undertakes any of the work required to comply with the request. The Act provides that a requestor may inspect public information without receiving a physical copy. If the requestor chooses to inspect the records, the governmental body generally may not charge for labor or overhead costs and is restricted in charging for paper copies. The effect of these limitations is the requestor can gain access to public information at a reduced cost or at no charge. A governmental body must notify the requestor if a less-expensive or no-cost alternative is available when providing a written itemized cost estimate.

Although a governmental body may not charge for labor when there are 50 or fewer paper pages of information, it may establish a reasonable limit on the amount of time it spends on requests without recovering its labor costs.² The limit may not be less than 36 hours within a 12-month period, and the governmental body must keep track of the amount of time it has spent responding to these requests for each individual requestor. It must provide notice of accrued time to the requestor. Because all requests must be treated uniformly, a governmental body that chooses to establish a limit may not single out frequent requestors. The governmental body may begin assessing labor charges once it has exceeded the established time limit, even if a request results in 50 or fewer pages of information or if the requestor chooses to inspect the records without receiving copies.

² The limits do not apply if the requestor is: (1) an individual who, for a substantial portion of the individual's livelihood or for substantial financial gain, gathers, compiles, prepares, collects, photographs, records, writes, edits, reports, investigates, processes, or publishes news or information for specified types of news media, (2) an elected official, or (3) a representative of a tax-exempt publicly funded legal services organization. *See* Tex. Gov't Code § 552.275.

A governmental body that receives repetitious or redundant requests for information may certify to the requestor the information was already provided and no further response is required. A governmental body also may recover reasonable costs associated with providing information, and it may be able to require a requestor to pre-pay a bond or deposit before complying with the request. The Act also limits the amount a governmental body may charge a requestor for inspection of records or for requests where few records are responsive.

The Committee heard from several governmental bodies that are experiencing repetitious requests for information under the Act. Each witness voiced support for government transparency and the Act's purpose, namely to provide access to government information and actions by citizens. They all agreed that the Act's guaranteed access to public information promotes transparency and is essential to holding governmental bodies and public officials accountable to their citizens. Despite the Act's promotion of governmental transparency, abuses by requestors do occur. Sometimes those abuses are intentional and punitive toward governmental bodies. In such situations, there is no real recourse by governmental bodies. The Act provides no effective means of countering what the governmental bodies know to be requests motivated by animus and intended to result in anything from excessive time and costs to virtual government shutdown.

Sherry Cook, Texas Alcoholic Beverage Commission (TABC), related her agency's experience. In recent months, the number of requests received by TABC has more than doubled, causing tremendous strain on agency resources. At present, the agency's process for responding to requests typically involves multiple divisions. Requests are received by the Public Information Coordinator, who then determines which employees in each division possess documents related to the request. These employees are asked to search their physical and digital records for the requested documents.

In cases where an employee is unable to locate the requested documents, TABC's Information Resources Division (IRD) may be asked to assist. IRD can, in some cases, search archived digital data such as e-mails in order to retrieve the requested files. These searches can take considerable time. The breadth of some requests have meant multiple TABC employees have spent numerous work hours searching for thousands of pages of records included in a single request.

Certain requests received have sought the release of the personnel files of an entire TABC division, including personal cell phone bills and text message records. In the case of one request, special software had to be purchased to comb through the data; thousands of personal text messages unrelated to the request had to be individually redacted; thousands more related to the duties of undercover peace officers had to be further restricted for security purposes; and, documents containing years of cellular phone data had to be created and vetted by agency employees prior to release.

According to Cook, in many cases a single request resulted in thousands of pages of electronic documents. Since March 2015, 61 separate case folders for requests hold 208,779 files taking up an estimated 268 gigabytes of server space. To store this request information, IRD has purchased a 500 gigabyte hard drive, which is already more than half full.

Requests have also had a significant impact on staffing. Currently, a single IRD employee is responsible for assisting with requests, spending more than 80 percent of total work hours on open record request-related issues. The agency's legal division has been forced to adjust its staffing in order to respond to the increasing number of requests. In all, 11 legal division employees (out of a total of 18) have been tasked with responding to requests. For seven of those employees, 100 percent of their work hours are spent responding to open records requests.

Currently, the Act allows requestors to request thousands of pages of documents, and then merely inspect the whole of the documents while keeping only those they wish. Requesting to inspect documents (rather than requesting copies) exempts the requestor from paying reproduction costs for the documents requested, leaving taxpayers with the bill for not only for making copies, but also for the staff hours required to locate and reproduce the unneeded documents. Additionally, an agency employee must be physically present while the requestor inspects the documents, leading to further expenditure of agency resources.

Bruce Green, City Attorney for the City of Lufkin, testified on the need for a legislative response to significant requestor abuses that regularly occur under the Act. A cottage industry of "professional public watchdogs" that attend trainings, engage in endless "research" and even accept "clients" and act as consultants on utilizing the Act to strike against governmental entities has arisen. These watchdogs often request massive amounts of public information that require many hours of personnel time just to generate a cost estimate, which is not itself compensable under the Act. Requests such as all offense reports or all 911 calls by the police department [intended as a weekly request]; to inspect all city documents from the personnel files of City employees whose last name begins with 'A' [intended to be the first in the process of working through the alphabet]; and to review the complete personnel records of all active police officers for the city. The police personnel file request alone took over 200 hours of employee time and 2,000 pages of documents. The requestor did not appear to review the documents.

Additionally, computers are being programmed to generate requests. According to testimony, a computer was used by a requestor to generate 126,000 separate PDF requests, which were submitted at one time. Complying with the Act under these circumstances was an impossible task for a small city staff. Another time, enough computer generated requests were received by the city to shut down the city secretary's computer.

These requestors appear to know the Act well. Often they request an inspection of responsive documents but limit the scope of the request to five archive boxes, which is the Act's limit beyond which the cost of personnel labor may be charged. At other times, they have referred to themselves as members of the media, which allows them to take advantage of certain exceptions to the Act that prevent the governmental body from recovering any costs.

Ed Jones, Angelina County Attorney, gave several examples in which the Act was being used to interfere with official governmental duties. His office received 9,197 requests sent by a political opponent of a county officeholder on a single day while the requestor was running against the officeholder. The requestor followed up with 7,500 requests four days later.

He also received 924 requests referencing various state statutes and asking the governmental body to look up a specific statute and then determine if he had any records in which the statute was implicated. These requests for information were produced using a computer program in which one field was changed in each request. The result is that the public official would have to review each and every request, searching for the different item in each, which takes many hours. Some requests are overbroad or vague. Because these requests are unclear, it is not possible to determine what information is being requested or the amount of time required to prepare the request. For instance, one request states "I want all files in your office in paper form" or "I want to inspect all spreadsheets, all word processing documents, and all databases."

The County Attorney now spends about 30 hours a week responding to and assisting other county officials with responding to public information requests. Other county officials have spent many hours complying with and responding to public information requests, as well.

Wes Suiter, Angelina County Judge, acknowledged the importance of the Act, but also noted that the Act creates opportunities for individuals to intentionally use it to file a large number of requests for the purpose of abuse, harassment, or intimidation of public officials and/or their staff. To that point, requestors sometimes send antagonistic, belligerent and childish chides with their requests, revealing their true intent.

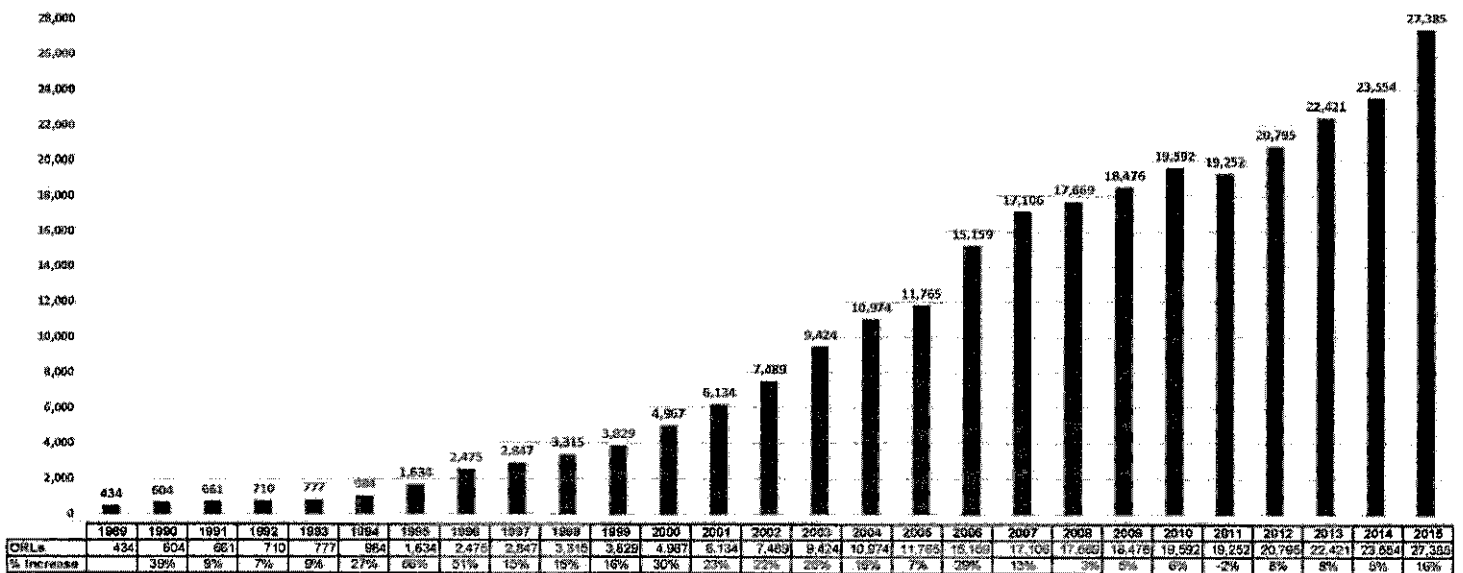
Among his examples of such abuse of the Act is a request for 44 years of records sent to a Justice of the Peace. The request was for all documents from January 1, 1970 to March 26, 2014. Another is a request to all elected or appointed officials or staff requesting to inspect screenshots of emails from and to every person you have either sent or received an email from. Persons include governmental entities or companies. This includes deleted emails, draft emails, and archived emails. The purpose for this request is to determine all the names of all the people, governmental entities, and companies that you have either sent or received emails from. Another request asked to inspect the criminal case records, both misdemeanor and felony, of all persons whose last name starts with "A" The complete register of actions for each case number only to be inspected. This will be followed by persons with a last name beginning with "B", then "C", etc.

Kelley Shannon, Executive Director, Freedom of Information Foundation of Texas testified regarding the Act's procedures for response to repetitious or redundant public information requests. In prepared remarks, she stated that it is important to note that the majority of information requesters are seeking a small amount of information on a limited, and possibly one-time, basis. She believes we must be diligent in protecting our longstanding law that protects these requesters and values an individual's right to information about his or her government. Some so-called "repeat" requesters may have a logical business reason or property ownership reason for making a recurring request for information. There are provisions in the existing Act to address many nuisance scenarios.

Ms. Shannon expressed her willingness to work with the legislature to try to address the abusive requests that were delineated by previous witnesses.

As an addendum to the hearing, the Committee received information on the workload of the Open Records Division of the Office of the Attorney General. The chart below illustrates the growth in the number of requests for calendar years 1989 through 2015.³ The chart makes clear that the number of requests for open records ruling is growing dramatically. The average annual percentage increase is more than 18 percent. By contrast, the average annual growth of the population of the state between 1990 and 2015 was less than two percent.⁴ This rapidly growing workload is creating challenges for the Open Records Division.

OPEN RECORDS RULINGS ISSUED
CALENDAR YEARS
1989-2015



3 Before 1989 the open records rulings were less common and were comingled with letter opinions.

4 January 1, 2015 population estimate: 27,213,214 (Source: Texas Demographic Center, May 2016)



RECOMMENDATIONS

Where feasible, revise allowable costs to encourage requests that are narrow and efficient and discourage requests that are wasteful, numerous, or overbroad.

Impose restrictions on the submission of clearly automated public information requests to prevent abuse. Incentivize use of standardized request forms and online request tools by governmental bodies.

Encourage the Open Records Division to issue more "broad scope" previous determinations to reduce the number of routine requests for open records decisions received by the Open Records Division, provided it can be done without negatively impacting requestors' access to public information.

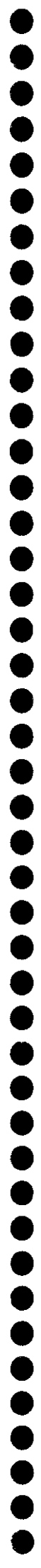
Ensure that governmental bodies make a reasonable effort to educate public officials on the requirements of the Public Information Act and a reasonable effort to recover responsive information.

Allow governmental bodies to petition a district court or other appropriate authority for injunctive relief in obvious cases of abuse, animus, or bad faith.



INTERIM CHARGE #4

Study the use of commercial cloud computing by state agencies and institutions of higher education, including efficiencies surrounding a utility-based model, security impacts of transitioning to cloud computing, and cost-savings achieved by the utilization of commercial cloud computing services.



BACKGROUND

Given the rapidly growing significance and maturity of cloud-based services, in 2012, the Department of Information Resources (DIR) determined it was necessary and timely to gain a deeper understanding of all facets of cloud-based offerings within the public-sector context. Cloud services are generally expected to offer reduced cost and increased efficiency for government organizations. However, at the time, the relative uncertainty of the contractual and operational components of cloud services had been a barrier to broad adoption in government. The following background was derived from the DIR study and testimony presented to the Committee.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources. It is a form of delivering information technology (IT) services via convenient, on-demand network access instead of through an organization's own technology infrastructure. Government organizations are using cloud computing solutions as a way to obtain IT capabilities that are flexible, have lower costs, and are quick to implement.

Cloud computing provides the same access to IT resources—such as email, databases, servers, storage, application software, development tools, and desktop services—as solutions that are procured and maintained on premises. In many cases, cloud computing reduces the need for organizations to incur capital expenses associated with procuring, implementing, and maintaining on-premises resources in exchange for services that are funded with operating expenses.

Cloud computing is enabled through virtualization of IT resources such as computing, storage, network, and software. Virtualization enables the creation of logically partitioned IT resources that share a set of physical resources. Virtualized resources become cloud resources when they can be defined and managed for specific organizations and made available with ongoing self-service ability to manage the virtual resources and leverage on-demand access (i.e., public or private Internet).

Cloud resources are also centralized, but shared by many groups and organizations to effectively increase use of the physical resources allocated, which can help to reduce overall costs. There are currently three different deployment models for cloud: public or hosted cloud, private cloud, and hybrid cloud.

- In a public cloud, the provider delivers common IT capability in a shared environment with great scalability. It is provisioned for open use by the general public. Demand from multiple customers with similar requirements are pooled together to optimize physical resources.

- In a private cloud, IT resources are dedicated and customized with the capabilities, resources, and administration required by a specific organization. Private clouds require a data center location, IT physical resources, virtualization, and operations team support. It is provisioned for exclusive use by a single organization that is made up of multiple consumers.

- In a hybrid cloud, the provider blends both private and public cloud features together, with preferences driven by a particular market niche or consumer group based on an application or system that has partial needs for highly secure or non-virtual resources.

There are three basic service models.

The Infrastructure as a Service (IaaS) model provides basic computing resources such as processing power, storage and network access. This approach works like a utility, where the client only pays for what is used.

The Platform as a Service (PaaS) model has the vendor provide not only hardware, but a software platform with tools the customer can use to develop solutions that are hosted by the cloud provider.

The Software as a Service (SaaS) model has the cloud vendor not only handle management of the hardware and background software tasks, but also provides specialized application software and databases.

Pilot Texas Cloud Offering

To develop a real and meaningful cloud experience, DIR pursued a pilot project aimed at institutionalizing the knowledge needed to successfully enable broad adoption. The Pilot Texas Cloud Offering (PTCO) project focused on the IaaS model, but many of the lessons learned can be generalized for government agencies adopting any cloud offering.

The PTCO allowed DIR and the pilot agencies to gain a greater understanding of cloud infrastructure offerings for state government and document options and issues with provider selection, pricing, access security, data security, credentialing, provisioning time frames, service levels, service remedy options, terms of use, billing models, interoperability, mobility, scalability, capacity management, provider compliance, monitoring, and licensing. Participating agencies used both large and small applications to investigate the appropriateness of cloud infrastructure hosting for the public sector.

PTCO demonstrated that, in general, the cloud environment should be considered for applications that:

- require rapid deployment,
- are approaching a technology refresh and/or the end of contractual obligations to a legacy environment,
- have variable storage needs,
- need bursting capability,
- use virtual servers rather than physical servers (the reliability, performance, or security of dedicated servers are considerably more expensive when procured through the cloud), or
- are based on federal funding with “cloud first” recommendations.

Additionally, the flexibility of cloud infrastructure offerings allows an organization to do the following:

- Stand up an application quickly. For example, the Secretary of State’s office was able to stand up www.votetexas.org, a mobile-enabled, interactive information website built to assist Texans with the complexities of redistricting and voter participation, within two weeks of beginning the sourcing and procurement effort. This was a mission-critical, highly visible, and advertised website that was urgently needed to support the 2012 Texas primary elections. It included a solution design, pricing, approval workflow, provisioning, and system monitoring of the site—all governed from a single web portal.
- Develop and test multiple applications in a flexible environment that cannot impact or be impacted by the production environment.
- Respond to recurring peak business demands with “bursting” rather than investing in bandwidth and infrastructure that is underutilized in non-peak periods.
- Host large, publicly accessible datasets separate from more sensitive information to free up capacity while strengthening and simplifying security requirements.

Security is an important element of cloud services, and the type of cloud solution chosen, whether public, private, or hybrid, impacts the security levels controlled by the customer. Just like most cybersecurity risks, many of the security risks associated with the use of cloud computing can be managed and prevented. It is incumbent on the agency using cloud services to be proactive in taking the necessary security precautions. Some ways to manage risks are to:

- Design for virtual private networks with private IP addresses, client-to-site and site-to-site VPNs, firewalls, and secure protocols,
- Monitor security controls,
- Tighten identity and access management,
- Virtualize anti-malware,
- Provide ongoing validation of security controls,
- Be aware of data state and location – know the location of data, processing, and backup,
- Update and maintain rules, regulations, and policies that impact cloud solutions, and
- Test applications for vulnerabilities and patch vulnerabilities if necessary

Since the DIR pilot project, cloud services have grown quickly. Government agencies, educational institutions, and non-profits are using the cloud in a variety of ways.

The Texas Department of State Health Services (DSHS) replaced traditional servers and an off-site backup service with an all-in-one Cloud Storage Services Platform. DSHS facilitated secure file synchronization and sharing that included was easy to use, always accessible, and enabled HIPAA and state regulatory compliance. As a result, DSHS reduced the total cost of ownership by 75 percent, saving millions of dollars, while facilitating greater productivity and security for agency employees and users.

The Human Genome Sequencing Center at Baylor College of Medicine used the cloud to analyze more than 14,000 human genomes. This project utilized more than 2.4 million core-hours of processing, involved nearly one petabyte of total storage, and generated 440 terabytes of data as research output.

The Texas Digital Library (TDL), a consortium of higher education institutions in Texas, uses the cloud to provide storage and access for the benefit of faculty, researchers, and students across Texas.

The Texas State Library and Archives Commission (TSLAC) uses the cloud as its foundation for the Texas Digital Archive, a searchable online repository. Among the first digital content to be safely stored in the archive will be the extensive records of the office of former Governor Rick Perry. The records include seven terabytes of data, 4,000 cubic feet of paper and an additional 26 terabytes of other electronic records. TSLAC chose a cloud-based solution to easily and securely provide access to archived records with minimal IT overhead.

The term “utility computing” or “public cloud computing” implies the ability of a customer to quickly acquire IT resources, use them, shut them down when not needed, and pay for only what it uses. One way to think about cloud computing is that instead of buying, owning, and maintaining their own data centers or servers, organizations can acquire technology resources such as compute power and storage on an as-needed basis, and dispose of it when it is no longer needed. Users only pay for what they use – by the compute-hour or storage-gigabyte – and they are not locked into long-term contracts.

The utility model allows for lower costs since customers do not need to procure and set up their own servers or data centers. Customers only pay for what they use, avoiding the challenges and costs of estimating server needs.

Utility computing is a service provisioning model in which a service provider makes computing resources, and management thereof, available to the customer as needed. This model charges customers for specific usage, in a metering model. The utility model seeks to maximize the efficient use of resources and/or minimize associated costs. This approach, sometimes known as pay-per-use service, is becoming increasingly common in enterprise computing. Another version of utility computing is carried out within an enterprise. In a shared pool utility model, an enterprise centralizes its computing resources to serve a larger number of users without unnecessary redundancy. This type of computing is ideally suited for private community clouds (DIR’s Data Center Services program).

With the utility-based model of cloud, if a program is funded one year and then unfunded the next, or a pilot project or test program does not achieve its expected results, Texas organizations no longer need to be tied to large capital IT outlays. If an IT project fails, agencies have more flexibility to adjust quickly and contain costs. Under the utility model, IT-based projects are far less likely to fail at all because utility computing allows for small-scale, inexpensive experiments followed by rapid adjustments in advance of any large investments, thus increasing knowledge via experimentation and decreasing the overall chance of failure. The result is achieving more return on one's investment and avoiding costly overruns and high profile failures.

According to some, advantages of the utility model include: IT users can trade capital expenditures for variable expenses - users can pay only for what they actually consume, and only when they consume it; variable expenses are lower with inherent economies of scale; users don't need to guess their capacity needs - before cloud, users risked the waste of buying too much IT capacity if demand were lower than guessed, or they risked dissatisfaction of their customers or citizens with shortages, if the users bought insufficient IT capacity to meet demand; the speed and agility of user innovation is dramatically increased with cloud - instead of waiting many weeks to obtain IT infrastructure, virtually unlimited capacity is available to users within minutes; cloud computing allows a user's scarce technical talent to focus on its core mission, not on maintaining basic compute and storage infrastructure to support it. With the budget challenges that agencies face today, that focus is valuable now more than ever to government users.

In 2015, DIR published their 2016-2020 Strategic Plan for Information Resources. In the plan, DIR noted barriers to cloud adoption among Texas state agencies similar to what has been observed and what the federal government has experienced. These barriers include concerns regarding security, legacy systems, procurement, and lack of industry standardization. These obstacles keep agencies from advancing cloud implementation beyond basic applications to a more holistic, streamlined, and interoperable IT infrastructure.

Cloud computing security has been a top priority for many providers and customers in recent years. The Central Intelligence Agency (CIA), U.S. Department of Defense (DOD), NASA, U.S. Health & Human Services, and the Federal Aviation Administration (FAA), among others, use Cloud computing. The committee received testimony that the cloud offers many security benefits over traditional IT infrastructure including the integration of compliance and security and the professional execution of a major portion of the security area with a focus and skill far beyond that of most customers.

HEARING

On April 5, 2016, the House Committee on Government Transparency & Operation met in a public hearing in Austin, Texas, to consider the following charge:

Study the use of commercial cloud computing by state agencies and institutions of higher education, including efficiencies surrounding a utility-based model, security impacts of transitioning to cloud computing, and cost-savings achieved by the utilization of commercial cloud computing services.

The committee heard testimony from the following:

Cam Beasley, UT-Austin;
Gerry Caffey, Legislative Budget Board;
Buddy Garcia, NEC Corporation of America;
Dale Richardson, Texas Department of Information Resources;
Mark Ryland, Amazon Web Services; and
Jennifer Saha, Computing Technology Industry Association.

The committee heard from a panel of private sector professionals first. Buddy Garcia gave an overview of cloud services available. He stressed that governmental agencies continually seek innovative ways to operate with limited resources and that technology is always changing. Because of this, companies and agencies are utilizing software to reduce the cost of replacing expensive, proprietary hardware when it becomes obsolete. There is also a transition to “standards based” software to reduce costs and to keep from being locked into a particular manufacturer’s line of products.

Agencies now have the ability to deliver applications to users and devices over the network in a way unlike any before. Using Hosted Cloud services reduces the need to replace equipment, update software and have onsite resources to manage the services. However, there is a loss of control, an added security risk due to additional connection to outside networks, and the fact that service fees never stop. With a Hybrid Cloud, there is an added element of control. The Hybrid Cloud model also adds a level of business continuity in the event of being cut off from the provider. Private Clouds offer the lowest return on investment, given the infrastructure is already in place. On the other hand, it can be the most secure, as outside connectivity is limited, and it provides the greatest amount of control.

Mark Ryland commented that many government agencies have taken advantage of the flexible, secure, powerful, and highly efficient way of accessing IT resources through cloud services. Before cloud computing services were readily available, organizations only had an option of either making massive capital investments to build their own datacenter or server infrastructure, or of entering into long-term contracts with a vendor for a fixed amount of datacenter capacity that they might or might not use. This choice meant either paying for wasted capacity or worrying about shortages, i.e., that the capacity they deployed was insufficient to meet their peak demands.

Cloud computing provides government with new ways to obtain IT and to deploy applications. This new model has changed the way government agencies do business through technology that provides lower costs, world-class security, and agility.

According to Ryland, the initial concerns regarding security in the use of cloud services have turned completely to a growing realization that the cloud offers many security benefits over traditional IT infrastructure. The cloud, and its accompanying automation and agility, provides the opportunity to enhance systems security, not just achieve improvements in system delivery and reductions in cost. He believes that the evidence holds that security should no longer be seen as a barrier to cloud adoption, but an argument in favor of it.

Jennifer Saha echoed the fact that cloud computing and deployments in government are becoming more prominent because of its platforms' flexibility, efficiency, dynamic and secure environments. It is important to note, according to Saha, that cloud computing adoption by government agencies takes other forms than just 'commercial' adoption, implying cloud computing is only available from a third party, or commercial vendors. Government organizations use both third party and internal cloud tools and capabilities. Some run their own cloud, some manage them internally and some have vendors operate the solution. There are a lot of different options and configurations in the public sector cloud space.

A handful of states, Texas among them, as well as the federal government, have adopted "Cloud First" policies that require agencies to examine cloud for existing and new applications. A best practice that Saha's organization has observed is that Cloud First initiatives must have solid policies behind them, including efficient contracting mechanisms, in order to be productive and not punitive. This includes records retention, security, service models and contracting terms. Governance and authority are important and tends to be more successful in centralized IT states or those that focus on governance.

Specifically related to security, the federal government's Federal Risk and Authorization Management Program (FedRAMP) has established a government-wide standardization related to security requirements for cloud systems. Another standard that many government clouds monitor and aspire to is the FBI's Criminal Justice Information Services (CJIS) standard as well as the Federal Information Security Management Act. Related specifically to cyber security, governments are adopting the National Institute for Standards and Technology's cyber security framework and using the Multi-State Information Sharing & Analysis Center (MS-ISAC) to help mitigate risk.

Saha noted one careful consideration as states adopt cloud solutions is the procurement mechanisms used. Terms and conditions designed for traditional hardware or software contracts need to be drastically modified for cloud. The most successful modifications start from scratch instead of simply modifying existing terms and conditions. National Association of State Chief Information Officers (NASCIO), in conjunction with governments and industry, have also developed terms and conditions that are being leveraged by governments as they seek to establish quality contract vehicles for procuring cloud services.

The committee also heard from Cam Beasley, Chief Information Security Officer (CISO) for the University of Texas at Austin and its System. Beasley focused on the security impact of transitioning to cloud services. UT has experienced many benefits from cloud services, but being a CISO, his focus is on security issues. After transitioning a number of different services to the cloud, it has gone well overall for UT.

Contracts are of the utmost importance. Security evaluations and terms and conditions must be included in a well-written contract for cloud services. In hosted applications specifically, such as web-based applications, providers will state that their systems are secure, but sometimes they are not. Oftentimes, it is simply because these applications are not primarily focused on security. Therefore, UT performs security evaluations. When they have found flaws, the hosted applications have addressed them quickly thereby, improving their service. On average, UT performs about 20 evaluations per month.

Other important contract provisions, which must be scrutinized, include who has access to data: contractors, subcontractors, or foreign nationals; whether those with access have undergone background checks; whether the system is housed on United States soil and if the agency is able to retrieve all the data. A third party cannot evaluate these specifics. Thus, it is important that agencies conduct these reviews.

In using the private cloud, UT has virtualized a lot of infrastructure into common data centers on campus. The university has realized tremendous savings in dollars, time, energy, and square footage usage from this virtualization. At the same time, there has been an increase in security.

The elasticity of cloud services is a tremendous benefit, specifically for certain cyclical demands, such as student registration and research. The cloud's resiliency and on-demand usage capabilities are remarkable.

Dale Richardson briefed the committee on commercial cloud computing use by the State of Texas. He included the following information on cooperative contracts, data center services, security, utility-based models and cost savings achieved.

Texas leads state governments in supplying both commercial cloud computing contracting vehicles and private community cloud services. In DIR's Cooperative Contracts program, there are 22 active Cloud Master Contracts. Total utilization from initial awards in 2013 for these master contracts is about \$3.4 million. The utilization has increased year after year as more entities become comfortable adopting cloud services.

Through DIR's Cooperative Contracts program, all qualified government entities (state agencies, institutions of higher education, K-12 ISDs and local governments) can purchase public cloud services. These master contracts have pre-negotiated terms and conditions that meet all state mandated procurement laws and have specific protections incorporated for cloud services.

In DIR's Data Center Services program, a private community cloud was put into place serving 28 state agencies in 2012. The Data Center Services (DCS) program currently offers private community cloud services and hybrid public cloud services. DCS services are delivered via a

private community cloud for all 28 designated state agencies in the program for IT infrastructure. In 2015, DCS implemented hybrid cloud services with two major public cloud providers, Amazon Web Services (AWS) and Microsoft's Azure. These offerings are limited to certain use cases, data types and security standards to protect the integrity of the state's data.

Richardson stated that state agencies' use of DIR's cooperative cloud contracts has been limited. Agencies are reluctant to use the cloud contracts, citing security concerns and lack of knowledge on how to operate cloud workloads. Institutions of higher education are steadily increasing the use of cloud master contracts. For example, the University of Texas is a major consumer of DIR's cooperative cloud contracts for local and satellite campuses.

Information Security of any type is focused on balancing business needs with risks. Information Security professionals focus on the risks to Confidentiality, Integrity, and Availability (known as the CIA Triad) of data and information systems.

Compliance with legal and regulatory frameworks in the cloud relies heavily upon a shared responsibility model. This model is similar to what is required of a hosted system where various controls are inherited from the service provider and the customer is left to address all the remaining controls.

Some cloud providers offer secure "Gov Cloud" offerings that provide compliance with stringent federal controls. While it might be cost prohibitive or nonsensical for a small organization to achieve all the required controls on their own, a Gov Cloud offering may provide the necessary protection.

Compliance can be achieved following a model of shared responsibility and inherited controls. Enforcing the shared model typically comes down to contractual terms.

Utility computing is a service provisioning model in which a service provider makes computing resources, and management thereof, available to the customer as needed. This model charges customers for specific usage in a metering model. The utility model seeks to maximize the efficient use of resources and/or minimize associated costs. This approach, sometimes known as pay-per-use service is becoming increasingly common in enterprise computing. Another version of utility computing is carried out within an enterprise. In a shared pool utility model, an enterprise centralizes its computing resources to serve a larger number of users without unnecessary redundancy. This type of computing is ideally suited for private community clouds (DIR's Data Center Services program).

Few technologies have affected the IT industry as profoundly as cloud computing. Part of cloud's appeal is clearly financial; it allows organizations to shed expensive IT infrastructure and shift computing costs. The State of Arizona recently decided to begin migrating its IT infrastructure to the cloud after recognizing that more than half of its servers were aging and needed to be replaced. The state now saves 75% in annual operating costs on its DNS solution when compared to its previous on-premises IT infrastructure.

A recent article by The Pew Charitable Trusts cited a survey, conducted by the National Association of State Auditors, Comptrollers and Treasurers (NASACT) and consulting firm Deloitte, lauding the Texas Comptrollers' Office for utilizing a cloud-based purchasing system to improve service and save more than \$8 million annually.

In addition to reducing up-front investment costs, cloud adoption can also reduce operational costs. By being able to rapidly scale to meet existing demands and future budget changes, funding is only needed to pay for what an agency consumes rather than having to pay to maintain excess capacity. An agency's IT footprint can be reduced through consumption-based buying—not only reducing hardware and software costs, but also providing significant labor savings and the ability to re-purpose government personnel for mission critical tasks.

Not all IT requirements though are suited for commercial cloud services. There are a lot of existing legacy applications that are not programmed to run in cloud environments. Commercial clouds do not always equal savings when factoring in additional costs to operate in the cloud. For example, one of the biggest additional expenses will involve acquiring new high-speed internet network connections. Total cost savings depends on each individual application.

Gerry Caffey, from the Legislative Budget Board (LBB), gave an overview of current and potential uses of cloud computing by Texas state agencies and institutions of higher education. Included in the presentation was identifying efficiencies and cost savings along with potential problematic issues related to security or management of the cloud. In brief, cloud computing consists of different types of service models, each with their own benefits and risks; state agencies are already using cloud computing for many tasks and that use is growing; and, the use of cloud computing by state agencies will continue to grow, but as with most issues in information technology, judgment must be applied. Agencies must understand both the benefits and the challenges of using cloud computing so that costs and risks can be minimized as they implement these still emerging technologies.

According to Caffey, over 74 percent of state agencies are using cloud services. The benefits of cloud computing include scalability and elasticity - instead of a large project beginning with the purchasing and configuring of hardware, resources can be made available in dramatically shorter time-frames; device and location independence - employees can access data and systems using a web browser using any kind of device at any location that has access to the internet, including tablets, laptops, and smart phones; and costs - some of the larger cloud infrastructure providers have tens of thousands of servers and commensurate economies of scale.

The Quality Assurance Team has observed that generally agencies have fewer cost and time overruns when purchasing third-party applications than developing custom applications. Software as a service is a type of third-party application which may be cheaper because the costs of development of the application are being shared among multiple customers.

Considerations of using cloud services include security concerns. The level of security varies enormously among different cloud providers. Records that include either health or criminal justice related information may be required to be stored using special care. As stated by DIR, specific contract requirements must be delineated. Not all cloud providers are compliant with

those special requirements. Microsoft and Amazon are examples of cloud vendors that adhere to the Criminal Justice Information Security requirements as defined by the Federal Bureau of Investigation.



RECOMMENDATIONS

Establish a strong "Cloud First" policy for the State of Texas

Currently, state agencies may consider cloud computing service options for a major information resources project. To fully leverage the potential savings of cloud services, Texas should require agencies to evaluate and consider commercial cloud computing services before making any new information technology or telecommunications investment.

Rather than spending money to maintain old technologies or the limited systems of the past, state agencies need clear direction from the legislature to focus their efforts on obtaining new technologies like cloud so that they can enjoy the speed, security and agility of startups and businesses.

Texas should remove restrictions from and open the data center to allow a new level of potential cost savings in agency budgets.

Although Texas has the infrastructure in place for Cloud networking and is already leveraging some private Cloud services, there are some restrictions that prevent the state from taking full advantage of that infrastructure. As an example, there are restrictions on the data center that prevent delivering voice services to state agencies. The same is true for the provision of cloud services through the data center. By making such changes, this would provide an excellent platform for Hybrid cloud, in the future, or moving directly to the cloud.

With the available technology, it is no longer necessary for the state to be locked into propriety based hardware solutions. With the excellent job the DIR has done implementing the data center, it is a perfect time to open the door and start leveraging these technologies.

Require Agencies to Assess their Total Cost of IT

To help properly assess IT costs and cloud savings, Texas state agencies should be required to account for the Total Cost of Ownership (TCO) of their IT systems, including Legacy Systems. The Technology committee attempted to learn state agency IT costs in 2013, to no avail. To improve state budgeting efforts, agencies should be required to assess their total IT costs.

Require Agencies to adopt use of Agile project management for IT software development projects

Private companies have broadly adopted use of the Agile Project Management with proven results indicating increased effectiveness for IT projects. Agile is an alternative to traditional waterfall or sequential software development and differs in that it allows project teams to respond to unpredictability through incremental, iterative work cadences and empirical feedback. Agile development methodology provides opportunities to assess the direction of a project throughout the development lifecycle. This is achieved through regular cadences of work, known as sprints or iterations, at the end of which teams must present a potentially shippable product increment. By focusing on the repetition of abbreviated work cycles as well as the functional product they yield, agile methodology is described as "iterative" and "incremental."



INTERIM CHARGE #5

Review the process of dissemination by public entities of criminal records containing incomplete or inaccurate information, assess options for the subjects of such records to correct the misinformation specifically as it interferes with their ability to obtain employment, and determine the need for greater regulations over this process. (Joint charge with the House Committee on Homeland Security & Public Safety)



BACKGROUND

Background checks, including criminal history records, have been used for some time by parties such as employers, volunteer organizers, banks, credit lenders, landlords and journalists for legitimate business and reporting purposes. More than two thirds of employers run criminal background checks on all of their potential employees as a contingency of employment according to a 2012 survey by the Society of Human Resource Management. The right to access these public records is protected under the Public Information Act, and this information plays an important role in social and economic commerce and public integrity.

There is now an ever widening expanse of public criminal record information including booking photos (or mug shots) being obtained for purposes of sensationalism and profit. Certain websites and publications have developed a business model around the bulk purchase of criminal history information. Income is generated from the further sale or distribution of those records, or by charging a fee to remove or modify false or misleading information from the website. In some cases even reputable news sources may be uploading bulk data simply to drive website traffic and garner advertising revenue.

Many states are turning to legislative measures to restore balance between an individual's right to privacy and fair trial, and the public's right to obtain information. A criminal background can create barriers to accessing employment, housing, education, and government benefits. Anecdotally, individuals trying to move beyond their past mistakes, even those who have had their records expunged or sealed by an order of non-disclosure, have experienced difficulty finding housing, employment or educational opportunities when evidence of previous criminal association is uncovered online. Once erroneous or incomplete criminal history information enters the public domain it can be nearly impossible to rescind.

Public Information Act

The Public Information Act, Texas Government Code Chapter 552, gives the public the right to access government records without being asked for what purpose they are being requested.

The Texas Public Information Act applies to all governmental bodies, including all boards, commissions, and committees created by the executive or legislative branch. It also may apply to a body that is supported by public funds or that spends public funds. Although certain exceptions may apply to the disclosure of the information all government information is presumed to be available to the public. Information collected and maintained by the judiciary is not covered by the Texas Public Information Act. That information is governed by public access rules set by the Supreme Court of Texas and other applicable rules and laws.

The Act defines 'public information' as information that is written, produced, collected, assembled, or maintained under a law or ordinance or in connection with the transaction of official business by or for a governmental body. This definition applies to information recorded in a variety of media and formats including any electronic communications. There is no set form to request public information, but the request must be submitted in writing to trigger obligations set forth in the Public Information Act.

Recent Legislation in Texas and Other States

Georgia, Illinois, Oregon and Utah enacted legislation in 2013 to prohibit commercial sites from charging fees for removing mug shots upon request or by prohibiting sheriffs from releasing mug shots to sites that charge a fee, among other provisions. Similar legislation was enacted in California, Colorado, Georgia, Missouri and Wyoming in 2014; in Maryland and Virginia in 2015; and in Florida and South Carolina so far in 2016.

In Texas, SB 1289, passed by the 83rd Legislature, aimed to ensure that all public criminal record information that is reposted by a business entity is correct and fair. The bill amended the Business and Commerce Code to require that criminal record information published by certain business entities must be complete and accurate. The bill established a process by which a person who is the subject of the criminal history information may dispute the completeness or accuracy of the information. SB 1289 required an individual disputing criminal record information published by a business entity to provide the business entity with a noncertified copy of a court order or other document that supports the individual's dispute. If the business finds that the published information is inaccurate or incomplete, it shall promptly remove the inaccurate information. The bill established a civil penalty of not more than \$500 for each violation in cases where a business entity publishes criminal record information it knows to be incomplete or inaccurate. It should be noted however that §109.002 of the Texas Business and Commerce Code exempts all of the following from SB 1289 and other provisions of the Chapter:

- A publication of general circulation or an Internet website related to such a publication that contains news or other information, including a magazine, periodical newsletter, newspaper, pamphlet, or report;

- A radio or television station that holds a license issued by the Federal Communications Commission;

- An entity that provides an information service or that is an interactive computer service;

or

- A telecommunications provider.

Recently many states have passed or considered legislation related to curbing the distribution of erroneous criminal history data including:

Alabama

H.B. 8

Status: Failed-Adjourned.

Requires websites containing personal information of persons charged with crimes to remove information at no charge upon request; provides civil penalties; provides presumption of defamation.

Florida

H.B. 293

Status: March 24, 2016; Filed as Chapter No. 2016-78

Provides that juvenile justice confidential information, including arrest records, is exempt from public records requirements; authorizes custodians to choose not to electronically publish juvenile arrest and booking photographs; provides an exception for intrastate criminal information; relates to employee background screenings, investigations, notifications, court records and fingerprinting.

S.B. 1072

Status: March 11, 2016; In Senate. Died in committee.

Relates to arrest booking photographs; prohibits a person who publishes or disseminates an arrest booking photograph through a certain medium from soliciting or accepting payment of a fee or other consideration to remove, correct, or modify such photograph; authorizes an action to enjoin publication or dissemination of an arrest booking photograph for a violation of the act; specifies the time limit for the removal of an arrest booking photograph pursuant to a court order.

Hawaii

H.B. 529

Status: March 10, 2016; Failed First Crossover Deadline - Second Year of Biennium.

For criminal cases resulting in no conviction: 1) prohibits commercial websites from collecting a fee for removing arrest booking photographs from the website; 2) prohibits criminal justice agencies from posting arrest booking photographs on a website except as provided by law.

Kentucky

H.B. 132

Status: Signed by the Governor

Prohibits for commercial purposes the use of booking photographs and photographic records generated by law enforcement for identification purposes and taken of an inmate under certain conditions; allows for a right of action for certain persons requesting the removal of a photograph taken; provides for civil penalties; defines related terms; provides for service credits and sentence reductions to county jail inmates for receiving a general equivalency or high school diploma, and for good behavior.

Oregon

Status: Passed. Filed as Chapter 330

H.B. 3467, Requires persons that operate websites that disseminate photographic records of arrested individuals and charge fees for removal of these records to remove photographs and related information from all websites within their ownership or control without charging fee when requested in writing and arrest resulted in acquittal or violation, or following expunction.

South Carolina

Status: Effective. Act No. 132

S.B. 255, Relates to the destruction of arrest and booking records; provides that an entity who publishes on a website the arrest and booking records of a person whose charges have been discharged or dismissed, or of a person who is found not guilty of a charge, shall, without fee or

compensation, remove the arrest and booking records within specified days of a written request; includes administrative hearings; provides penalties for failure to remove such records; provides for correction of crime database records.

Utah

Status: Passed. Filed as Chapter 404

H.B. 408, Enacts a provision relating to photographs of criminal suspects; prohibits county sheriffs from providing a copy of a booking photograph to a person if the photograph will be placed in a publication or posted on a website that requires a payment in order to remove the photograph; requires a person requesting a copy of a booking photograph to sign a statement that the photograph will not be placed in a publication or on a website that requires payment in order to remove the photograph; relates to penalties.

Virginia

Status: Signed by Governor. Chapter 414

S.B. 720, Relates to dissemination of criminal history record information and civil actions; provides that any person who disseminates, publishes, or maintain or causes the same of the criminal history record information of an individual pertaining to that individual's charge or arrest for a criminal offense that solicits, requests, or accepts money or other thing of value for removing such information shall be liable to the individual who is subject to the information for actual damages or a specified amount.

Wisconsin

Status: Failed to pass.

A.B. 258, Relates to removal of certain criminal record information from Internet sites without a fee; provides a criminal penalty.

Some legislation, in line with those who note that access to mug shots and other criminal background information is an important part of journalistic coverage, freedom of speech and the public's right to know, has come at the issue from a different angle:

District of Columbia

Status: Failed to pass

B. 73, Requires the Metropolitan Police Department to release photographs of arrested individuals to the public.

Louisiana

Status: Failed

2012 S.B. 452, Provides that the booking photograph of any person arrested for an alleged offense held by law enforcement agencies and communication districts will be disclosed upon request.

New Jersey

Status: Failed

A.B. 2177, This bill would clarify that the booking photographs taken of a defendant after an arrest, commonly referred to as mug shots, are to be available to the public under the state's open

public records law. Current law does not specifically address the availability of mug shots to the public. Instead, decisions on whether to release mug shots are left to the discretion of investigative agencies, allowing inconsistent policies on the release of these records to be applied throughout the state. This bill would provide a uniform policy that all mug shots are to be made available to the public.

South Dakota

Status: Failed

H.B. 1109, Provides that criminal booking photos and police logs are open records.

Washington

Status: Failed

H.B. 1689, Requires department of corrections officers and chief law enforcement officers to maintain a jail register that is open to the public and includes booking photographs of each person after charges have been filed.

HEARING

On May 25, 2016 the Committee met jointly with the House Committee on Homeland Security & Public Safety to hear testimony on the following charge:

Review the process of dissemination by public entities of criminal records containing incomplete or inaccurate information, assess options for the subjects of such records to correct the misinformation specifically as it interferes with their ability to obtain employment, and determine the need for greater regulations over this process. (Joint charge with the House Committee on Homeland Security & Public Safety)

The Committee heard testimony from the following:

Joe Ellis for Freedom of Information Foundation of Texas;
Eric Ellman for Consumer Data Industry Association;
John Fleming for Texas Mortgage Bankers Association;
David Foy for LexisNexis;
Skylor Hearn for Texas Department of Public Safety;
David Mintz for Texas Apartment Association;
Kathy Mitchell for Texas Criminal Justice Coalition;
Stephanie Morgan for General Information Services;
Dianna Muldrow for Texas Public Policy Foundation;
Galen Svanas for National Association of Professional Background Screeners; and
Caroline Woodburn for County and District Clerks' Association of Texas.

During the 71st Regular Session, the Texas Legislature enacted House Bill 2335 and Senate Bill 41 establishing Chapter 60 of the Texas Code of Criminal Procedure and therein the Criminal Justice Information System (CJIS). The CJIS must capture, for each arrest for a felony or a Class B or higher misdemeanor, information relating to:

- offenders
- arrests
- prosecutions
- the disposition of cases by courts
- sentencing; and
- the handling of offenders received by a correctional agency, facility, or other institution.

This information is collected in two databases maintained by two agencies. The Texas Department of Criminal Justice (TDCJ) oversees the Corrections Tracking System, which it uses to manage information on offenders who are currently sentenced to prison, jail, parole, and probation. Independently, the Department of Public Safety (DPS) manages the Computerized Criminal History (CCH) System, the statewide repository for criminal history data and the system which is used to provide criminal background check services. (Appendix from SAO Report)

The CCH collects arrest information submitted by law enforcement entities; records submitted by district and county attorney's offices; and records submitted by county, district, and other courts - including conviction decisions and sentencing information. By law, arresting agencies must provide arrest information to the DPS within 7 days. Within 30 days of when they become available, prosecuting offices are required to report their decisions regarding acceptance or rejection of charges in the CCH, and court clerks are required to report into the CCH the disposition of charges decided in their courts.

DPS is tasked with monitoring the submission of arrest and disposition information by local jurisdictions and is required to annually submit to the Legislative Budget Board, the governor, the lieutenant governor, the state auditor, and the standing committees in the senate and house of representatives that have primary jurisdiction over criminal justice and the Department of Public Safety a report regarding the level of reporting by local jurisdictions in order to identify local jurisdictions that do not report arrest or disposition information or that partially report information. The fourteenth and most recent 'Report Examining Reporting Compliance to the Texas Computerized Criminal History System' published January 2016, can be found on the DPS website.

A September 2011 report by the State Auditor's Office (SAO) determined that the quality of information that DPS uses to conduct criminal history background checks was impaired by the significant number of prosecutor and court records that were not reported to DPS. As of January 2011, prosecutor offices and courts had submitted disposition records to the CCH System for 73.68 percent of arrests made in 2009. In May 2016 the SAO reported that the completeness and timeliness of the CCH System data had improved, reaching an 80.21 percent completion rate for arrests reported in 2013. In their reporting DPS found the statewide disposition reporting completeness rate for 2014 adult arrests was 78 percent and 89 percent for juvenile arrests. One factor that may impact the completeness of certain records is the length of time it may take to reach a final disposition in a contested case, but these numbers illustrate that 1 in 5 arrest records maintained by DPS have not been updated with a final disposition and remain incomplete. DPS has no means for enforcing when local agencies update those records in the database, but some departmental grants are contingent on keeping the number of complete records in CCH at or above a certain threshold.

Access and Sale of Criminal Records

Texas Government Code, Chapter 411 outlines who and for what purpose a person or organization may be granted access to criminal history record information. Any member of the public is entitled to obtain from DPS criminal history record information maintained by the department that relates to the conviction of or a grant of deferred adjudication to a person for any criminal offense. A person who obtains information from the department may use the information for any purpose and may release the information to any other person.

DPS makes this information available to individuals, for a fee, via the Conviction Database. The Conviction Database is public record information extracted from the DPS Computerized Criminal History System (CCH). The information contained in CCH is only public if a conviction or deferred adjudication has been reported to the Department on an offense.

DPS also provides publicly available data in the CCH system to private companies in the form of bulk sales. A list of bulk sales customers is maintained online along with the date of their last purchase. DPS communicates to these customers on a regular basis when existing records become subject to orders of nondisclosure or are expunged, and customers are required to redact those records within 30 days. DPS has had good responsiveness with its customers in compliance with such orders.

Criminal history information can also be obtained directly from local government sources such as county and district clerks, clerks in justice or municipal courts, and law enforcement agencies. Users suggest that the most accurate and up to date arrest, booking, and criminal information can be obtained from these local sources since it can be obtained with a written public information request, without much delay, and at any point in the criminal justice process. Government subdivisions rarely maintain copies of the records that are released, nor do they register who requested or received those records. The result is that once the information has been released there is no means for correcting misinformation, updating disposition information on each file, or redacting a file if a case is expunged or a person is issued an order of non-disclosure.

Neither DPS nor local governmental subdivisions are able to trace or update information passed or sold to a third party.

RECOMMENDATIONS

Amend the Business and Commerce Code to prohibit business entities from charging consumers for having their mug shots removed from an offending website if the information is inaccurate, misleading, or has been ordered expunged or sealed by an order of nondisclosure.

The websites can be a source of misleading or inaccurate information. Oftentimes these businesses exploit people who have been acquitted or against whom charges were never filed. Persons who have had an encounter with the criminal justice system may seek to have inaccurate or misleading information removed from these websites only to be met with a demand to pay an administrative fee to have their arrest photo or information removed from the website. Current state guidelines cap these fees but, if the information is displayed on more than one website, the cost multiplies, which the parties claim has essentially created a for-profit industry based solely on the exploitation of others.

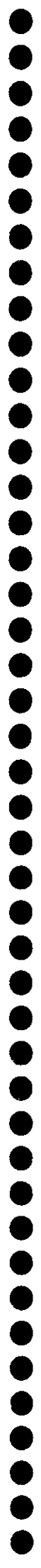
Prohibit the bulk sale of mug shots until time of arraignment.

Bulk criminal records are sold for legitimate reasons such as background checks for new employees, loans or apartment rentals. However, a person who is completely innocent could be arrested for simply being in the wrong place at the wrong time, and never have charges brought against them. Unfortunately, their mug shot could be on websites in perpetuity simply for being falsely arrested. By prohibiting the bulk sale of mug shots until arraignment, those who are never charged with a crime would not have their mug shot widely dispersed on the internet, but individual mug shots could be released in separate requests.



INTERIM CHARGE #6

Study the impact of emerging technologies used by law enforcement and issues related to appropriate dissemination of the data provided by those technologies, including the impact of technologies on the operation of law enforcement agencies, the operation of the Public Information Act, and any appropriate safeguards for citizens and law enforcement officers who interact with those technologies or whose data is recorded. (Joint charge with the House Select Committee on Emerging Issues in Texas Law Enforcement)



BACKGROUND

Law enforcement has been in the spotlight in recent years. Officers performing their duties have been called into question regarding the appropriateness of their actions. Citizens have made an outcry for transparency and access to information. As a result, new technologies and programs have been developed to create more efficiency and transparency.

The Public Information Act guarantees a citizen's right to obtain public information in a timely manner. Gaining information in circumstances involving law enforcement or investigations have specific parameters that may result in the delay of the information's release. Information used in an investigation as well as privacy rights may result in redactions. There are provisions in law that take the circumstances of the information into account. As an example, prohibiting the immediate release of information may be due to maintaining the integrity of an investigation or future adjudication. Each request for public information has to be reviewed individually as to the legal circumstances regarding the ability to release the information requested.

Technology in the law enforcement arena is a growing market. New technologies are constantly being developed, however, a department's ability to utilize the equipment or software is oftentimes driven by cost and funding. The demand for certain equipment has resulted in many companies developing programs. Multiple companies entering that market creates competition and helps drive the costs down for law enforcement.

Technologies being used across Texas varies. During the 84th Legislative Session, Senate Bill 158 was passed and became effective September 1, 2015. This bill established basic policy for the use of body worn cameras in Texas and provided a state-funded grant program to assist in the costs of these programs.

HEARING

The House Committee on Government Transparency and Operation and the House Select Committee on Emerging Issues in Texas Law Enforcement met in a joint hearing on May 24, 2016, and heard testimony from the following witnesses:

Barbara Armstrong, (Harris County Sheriff's Office)
David Cook, (Fort Worth Police Officers Association, CLEAT)
Dean Gilliam, (Fort Worth Police Officers Association, CLEAT)
Greg Glod, (Texas Public Policy Foundation)
Justin Gordon, (Office of the Attorney General)
Skylor Hearn, (Texas Department of Public Safety)
Craig Kelso, (Texas State Library and Archives Commission)
Kathy Mitchell, (EFF-Austin)
Elizabeth Morris, (Texas A&M Engineering Extension Service)
Matt Simpson, (ACLU of Texas)
Ryan Sullivan, (Harris County Sheriff's Office)

PRIVACY

Technology in law enforcement includes everything from the advanced design of brakes on vehicles, red light cameras, toll road cameras, video usage, advanced communication abilities, computer forensics, to surveillance technology. Advancements are far-reaching and all encompassing. The public is sensitive to their privacy regarding law enforcement, but their right to privacy from the general public does not gain the same attention. Criminals and every day citizens have direct access and ability to utilize the expanding technology capabilities. The difference is that law enforcement must have cause and gain a search warrant, whereas the citizen can download an app or software at will. Privacy for today's public is relative.

Parameters are placed around what and how law enforcement uses technology tools. Not necessarily legal, but the general public operates at will using many of the same technologies. An average citizen is subject to a criminal gaining their banking information through card reading devices, hotel keys, smartphones or computer use. Tracking technology through apps and software can be installed on a person's device through email or text. No permission on the receiving end is necessary. Private email accounts can be hacked in various ways without the user's knowledge. Law enforcement must operate under very specific standards and laws, however, a citizen is vulnerable to an invasion of privacy from the general public at will. It has been said every person should operate under the assumption that all of their private information has been compromised; be alert and engage defensive measures. As an example, Radio-

frequency identification (RFID) technology has been added to wallets and credit card sleeves to protect the user's information from being secretly downloaded by a criminal. Law enforcement operates under the assumption the technology they use can be duplicated in the private sector making firewalls and technology security a paramount concern.

With the public expansion of law enforcement technology gaining attention, privacy among some has become a concern. The public is entitled to information held by a public entity; however, there are exceptions. The *Texas Government Code* excludes from disclosure information that relates to internal law enforcement records, the release of which would interfere with law enforcement or prosecution. Additionally, the law includes provisions that make confidential information related to homeland security, such as information collected for the purpose of preventing, detecting, or investigating an act of terrorism, as well as information related to security systems and critical infrastructure. *Texas Government Code Section 552.108* states that information held by a law enforcement agency or prosecutor that deals with the detection, investigation, or prosecution of crime is excepted from required public disclosure. It further excepts from disclosure information concerning an investigation that concluded in a result other than conviction or deferred adjudication. The Attorney General, in a memorandum opinion of June 8, 2015, stated that in accordance with *Section 552.108(a)(2)* a city may withhold ALPR information. Additionally, *Section 552.130* provides a governmental body to withhold motor vehicle information such as the driver's license number, vehicle identification number, the type/class of license, copy of the license and license plate number. Further, in Opinion No. KP-0076, the Attorney General opined that "*a court is likely to conclude that counties are not authorized to utilize an automated photographic or similar system to enforce the financial responsibility laws in chapter 601 of the Transportation Code.*"

There are other exceptions that generally focus on the impact upon a governmental body's interests or third party proprietary interests, if the information is released. The Office of the Attorney General has determined that *Government Code Section 552.104*, which protects information related to competition and bidding; *Section 552.110*, which protects commercial interests; and *Section 552.107(2)*, which protects court-sealed information, are applicable to information related to law enforcement technologies in particular circumstances.

Current law provides for privacy protection with regard to private locations, such as a person's home. However, instances regarding public locations that may capture private events are a concern. An example is an officer responding to a call at a hospital and inadvertently a patient receiving care being captured on camera. Although the patient is in a public location, their right to privacy remains intact.

The Arlington, Texas Police Department (APD) reported, *‘The management and processing of open records requests related to this technology (body camera technology) requires additional personnel to review and prepare legally releasable information and video footage. Many police incidents require multiple officers to respond. For example, a recent incident we responded to and received an open records request for. showed 40 patrol officers responded to the incident. This increases the number of cameras related to that incident. On a major incident which extends for a significant amount of time and requires significant resources, a request for body camera footage related to that incident may require days of staff time to gather and download the responsive video. In addition, video evidence must be reviewed minute for minute for possible redactions, and based upon our experience a single hour of video takes over an hour and a half to redact.*

In a white paper titled, "Police Body Mounted Cameras: With Right Policies in Place, a Win for All", the ACLU states, *‘While we have opposed government video surveillance of public places, for example, we have supported the installation of video cameras on police car dashboards, in prisons, and during interrogations. At the same time, body cameras have more of a potential to invade privacy than those deployments. Police officers enter people's homes and encounter bystanders, suspects, and victims in a wide variety of sometimes stressful and extreme situations. For the ACLU, the challenge on officer cameras is the tension between their potential to invade privacy and their strong benefit in promoting police accountability. Overall, we think they can be a win-win—but only if they are deployed within a framework of strong policies to ensure they protect the public without becoming yet another system for routine surveillance of the public, and maintain public confidence in the integrity of those privacy protections. Without such a framework, their accountability benefits would not exceed their privacy risks.’*

Delaware State Supreme Court Decision on Warrants

A March 2016 article in the *News Journal* by Saranac Hale Spenser reported that Delaware police searching for evidence in the digital world are going to have to be more specific in their warrants, following a decision from the State Supreme Court. When the state's high court reversed a child pornography conviction for former Town Hill headmaster, Christopher Wheeler, it also waded into new territory about the scope of search warrants for digital evidence.

Orin Kerr, a leading scholar on computer crime law, called it an *‘aggressive opinion’* because of how the court interpreted the Constitutional requirements for a search warrant in the digital age. *‘Most courts have been more generous to the government in allowing broad computer warrants. The Delaware opinion is part of an increasing trend recently toward courts being more strict in computer search and seizure cases since they are recognizing that those computers are home to people's digital lives.*

The reason that Wheeler (who was sentenced to 50 years in prison following his conviction involving 25 counts of dealing in child pornography) is getting ready to walk free is because the warrants used to search his home were far too broad. The State Supreme Court found that the warrants, which were supposed to be used to search for evidence of witness tampering, were worded almost identically to warrants used to search for child porn and they were not limited to any specific timeframe. Police had seized from Wheeler's home 19 pieces of digital or electronic evidence, including an iMac found in his piano room closet that hadn't been turned on since 2012. The iMac is the device that had the child porn on it. The problem the court found was that there could not have been any evidence of witness tampering before 2013, since Wheeler had not been contacted by the witness he might have tampered with until July of that year. So, there was no reason to search a computer that hadn't been turned on since 2012. *However, the state unsystematically sifted through Wheeler's digital universe, even though the iMac logically could not have contained material created or recorded during the relevant time-period,* the court said in its opinion, written by Justice Karen Valihura. All five members of the Delaware Supreme Court heard the case, which is something they typically do only for complex cases or ones that they anticipate will interpret important points of law. Usually, the court sits in three-judge panels.

Earl Bradley is a Lewes, Delaware, pediatrician who was convicted of raping his young patients. His final appeal was reviewed by the traditional three-judge panel. This panel rejected his argument that he deserved a new trial. One of Bradley's claims had been that he should get a new trial because his lawyer, during the first trial, had failed to get some of the digital evidence tossed out. Bradley argued that a video featuring himself with a 3-year-old girl had been gathered on a broad overreach of the warrant and his initial lawyer had failed to effectively make that case in an earlier round of hearings. During those proceedings, when the court had first been presented with the warrant-overreach argument, it had found that Bradley and his lawyer were reading the warrant too narrowly and rejected that interpretation. The court stated Bradley was using the same argument he had already raised and dressing it up as a claim of ineffective assistance of counsel.

While the court found that Bradley was interpreting the warrant in his case too narrowly, it found that the detectives in Wheeler's case were interpreting that warrant too broadly. The court said, *'We caution that the risk that warrants for digital and electronic devices take on the character of 'general warrants' is substantial, this reality necessitates heightened vigilance, at the outset, on the part of judicial officers to guard against unjustified invasions of privacy.*

The Delaware State Attorney General's Office took the opinion to mean that there had been no concrete changes to the existing rules for search warrants. They said, "It provides prosecutors, trial court judges and law enforcement officers with some guidance about tailoring warrant applications seeking electronic or digital evidence.

In a landmark opinion from the U.S. Supreme Court, they found unanimously that police cannot seize the digital contents of a cell phone during an arrest without a warrant.

TECHNOLOGY RECORD RETENTION AND MANAGEMENT

Within the Texas State Library and Archives Commission (TSLAC) is the State and Local Record Management Division (SLRM). The SLRM's principal role is to provide support services to Texas state agencies and local governments in their efforts to comply with state records management laws and to efficiently manage their information resources. These services include records management training; consulting; retention schedule development and certification; and document imaging and records storage services. The Records Management Assistance (RMA) unit serves all state agencies and approximately 10,000 local governments. Every local government must file with SLRM either a retention schedule they created, or submit a Declaration of Compliance stating that they will adopt one or more of the 12 records control schedules issued by TSLAC for local government.

Texas records management law only authorizes the destruction of a government record if the record appears on a records retention schedule approved for use by the government and the required minimum retention period for that record has expired (Government Code § 441.187 and Local Government Code § 202.001). TSLAC reported that it reviews and recommends records retention periods based on:

- State and federal statutes;
- Administrative rules and code of federal regulations;
- Reviewing statute of limitations for civil or criminal offense where applicable;
- If no statute or rule defines a retention period then researching best practice; and
- Best practices can include guidelines from associations or reviewing how other states or local governments are categorizing records.

The Texas State Library and Archives Commission provided information on the following:

Body Cameras

Upon the effect of SB 158, the "body camera bill," TSLAC received calls from local governments seeking assistance. On September 14, 2015, the Records Management Assistance unit issued preliminary guidance for body camera video by posting in the *Texas Record*, the team's blog, recommending records series meeting the minimum retention requirements of SB 158. SLRM began the process to revise local government schedule PS (Records of Public Safety Agencies) at the end of 2015. Local schedules are adopted in the *Texas Administrative Rules*. A

draft copy of the proposed schedule was circulated and informal comments were received from April 5, 2016 until May 6, 2016. Currently, the RMA team is reviewing those comments and incorporating necessary changes ahead of presenting the draft to the commission. TSLAC's plan is to have the revised schedule PS approved by the fall of 2016.

TSLAC offered written testimony stating, the proposed revisions refine RMA's preliminary guidance. Body camera video would be classified as one of two subseries:

- PS4125-04e – video and audio recordings – body worn cameras that do not capture a violation – 90 days;
- PS4125-04f – video and audio recordings – body cameras that do capture violations such as use of force or captures content that may be used as part of a criminal investigation - follow retention periods for internal affairs investigations (PS4075-01) or offensive investigation records (PS4125-05), but not less than 90 days regardless.

Examples of Texas local governments and other state's body camera retention policy were provided to the joint committee.

Research from *Police Body Worn Cameras: A Policy Scorecard (November 2015)* (www.bwccscorecard.org) compares 37 city policies from around the country for "footage retention."

- 16 do not require retention or could not be determined;
- 3 did not find any policies;
- 2 retain more than six months; partial retention or room to improve; and
- 6 delete unflagged video within six months.

Houston Police Department deletes non-evidentiary footage after 90 days.

- Recordings not classified as evidence or not needed for other official HPD business shall be retained for 90 days from the date of the recording before being automatically purged from the Video Evidence Management System database.

Dallas Police Department automatically deletes unflagged footage after 90 days.

- All video will be maintained for a minimum of 90 days. If the video has not been categorized as one which is to be retained it will automatically be deleted after 90 days.

Austin PD deletes non-evidentiary footage after 45 days.

- Downloaded incidents not needed as evidence or other official APD business will be erased after 45 days from the date of the recording.

USA State by State Body Camera Research, Bureau of Justice Assistance, Department of Justice, (www.bja.gov/bwc/pdfs/USA_StatebyStateBWC_Research.pdf) (August 2015) reports the following:

- 24 states do not have statewide body camera laws;
- 12 states have pending or proposed BWC laws; and
- 8 states have statewide statutes (few with retention periods)
 - **Texas** – at least 90 days;
 - **Oregon** – at least 180 days but not more than 30 months (if no court proceeding); and
 - **Kentucky** Archives added to retention schedule;
 - Non-evidentiary for 30 days; and
 - DUI-related incidents for 14 months unless accident occurred, then 26 months if no appeal.

Brennan Center for Justice at the New York University School of Law, Body Camera Policies (www.brennancenter.org/analysis/police-body-camera-policies-retention-and-release) reports the following:

- 24 cities’ policies – 8 do not specify retention; 45 days to 2 years for most others;
- ACLU Model Statute recommends 6-months for non-evidentiary video and 3 years for video flagged for retention by officer or subject; and
- Police Executive Research Forum (PERF) 60-90 days common for non-evidentiary video.

Automated License Plate Reader Systems (ALPR)

Several law enforcement agencies have requested TSLAC to issue minimum retention requirements for ALPR data. TSLAC plans to include a records series for ALPR data on the proposed draft of local government schedule PS. The minimum retention period for the series is “as long as administratively valuable (AV).” In the absence of state law or administrative rules from a public safety agency on retention of non-evidence ALPR data, SLRM defers to local governments to create policies and decide the appropriate amount of time to retain non-evidence. AV provides local governments maximum discretion when setting the retention period. At least one jurisdiction has chosen no more than 90 days as the appropriate retention period for non-evidence.

A number of local Texas governments have deployed ALPR systems. They are:

- Guadalupe County
- Arlington
- Blue Mound
- Decatur
- Fort Worth
- Grapevine
- Orange
- Austin is currently rolling out a pilot program.

Twelve states have statutes relating to the use of ALPR's or the retention of data collected by ALPRs. Five have no retention listed and the remaining states have retention from "not more than" 21 days to "within" 3 years (21 days, 30 days, 60 days, 90 days, 150 days, 3 years). Several states spell out "unless" or "except" reasons to hold the data. One state prohibits government from capturing ALPR data and allows the government to use the information only if the private company holds the data no more than 30 days.

Cell-Site Simulators or Stingrays

Cell-site simulators (CSS) or Stingrays are mobile surveillance systems the size of a small briefcase that emits a signal stronger than the signal of a legitimate cell tower in their vicinity in order to force mobile phones and other devices to establish a connection with them and reveal their cell phone-specific unique ID. Stingrays can then determine the direction from which the phone is connected with them, data that authorities can then use to track the movement of the phone as it continuously connects to the simulated tower. Stingray technology provides valuable assistance in support of important public safety objectives. They have been used as part of fugitive apprehension efforts, complex narcotics investigations, and to locate or rescue kidnapped children. Law enforcement feel they fulfill a critical operational need.

The DOJ states that, *"As with any law enforcement capability, the Department must use cell-site simulators in a manner that is consistent with the requirements and protections of the Constitution, including the Fourth Amendment, and applicable statutory authorities, including the Pen Register. Moreover, any information resulting from the use of cell-site simulators must be handled in a way that is consistent with the array of applicable statutes, regulations, and policies that guide law enforcement in how it may and may not collect, retain, and disclose data."*

The Guardian reports that in addition to traditional law enforcement agencies, the Internal Revenue Service possesses and is using the surveillance equipment for criminal investigations.

Washington State joined Virginia, Minnesota, and Utah in imposing a warrant requirement at the state level. Washington state law restricts use and places limitations on retention of data by requiring that any incidental information collected from bystanders not be used and be deleted promptly.

ACLU Testimony to Congress in October 2015 said, *“Given the large amount of information collected by Stingrays, it is critical that there be strict limits on the retention of information. All information of non-targets should be purged immediately to prevent improper access. While the guidance contains this requirement in some circumstances, it permits retention for up to thirty days in cases where law enforcement is attempting to locate an unidentified phone. ACLU believes such a lengthy retention period is concerning, given that Stingrays may gather the information of thousands of individuals at any given time. To address this concern, officials should be required to obtain permission from a judge to retain information longer than three days, for a maximum of thirty days.*

Stingrays do not function as a GPS locator, as they do not obtain or download any location information from the device or its applications. The Department of Justice reports a Stingray may not be used to collect the contents of any communication. This includes any data contained on the phone itself: the simulator does not remotely capture emails, texts, contact lists, images or any other data from the phone. In addition, Justice Department cell-site simulators do not provide subscriber account information (name, address, or telephone number). To address the issue of over-collection, the DOJ announced a policy requiring federal law enforcement agents to delete all data the Stingray collects “as soon as” it has located the specific device it is tracking. The DOJ policy allows for exigent circumstances or exceptional circumstances, whereby law enforcement agents can use Stingrays without a search warrant in emergency situations, when obtaining a warrant is not practical. The DOJ is required to track and report the number of times the technology is deployed under these exceptions.

Red Light Cameras

SB 1119 (80(R)) created a photographic traffic signal enforcement system for Texas. Since the last revision of the TSLAC local government schedule PS in 2011, Record Management Assistance has received several inquiries from local governments about adding a records series to their schedules to authorize destruction of these records. The proposed draft of local government schedule PS includes two records series for red light camera data. The first includes data that does not capture a violation or for which a notice of violation is not mailed. TSLAC set the retention period at 30 days based on *Transportation Code, §707.011(b)*. For data that does capture a violation, a retention period was set based on *Transportation Code, §707.016*. The minimum retention period for these records is “date civil penalty paid or 31 days after judgment, whichever sooner.” This permits the record to be retained long enough for the owner

of a motor vehicle time to appeal the violation. Records that are part of a legal appeal may not be destroyed until the completion of that legal action.

Unmanned Aircraft

The use of drones by law enforcement is discussed in *Government Code Chapter 423, Use of Unmanned Aircraft*. The statute was created by the 83rd Legislature with the passage of HB 912. Additional language was added to the statute by the 84th Legislature with the passage of HB 2167. The statute recognizes the use of unmanned aircraft by law enforcement. The statute requires law enforcement agencies to send a report to the Legislature on odd numbered years (*Government Code §423.008*). However, the statute does not specify a retention period for images captured. In addition, no state agency or local government has inquired about records retention for unmanned aircraft video at this time. TSLAC will continue to track this emerging technology.



RECOMMENDATIONS

The Legislature should amend the Public Information Act to protect the privacy of citizens inadvertently captured on police body camera footage and require TSLAC to set specific retention rules for the images. An instance cited to the committee was while on an official call to the hospital, an officer's body camera captured a person in a private encounter while in a public place; such as a patient receiving medical care in the hospital that is unrelated to the officer's call. The committee recommends review and possibly amend the statute to ensure appropriate privacy is given. Through the rulemaking process, TSLAC will be able to address concerns in a more timely manner with some flexibility.

For privacy, the Legislature should consider not only additional exemptions to the Public Information Act such as information garnered by ALPRs, but a specific prohibition from disclosing private citizen information. As technology develops, new types of data are emerging that may be subject to provisions of the Public Information Act. The Legislature has responded to concerns arising from specific emerging technologies, such as iris scans, fingerprints and certain DNA analyses in the past.

The Legislature should set a specific retention schedule of non-evidence ALPR data. Under current state law, there are no restrictions that limit police departments from storing collected information from automatic license plate readers indefinitely or from preventing the inclusion of this data into a regional or nationwide tracking database program. While automatic license plate readers can serve a legitimate law enforcement purpose when they alert police to the location of a car associated with a criminal investigation, the ability for police departments to retain this information without restrictions has raised significant privacy rights concerns.

The Legislature should review and determine if the statutes regarding granting and enforcing search warrants are sufficient, taking into consideration emerging technologies such as ALPRs and Stingrays in law enforcement. A Delaware Supreme Court decision resulted in similar cases having very different outcomes due to the scope and search under the warrant. One was ruled too broad, while the other was ruled too narrow.





1

2

,

,

