

## HOUSE COMMITTEE ON APPROPRIATIONS

### SUBCOMMITTEE ON STATE INFRASTRUCTURE, RESILIENCY, AND INVESTMENTS

#### INTERIM CHARGE 2:

*Review the funding appropriated to state agencies for information technology (IT) and cybersecurity improvements and modernization. Evaluate the cost of ongoing IT and cybersecurity upgrades and the methodology for prioritizing projects.*

The following constitute responses to a request for information regarding the above interim charge posted on August 5, 2020.



## **House Appropriations**

### **Subcommittee for Infrastructure, Resiliency, and Investments Request for Information**

***Interim Charge 2: Review the funding appropriated to state agencies for information technology (IT) and cybersecurity improvements and modernization. Evaluate the cost of ongoing IT and cybersecurity upgrades and the methodology for prioritizing projects.***

The Texas Health and Human Services Commission (HHSC) is responsible for the overall delivery of health and human services across the state, including hundreds of programs and services. It provides for those who need assistance to buy necessities, eat nutritious foods, and pay for health care costs by administering programs such as Temporary Assistance for Needy Families (TANF), Supplemental Nutrition Assistance Program (SNAP), Women, Infants and Children (WIC), Medicaid, and Children's Health Insurance Program (CHIP). The agency also operates 13 state-supported living centers (SSLCs) that provide direct services to people with intellectual and developmental disabilities and 10 state hospitals which serve people who need inpatient psychiatric care. All 23 of these facilities are operated 24 hours a day, seven days a week. HHSC also provides a multitude of other mental health and substance abuse services, help for people with special health care needs, community supports and services for older Texans, disaster relief assistance, and resources to fight human trafficking.

HHSC's Regulatory Services division works toward health and safety in public establishments such as medical facilities, nursing homes, childcare centers, and facilities operated or contracted by the state. In addition to the well-known programs like Medicaid or CHIP that assist millions of Texans every day, there are numerous administrative divisions including financial services, legal services, policy, system support services, contracting/procurement, and public affairs that support and maintain the environment for the wide variety of programs and effective delivery of services.

Pursuant to Rider 175 of the 2020-21 General Appropriations Act, House Bill (HB) 1, 86th Legislature, Regular Session, 2019, specified HHS prepare and submit to the Governor, Legislative Budget Board (LBB), and post to the commission's website a 10-year system-wide plan outlining the manner in which the commission intends to

transition its information technology and data-related services and capabilities into a more modern, integrated, secure, and effective environment.

The Rider 175 plan details HHS's 10-year plan for IT and Data Services Modernization, including goals, objectives, deliverables, measures of success, and recommendations for each of the following key topic areas:

- Legacy Infrastructure Modernization;
- Security;
- Legacy Systems Modernization;
- Data Services;
- Identity and Access Management;
- Converged Services;
- Client and Agency Computing; and
- Workforce.

The HHS Information Technology and Data Services Modernization Plan addresses information technology and data services for HHSC, Department of State Health Services (DSHS), Office of the Inspector General (OIG), as well as the shared technology and support services provided to the Department of Family and Protective Services (DFPS).

The 86th Texas Legislature funded exceptional items in addition to base funding to support IT-related projects in programs throughout the HHSC system. These included funding for modernized systems to support the transition of Long Term Supports and Services (LTSS) for persons with intellectual and developmental disabilities to managed care; technology to improve care for persons in state hospitals and SSLCs; automation changes allowing for enhanced and expanded criminal background checks for child care providers, long term care facilities, certified nurse aides, and other professional licensees; and automated improvements to the fair hearings and contracting processes.

Exceptional items funded by the legislature in the 86th Session are not only for enhancing technology to support specific functions and services, but also help lay the groundwork for the transition into a more modern, integrated, secure, and effective environment. Specifically, the legislature provided \$7,960,640 funding for HHSC to create a cloud-based Business Enablement Platform (BEP). BEP will be a shared platform that provides multiple benefits for constituents, the state, and the agency's federal partners, including significant improvements in the efficiency and effectiveness in program operations, continuous system enhancements, and reduced costs for system maintenance. Furthermore, the platform will provide a foundation that may be used to consolidate and simplify the current complex and dated system landscape, lowering risks, costs, and time requirement to implement system changes.

Additionally, the Legislature provided \$26,282,334 in exceptional item funding for IT security, including funding to improve the agency's security posture, conduct a comprehensive security risk assessment of certain legacy functions, and implement a risk management plan to address vulnerabilities.

Finally, \$126,654,750 was provided for Data Center Services (DCS).

**IT Projects Funded by 86<sup>th</sup> Legislative Session**  
**Base and Exceptional Items**

<b>IT Project</b>	<b>EI Funding</b>
Application Remediation for Data Center Consolidation	\$600,000
Business Process Redesign	\$2,130,159
Cybersecurity Advancement for HHS Enterprise	\$1,261,870
Data Center Consolidation	\$126,654,750
HHSC Telecom Technology Upgrade	\$6,331,593
Information Technology – Mental Health (infrastructure for State Hospitals)	\$1,738,497
Infrastructure Maintenance at SSLCs to Support Electronic Health Records	\$1,000,000
IT Security Posture Improvement	\$3,631,754
Network, Performance, and Capacity	\$3,116,000
Office for Civil Rights (OCR) Corrective Action Plan (CAP) Response	\$21,388,710
Seat Management Services (PCs, Laptops, & Servers)	\$39,876,250
System-Wide Business Enablement Platform	\$7,960,640
Texas Integrated Eligibility Redesign System	\$108,122,959
Medicaid Management Information System	\$133,635,867
Enterprise Data Governance	\$10,918,975
Regulatory Services System Automation Modernization	\$2,532,000
WIC Hardware/Software Refresh (former PC Replacement)	\$1,350,000
Medicaid Fraud Detection System	\$5,000,000
Performance Management and Analytics System (former SIAM)	\$7,828,160
System Changes to Support IDD Carve-In	\$13,538,542
Criminal Background Checks	\$878,329
Health and Specialty Care System Technology Enhancements	\$12,028,000
CMBHS Roadmap Enhancements Phase 3 (Data Sharing)	\$383,769
WIC Chatbot Messenger	\$950,000
WIC Mosaic	\$40,000,000

IT Project	EI Funding
Child Care Licensing Automated Support System (CLASS)	\$4,245,633 authorized \$2,929,993 funded
Fair Hearings Decisions Accessibility	\$304,395
Database of Hospital Financial and Payment Information	\$400,000
CAPPS Financials (HHSAS to CAPPS Upgrade and Enhancements)	\$4,734,542
CAPPS Enterprise Resource Planning (ERP/HCM)	\$10,350,277
CAPPS People Soft Licenses	\$2,795,364
CAPPS Upgrades and Inventory (PCIP)	\$5,000,000

HHSC IT is comprised of approximately 1,700 employees and contractors located throughout the state, providing IT support and services for more than 325 mission-critical applications and approximately 50,000 desktops/laptops and email accounts. HHSC IT manages 500 IT contracts (some of the largest in the state), 44,000 computing devices and users, 58,000 telephones and cell phones, 6,220 servers, 600 websites, 4.5PB data storage, and 1.6 million network addresses.

HHSC is required to ensure its systems and processes are aligned with the 2020-2024 State Strategic Plan for Information Resources Management, in compliance with Government Code, Chapter 2054; Texas Administrative Code, Title 1, Part 10, Chapter 202; and the DIR Software Currency Policy.

Like most state agencies, HHSC maintains “mission-critical” business applications for program areas that use legacy software or hardware, and in most cases, both. HHSC IT must continue to modernize legacy infrastructure, by implementing enterprise IT system tools and services and applying industry standard service management processes.

A modernized IT system requires modernized IT infrastructure to work optimally and deliver the benefits of increased productivity and reduced operating costs. HHSC uses many obsolete and custom-developed applications that take longer to deploy and require considerable inefficient human and technological resources to operate and maintain.

#### **Legacy Infrastructure Modernization Costs:**

Health and Human Services Information Technology Infrastructure Services support the operations and maintenance of over 6,000 servers and a legacy mainframe environment.

The HHSC IT infrastructure system hosts over 300 business applications; these applications include a variety of statewide case management systems, content management solutions, databases, business data analytic and reporting systems, administrative and collaboration systems, and system support tools. Access to these systems happens across a complex and intricate network spanning across multiple HHSC campuses, Health Service Regions, Regional Field Offices, SSLCs, and state hospitals.

When servers experience unexpected outages, clients may experience delays when applying for on-line health benefits or receiving critical care from our SSLCs or state hospitals. Unexpected outages with systems such as the National Electronic Disease Surveillance System (NEDSS) may also directly impact the health and safety of our citizens as delays could occur with reporting, laboratory testing, diagnosing and treating chronic and infectious diseases, such as COVID-19 pandemic.

Providing current, reliable, and scalable IT infrastructure is required when ensuring the highest level of system availability. Not doing so could result in the following.

- Outdated hardware can result in an increased number of unexpected outages, limited available parts, and limited hardware support maintenance agreements.
- Unsupported software can lead to incompatibility with newer application software, limits the ability to increase functionality, may cause hardware to malfunction, and, most importantly, the inability to apply critical security updates or software patches.
- Non-virtualized environments are unable to provide resiliency and scalability when the system experiences peak capacity.
- There are significant financial risks if legacy infrastructure is not up-to-date, and there is a delay in modernization efforts. Hardware and software that is at End of Life or in limited support status can result in many unexpected direct and indirect costs to the agency as well as costs to citizens funding these services.
- Aged and/or unsupported hardware and software can result in premium-priced maintenance support agreements. When systems are aged, many vendors do not invest resources in developing upgrades or patches and charge higher than usual prices for extended or limited support maintenance agreements.
- Aging infrastructure is more likely to result in unexpected outages, resulting cost associated with loss of productivity for program staff, potential data loss and recovery efforts, acquiring premium-priced niche support vendors or contractors, and other possible expenses related to parts and labor, and resolution.
- Legacy environments with no modernization path can result in stranded assets and costs associated with hiring personnel or contractors.

- Multiple software versions make it difficult to consolidate services and shrink costs associated with expensive software license agreements, overall resulting in redundant costs for similar services.
- The inability to accurately identify and classify data requires building all systems using the highest level of data retention requirements, resulting in uncontrolled storage growth and management costs.
- Redundant legacy systems can result in extraneous hardware and software license costs, as well as operating expenses for support personnel.
- Unsupported infrastructure and software may result in security vulnerabilities, resulting in potential penalties, audit findings and the potential loss of funding for programs.

With the funding provided in the 86th Legislative Session, efforts are currently underway to consolidate almost 900 servers into the State's DCS program. These efforts will ensure that the legacy equipment is in a modern virtualized private community cloud environment with up-to-date hardware infrastructure, expandable storage, tapeless backup and recovery systems, disaster recovery, and managed using federal security controls. These servers support the Medicaid Management Information System (MMIS) and Local Office Infrastructure (LOI) servers [60 percent].

The Texas Integrated Eligibility Redesign System (TIERS) has an exemption from the DCS program for a minimum of five years. However, the HHSC IT Infrastructure teams will be working with third-party vendors to assess the viability for TIERS to be cloud-enabled.

Ongoing costs will include the consolidation of the remaining 40 percent of the 868 LOI servers and implementing cloud-like technology and/or migrating to the cloud, overall enabling the benefits of flexibility and scalability offered through cloud computing.

### **Security Costs:**

The HHSC IT Information Security Program is based on well-established federal, state, and international frameworks, standards, and best practices. The Program is a robust system that covers 39,000 full-time employees and 5,000+ contractors using 500+ business programs. The agency faces more than 94 million cyberattacks annually.

HHSC IT manages the safety and protection of agency services and programs through the cyber protection of sensitive information and information resources. HHSC maintains sensitive, protected information and systems/applications that perform mission-critical functions for the state's safety net, both of which require continuous

security monitoring. Maintaining an optimal cybersecurity infrastructure and operations program reduces the likelihood of security breaches and helps protect confidential information from unauthorized access.

Though guided by sound policy and supported by key legislative funding, these technology advances and the large number of HHS systems, networks, and devices increase the complexity, severity, and number of attempted breaches and potential for failure. While HHS IT has taken definitive actions during the past several years to improve its information security program, achieving compliance is a dynamic challenge across the complex HHS system, especially as the agency's funding for information security is only .049 percent of the overall agency's budget. As security systems are enhanced, cybersecurity perpetrators also get smarter. It is a cycle with no end, continuously challenging the agency's ability to protect its cyber environment.

During recent legislative sessions, the Legislature has recognized the importance of cybersecurity, including by passing HB 8 (2017) and SB 64 (2019). Funding was approved in the 86th Legislative Session for HHS Information Technology Security and was dedicated to improving the agency's security posture, conducting a comprehensive security risk assessment of certain legacy functions, implementing software code scanning tools, and implementing a risk management plan to address vulnerabilities. Agency security processes developed this biennium for risk assessments and analysis of functions are repeatable across HHS in a risk-based approach to implement ongoing compliance with federal and state security requirements.

Even with state-wide focused efforts to achieve compliance and protect customers and agency functions, HHSC IT faces a uniquely dynamic challenge among such a vast, complex system. All individuals with data stored by HHS systems, including Texas citizens' Personally Identifiable Information (PII) and Protected Health Information (PHI) must be protected from data breaches or malicious acts.

The security threat to confidential information continues to grow and represents one of the most serious challenges that HHSC IT must confront. Security of HHS information depends on its ability to protect the agencies' critical systems and infrastructure in the face of such threats. Continued funding to address this constantly evolving environment to remain vigilant in protecting the data of Texans and the services they receive is a mission critical necessity.

Furthermore, HHSC IT's success depends on the reliable functioning of critical programs and infrastructure. While modernization has added capacity and capabilities to the system, cyberattack threats exploit the increased complexity and connectivity



of critical infrastructure systems, placing HHS's cybersecurity, resources, safety and health of clients at risk.

During Fiscal Year (FY) 2020-21, HHSC invested and addressed cybersecurity issues. HHSC IT will need to invest consistently to ensure optimal cybersecurity for these funded improvements give HHSC application teams an important tool to use during development to identify and remediate security vulnerabilities and weaknesses before production.

Information system security plans and risk assessments include the on-going processes of discovering, correcting, and preventing security weaknesses. These include application assessments via application vulnerability scans. If potential application security weaknesses are not prevented or discovered and remediated, the risk of a potential data breach could occur. This could prove to be costly in both the potential fines associated with certain data breach types but in the loss of public trust.

As part of the agency's FY 2022-23 Legislative Appropriations Request, the agency is planning to request funding for the HHSC Cybersecurity Perimeter and Decryption platform. This platform will allow for increased capability in detection and prevention, increase visibility into the agency's network traffic to allow improved security monitoring, and allow better strategies for managing potential risk.

In FY 2024-25 it is estimated that the agency will request \$10.1 million for HHSC Cybersecurity Security Information and Event Management (SIEM) migration, cybersecurity equipment migration, governance risk compliance integration, and conducting third-party security assessments. These efforts would ensure a secure architecture is considered and implemented, as well as the deployment of a cybersecurity platform to protect agency cloud infrastructure.

To align with the HHS Information Technology and Data Services Modernization Plan, it is anticipated that the agency will request \$8.0 million in FY 2026-27 to move business processes which are currently on-premise or located in managed data centers to cloud-based solutions. Additional cybersecurity tools will be needed for this key platform. This funding will also establish an independent penetration testing program to continuously improve the security posture and comply with the National Institute of Standards and Technology (NIST) requirements.

In FY 2028-29, it will be time to refresh the Cybersecurity Perimeter and Decryption life cycle infrastructure with an estimated cost of \$9.0 million. This effort will seek to maintain effective security in the most efficient manner with the least amount of complexity while proactively reducing risk, meeting regulatory requirements, maintaining privacy and supporting HHS system initiatives.

**Legacy Application Modernization Costs:**

HHSC Application Services oversees the development, deployment, and ongoing management of the agency's software application suites. Application Services manages over 300 applications that support multiple stakeholder types. These stakeholders consist of; internal programs and departments within HHSC, external stakeholders such as partner governmental/care agencies, and the citizens of the State of Texas that receive state supported benefits and care. These applications include some of the largest and most complex systems in Texas, including but not limited to:

- TIERS
- MMIS
- Client Assignment and Registration System (CARE)
- Clinical Management and Behavior Health Services (CMBHS)
- Centralized Accounting and Payroll/Personnel Systems – Financial and HR CAPPS-FIN and CAPPS-HR

HHSC Application Services' ability to modernize their application suites and legacy systems requires multiple projects and programs. This modernization effort requires consistent management support, year over year funding, and constant review and adjustment as technologies continue to change. The following is dependent on future funding availability: DCS and Information Security to migrate production applications to middleware software and infrastructure that is reliable, scalable, and secure.

The full utilization of an information technology system management system will allow Application Services to use an integrated approach to ongoing application management. Disposition and modernization of all legacy applications begins to increase with a destination of:

- Implement an Agile delivery framework;
- Develop a Dev/Ops pipeline;
- Retire all duplicative applications;
- Rewrite custom agency process applications on the BEP;
- Reinvest in customized COTS products that are needed for key business functions such as ERP;
- Replace standard business functions with Commercial Off the Shelf (COTS) solutions;
- Replace standard business functions with Software as a Service (SaaS) solutions;
- Keep production applications in a healthy state; and
- Continue migration of the modernized applications to the cloud until all applications identified for cloud adoption are migrated to their new environment.

The evolution of the HHSC Application Services must be a priority for both the organization's management and the legislature. These core applications are the information systems that maintain all the state's health data and benefits processing, including but not limited to; clients who receive benefits, such as WIC, SNAP, TANF, etc., reimbursement rates and history for Medicaid and Medicare funding, and personal information on citizens with infectious diseases, such as COVID-19 pandemic.

Any security breach, loss/leakage of data, and/or unexpected disruption of service for any of these applications would lead to federal violations (such as the HIPAA Act), loss of state revenue (without partner/federal reimbursements), and overall brand destruction as millions of Texans' personal information would be at risk.

### **Converged Services Costs:**

HHSC Converged Services oversees the agency's telecommunications and network infrastructure. The primary objective of HHSC Converged Services is to provide a secure, scalable, and reliable enterprise-level network that provides voice, video, and data service delivery.

HHSC Converged Services provides network services to more than 750 locations across Texas – including 24/7 support to 50 "critical service" locations such as state hospitals and SSLCs – as well as voice services to approximately 465 of these locations. Examples of services provided include: private multi-protocol label switching transport; establishment of the appropriate network type [Wide Area Network (WAN), Local Area Network (LAN), or Wireless Local Area Network (WLAN)]; access to public and private cloud service platforms (e.g., Microsoft Office 365) and DIR DCS; Internet access; unification and integration of communication modes and platforms; and a physical client support center with remote support capabilities, for HHSC telework and mobility initiatives.

HHSC IT Converged Services must continue to acquire additional capacity to ensure the viability of existing infrastructure, which provides the support required to meet the evolving needs of the HHSC program areas that oversee the delivery of client services. These ongoing efforts are also an essential component in HHSC' business operations priority to expand telework and alternative work capabilities, particularly in light of the challenges that surfaced as a result of the COVID-19 pandemic that was declared a statewide public health disaster by Governor Greg Abbott.

By the end of fiscal year 2021, 48 percent of the existing HHSC network infrastructure hardware and software will have reached manufacturer end of support, with that percentage exceeding 90 percent by the end of 2023. IT industry nomenclature refers to this juncture in a product's life expectancy as the End-of-Service Life (EOSL).

In addition to EOSL equipment no longer being supported by the manufacturer, repairs or replacements are often unavailable, and unavailability of security patches increases overall network vulnerability. Maintaining threat protection updates is an important component of protecting employee access to mission-critical applications and data, as well as safeguarding HHS data and systems from unauthorized access and intrusion.

The legislature funded an appropriation request in the amount of \$6.3 million for FY 2020-21 to complete the transition of voice access services to IP-based technologies, beginning with a Time-Division Multiplexing (TDM) to Session Initiation Protocol (SIP). TDM technology has been the industry standard for more than 50 years, but with the increasing reliance on high-speed connectivity, the ability to transmit data quickly has resulted in transmission over phone lines becoming nearly obsolete. SIP technology utilizes Ethernet to transfer data at much faster speeds, providing the flexibility to integrate with cloud platforms, and resulting in significant cost savings due to lesser demand for physical hardware and infrastructure.

For FY 2020-21, the legislature provided \$3,116,000 in base funding for a routine network infrastructure refresh program to be developed and deployed. The agency has developed another exceptional request as part of its FY 2022-23 Legislative Appropriations Request.

### **Prioritizing Projects:**

HHSC IT coordinates a governance structure with representatives from central parts of the enterprise, including Business, Applications, Infrastructure, Finance, and Security, to participate in IT decisions using the IT Governance Intake Process. The process ensures that program requests for IT services are clearly defined and that IT solutions are approved and prioritized by leadership. This structure also provides a forum for notification of IT policies to facilitate awareness and compliance, which will assist with implementing and sustaining the desired streamlined, standardized, and simplified service delivery model for IT services.

Each portfolio has an Executive Steering Committee (ESC), which includes the Chief Information Officer and other members of executive management from the portfolio. The ESC focuses on prioritization, application and contract lifecycle planning, data analytics and ensures that program decisions are aligned with and prioritized to the HHSC strategy and goals.

HHSC IT has a plan to achieve the desired future state with a solution that will be designed, developed, and deployed with an agile/iterative approach. The approach is careful and methodical, and based on an agency wide needs assessment to ensure

maximum benefit, proper ordering of legislative and agency priorities, and the ability to leverage and build on existing capabilities.

**Department of State Health Services**  
**Response to the House Committee on Appropriations**  
**Request for Information – Sept. 2020**

**Subcommittee on Infrastructure, Resiliency, and Investments**

**Charge 2: IT and Cybersecurity Improvement Funding**

**Projects Covered:**

- NEDSS
- LIMS
- Video Direct Observed Therapy Pilot (VDOT)
- THCIC

**DSHS Exceptional Item 1b, Laboratory Information Management System (LIMS) Improvements**

- **Amount:** \$5,888,099 in General Revenue Funds.
  - DCS Hosting Solution: \$2,012,035
  - LabWorks Upgrade: \$192,000
  - LabWare Upgrade: \$2,000,000
  - Harvest Upgrade (Orchard): \$650,000
  - Staffing/HHSC IT:
    - FTEs \$531,558
    - Contractors \$513,231
- **Scope:**
  - This exceptional item provides funding to upgrade portions of the Laboratory Information Management System (LIMS) system.
  - Three applications, LabWorks, LabWare, and Harvest will be upgraded to improve the speed of processing lab orders and tests results within the lab, as well as submitting DSHS lab results to ordering entities.
  - To facilitate this, hosting of all laboratory servers must be transferred to DCS. The transfer also includes a disaster recovery solution.
- **Progress:**
  - Due to competing IT demands required by responding to COVID-19, the implementation of this item was delayed.
    - Two IT staff were hired September 8, 2020 to work on the project (Security Analyst, Test Analyst).
  - DCS Hosted Server Transfers:
    - Prior to the delay, LabWorks was migrated to a DCS server on March 31, 2020.
    - DSHS continues to work with DIR on DCS hardware installations for LabWare and Harvest. Estimated completion dates:

- LabWare: Migration is dependent on upgrade. The migration is planned for completion by July 2021.
  - Harvest: August 2021.
- LabWorks upgrade:
  - Estimated completion date: October 3, 2020.
- LabWare upgrade:
  - RFO release: estimated for mid-October 2020, with an engagement of the vendor planned for mid-November 2020.
  - Estimated completion date: August 2021.
- Harvest upgrade:
  - Purchase Order: in process as of September 2020.
  - Estimated completion date: August 2021.

## **DSHS Exceptional Item 4, Texas Enhancement of the National Electronic Disease Surveillance System (NEDSS)**

- **Amount:**
  - Exceptional Item:
    - Program FTEs: Increase surveillance/analysis capacity: \$689,993
    - IT Costs/IT FTEs: \$3,516,037
  - COVID-19 Driven Scope Expansion:
    - IT Costs: \$2,055,871
- **Scope:**
  - This exceptional item supports enhancements to the National Electronic Disease Surveillance System to bolster statewide infectious disease reporting, public health information exchange, and outbreak response capability in Texas.
  - COVID-19 response required the expansion of the product to meet the unforeseen need to capture positive, negative, and indeterminate results for a new reportable condition on a wide-scale basis.
  - The investment by the 86<sup>th</sup> legislature provided an essential foundation for expanding the project, which was supported by federal COVID-19 funds.
- **Progress:**
  - Program FTEs:
    - Full time: 4. All positions are in hiring/posting phases.
  - IT FTEs:
    - Full Time: 3. One position filled, with 2 others in hiring process.
    - Temporary: 5. All temporary IT staff hired.
  - NEDSS Infrastructure Analysis:
    - Completed May 2020.
    - Analysis identified need for Amazon Web Services (AWS) environment.
  - DCS Transfer:
    - Migrated to AWS: June 2020.
    - Server migration: Oracle to SQL completed August 2020.
  - Implement System Upgrades/Improvements:
    - This process was driven by the NEDSS infrastructure analysis results.
    - NEDSS upgrade to version 5.4.6 completed August 2020.
- **COVID-19 Scope Expansion:**
  - Due to pressing needs to stabilize NEDSS for the COVID-19 response, additional actions were taken to increase the scope of the project, resulting in the following increased capital costs. These costs are covered primarily with federal dollars:
    - \$1,393,371: Paycheck Protection Act
    - \$300,000: CARES Act – Coronavirus Aid, Relief, and Economic Security Act
    - \$362,500: General Revenue (to cover DCS capital needs)
  - Capital Cost Increase: \$2,055,871



- Cloud transition (AWS): \$925,182
- New security portal for cloud environment: \$357,492
- Expediting and initiating new functionality to process increase Electronic Lab Results (ELR) intake: \$666,157
- Software application to more accurately and more quickly process problematic and duplicative data: \$107,040.
- Transitioning to AWS will result in increased ongoing DCS costs in future fiscal years.

#### **DSHS Exceptional Item 5 – Video Direct Observed Therapy Pilot (VDOT)**

- **Amount:**
  - \$0. Provided capital authority to acquire IT solution.
- **Scope:**
  - The purpose of the Video Directed Observed Therapy (VDOT) pilot is to more efficiently respond to treating persons with outpatient medication therapy for individuals who test positive for tuberculosis infection (TB).
  - Without the pilot, nurses stationed in regional offices must travel great distances to visit patients to ensure medications are taken consistently and to monitor symptoms.
  - Use of VDOT reduces travel time and costs, and allows nursing staff to serve more patients in a given day.
  - VDOT requires the use of a secure IT solution to facilitate.
- **Progress:**
  - **Short-term solution:** In response to COVID-19, DSHS was able to secure a temporary VDOT solution using an emergency procurement. The use of this solution is time-limited to the duration of COVID-19 response.
    - Cost: \$77,500.
    - Acquired: March 25, 2020, using General Revenue funds.
    - Additionally, a second short-term procurement for this began September 1, 2020 and will end February 28, 2021, using General Revenue Funds.
  - **Long-term solution:** DSHS is also proceeding with the standard Health and Human Services procurement process.
    - Due to prioritization of COVID-19 response related procurement needs, the VDOT procurement was delayed through August 2020.
    - The solicitation was posted by HHSC IT on August 3, 2020.
    - Solicitation review is expected to be completed by February 1, 2021.
    - HHSC Procurement and Contracting Services is planning to have a contract secured by March 1, 2021.

## HB 2041 – Freestanding Emergency Medical Facility Data Collection

- **Amount:** \$841,886, 1 FTE
- **Scope:**
  - HB 2041 increased the scope of the Texas Health Care Information Collection system by allowing DSHS to collect administrative claims data from Freestanding Emergency Medical Facilities.
    - Administrative claims data commonly include the diagnosis, procedural, and charge information. Charge information means, the amount charged prior to any adjustments due to insurance type or status prior to actual billing and payment.
  - To do so, DSHS needed to amend an existing contract with a third party, System13, Inc. to facilitate data collection with facilities subject to the requirements of Chapter 108 of the Health and Safety Code.
  - One FTE was appropriated to oversee the data collection process, communicate with entities subject to the reporting requirement analyze received data, and organize dissemination of the collected data.
- **Progress:**
  - DSHS rules modified the current Texas Health Care Information Collection process were adopted February 18, 2020.
  - The vendor contract was amended to incorporate the new requirement outlined in statute and rule.
  - Throughout the process, DSHS worked with FEMC stakeholders to communicate about the new requirement, discuss data dissemination needs, and to alert FECs to begin reporting Fourth Quarter 2020 data beginning October 2020 through March 1, 2021. This will align FEMCs with other facilities required to report on a quarterly basis.
  - DSHS will begin analyzing Fourth Quarter 2020 beginning mid-2021 to determine what will be included in regular reports by DSHS that will cover FEMC administrative claims data.
  - The FTE was hired in August 2020.



# TEXAS ALCOHOLIC BEVERAGE COMMISSION

*Texans Helping Businesses & Protecting Communities*

P.O. Box 13127  
Austin, Texas 78711-3127  
(512) 206-3333  
[www.tabc.texas.gov](http://www.tabc.texas.gov)

September 30, 2020

The Honorable Giovanni Capriglione, Chair  
The Honorable Gene Wu, Vice Chair  
Committee Members  
House Appropriations – S/C on Infrastructure, Resiliency and Investment Committee  
Capitol Building, Room E1.032  
Austin, TX 78701

Dear Chairman Capriglione, Vice Chair Wu, and Committee Members:

The Appropriations – S/C on Infrastructure, Resiliency and Investment Committee requested information pertaining to Interim Charge 2. Enclosed is a detailed summary of the TABC Technology Transformation Initiative, including the appropriations for information technology (IT) and cybersecurity improvements and modernization; and a breakdown of priority projects and identified future costs and challenges for IT and cybersecurity upgrades.

In the 2018 Legislative Appropriations Request (LAR) process for the Fiscal Year 2020-21 biennium, TABC requested a total of \$13.5 million in capital funding and authority for its TABC Technology Transformation Initiative needs. Of this \$13.5 million request for technology capital projects, the Texas Legislature appropriated and authorized \$9.9 million to TABC.

This \$9.9 million appropriation is being used to replace as many of the agency's 18 disparate legacy systems as time and funding will allow during this current biennium.

TABC anticipates annual cost to be approximately \$1.2 million per year. This cost will cover the Alcohol Industry Management System (AIMS) cradle-to-grave solution, the Enterprise Data Solution that includes the Google Cloud Platform, and ongoing maintenance and support fees for the new public website hosted on Texas.gov. Because TABC will have to continue most of its legacy systems through the next biennium during the transition period, Data Center Services costs must also continue as is throughout FY 2022-23. TABC expects that by FY 2024, DCS costs for current infrastructure will significantly decrease as legacy systems are fully decommissioned and data from the old systems is purged over time.

## **TABC Technology Transformation Initiative**

### **1. AIMS Project**

The bulk of the current scope includes the build-out of AIMS, a cloud-based Software as a Service (SaaS) platform hosted on the Amazon Web Services GovCloud, which is designed to be a cradle-to-grave solution useable by all licensing, compliance, enforcement, and business divisions within TABC. AIMS will include functionality for industry members to self-manage their online account profile; have access to an online



# TEXAS ALCOHOLIC BEVERAGE COMMISSION

*Texans Helping Businesses & Protecting Communities*

P.O. Box 13127  
Austin, Texas 78711-3127  
(512) 206-3333  
[www.tabc.texas.gov](http://www.tabc.texas.gov)

dashboard that will include pertinent information about existing licenses/permits, applications for new licenses/permits, applications for license/permit renewals; and review, in real time, information needed throughout the original and renewal application process, etc.

Additionally, because the licensee information will be in a single repository, all workflows for compliance, enforcement, and legal activities will be performed within the system to manage each case related to a licensee/permittee. Because of time and cost, TABC anticipates only a partial build-out of this overarching lifecycle management module with plans to request capital funding and authority to finish the build-out in the upcoming FY 2022-23 biennium.

## **2. Public Website Redesign Project**

Using the Texas.gov platform, TABC utilized a portion of this biennium funding to design a new public website that provides a fresh, modern look-and-feel to its online presence. This new website ([tabc.texas.gov](http://tabc.texas.gov)) went live on September 1, 2020. The agency will continue to look for opportunities to improve the website, but no further general revenue funds are needed for the improvements.

## **3. Enterprise Data Solution Project**

The remaining scope of the TABC Technology Transformation Initiative includes the development of a new Enterprise Data Solution that incorporates the Google Cloud Platform (GCP) within DCS as part of the overall solution. Pertinent non-criminal justice data will be synched between AIMS and GCP and utilized for business analytics using Google Analytics and for business intelligence using Tableau Software. These analytics and business intelligence will provide TABC the ability to make well-informed business decisions that are forward-thinking and data-driven in its approach.

### **Current Initiative Challenges**

- Creating and managing well-defined requirements for highly complex, inter-related functionality.
- Addressing needs related to transitioning away from years of disparate, outdated legacy systems.
- Development delays created by the extensive, albeit necessary, requirements-gathering process.

### **Anticipated Challenges**

- Full participation for a seamless transition of approximately 60,000 industry partners to the new system.
- Maintaining a workable cadence with adequate funding on the AIMS project into and throughout the next biennium.



# TEXAS ALCOHOLIC BEVERAGE COMMISSION

*Texans Helping Businesses & Protecting Communities*

P.O. Box 13127  
Austin, Texas 78711-3127  
(512) 206-3333  
[www.tabc.texas.gov](http://www.tabc.texas.gov)

- Maintaining legacy data and files in the legacy systems that are at or beyond end of support for approximately two to three years during the transition.
- Potentially not receiving adequate funding in the next biennium, which will force the agency to continue supporting and paying for its current legacy systems as well as ongoing expenses related to a partially implemented AIMS system and synchronization between it and the legacy systems.

## Strategy for FY 2022-23

This strategy assumes capital appropriation and authorization in the amount of \$6.5 million in the agency's LAR will be appropriated to finish the AIMS solution with applicable tie-ins finalized within the Enterprise Data Solution.

TABC will build out the agency's data management needs in line with the Department of Information Resources' Texas Data Management Framework. This scope will include needs for data governance, implementation of retention rules, cybersecurity, and criminal justice information.

The agency anticipates requesting capital funding and corresponding authority in FY 2024 and beyond, but on a much smaller scale to incorporate necessary functionality that is needed to implement new requirements set forth by statute or rule — or for general system upgrades as needed to minimize legacy issues as we move forward.

We appreciate the opportunity to provide this information to the committee. Please do not hesitate to contact us if you need additional information.

Sincerely,

A. Bentley Nettles  
Executive Director  
Texas Alcoholic Beverage Commission





# Texas Department of Criminal Justice's Information Technology (IT) and Cybersecurity Improvements and Modernization

*Interim Charge 2: Review the funding appropriated to state agencies for information technology (IT) and cybersecurity improvements and modernization. Evaluate the cost of ongoing IT and cybersecurity upgrades and the methodology for prioritizing projects.*

## Introduction

The Texas Department of Criminal Justice's (TDCJ) mission is to provide public safety, promote positive change in offender behavior, reintegrate offenders into society, and assist victims of crime. This mission has become increasingly reliant on information technology, thus increasing the risks associated with cybersecurity and lack of modern technology. All potential projects are first and foremost measured by their direct relationship with these two crucial factors. As for the methodology of prioritizing projects, consideration of how the project will impact the ability to achieve the Agency's mission, security risk, and sustainability of existing platforms is the primary criteria.

## Information Technology (IT) Initiatives

Following recommendations defined in the Legacy System Study (LSS) required by House Bill 2738, 83rd Legislature, the TDCJ Information Technology Division (ITD) established a modernization strategy to address the Agency's aging mission critical information systems. The strategy resulted in the successful upgrade of the Agency's desktop equipment, server hardware and operating software, development of the Texas Risk Assessment System (TRAS), and the transition to a centralized electronic document system, as funded by the 83rd Legislature. While these first steps were critical to the Agency's ability to stay secure and modern, it was only a small first step in the right direction.

	2016-17 <sup>1</sup> (84 <sup>th</sup> Leg)	2018-19 <sup>1</sup> (85 <sup>th</sup> Leg)	2020-21 <sup>1</sup> (86 <sup>th</sup> Leg)
<b>Computer and Software Acquisitions</b>	\$6,930,400	\$2,490,000	\$2,490,000
<b>Data Center Consolidation</b>	\$25,635,740	\$31,645,121	\$42,006,632
<b>Corrections Information Technology System<sup>2</sup> (SB 500, 86<sup>th</sup> Leg)</b>	\$0	\$0	\$24,164,000
<b>Totals</b>	<b>\$32,566,140</b>	<b>\$34,135,121</b>	<b>\$68,660,632</b>

<sup>1</sup>Excludes Board of Pardons and Paroles

<sup>2</sup>Accepted as part of the agency 5% reduction plan

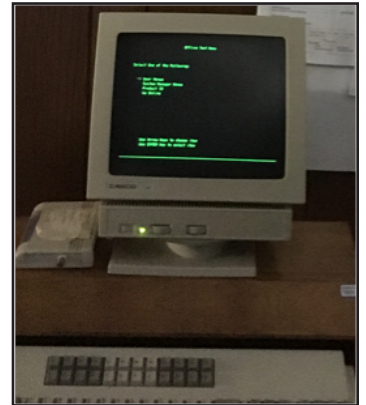
The Agency is continually using appropriated funding to keep information technology infrastructure up-to-date and secure. Ongoing initiatives include the Personal Computer Replacement Program (PCRP), ensuring end users have modern desktop technology therefore helping with cybersecurity. The Agency has been fiscally responsible by repurposing older, but still reliable PCs, and using them to replace green screen terminals currently still in use today, however these PCs are unable to interface with any modern technologies. ITD personnel evaluate the enterprise network infrastructure by identifying low bandwidth facilities and replacing and/or supplementing these with additional network capacity in an attempt to handle the increasing



## Texas Department of Criminal Justice's Information Technology (IT) and Cybersecurity Improvements and Modernization

technology needs of a correctional facilities system. The Agency participates in the Department of Information Resources (DIR) data center services contracts helping to ensure all network infrastructure is kept modern. The TDCJ is also taking advantage of DIR's managed application services contracts by obtaining technology related talent not available in the current organizational structure.

As technology use has expanded within the corrections field specifically, cybersecurity has become increasingly critical and challenging. Due to this, the TDCJ has used past and current appropriations to invest in enterprise-wide technologies such as Microsoft O365, application security scanning, Security Information and Event Management (SIEM) software, and risk assessment software. This investment in technology will ensure the cybersecurity protection of all Agency data and infrastructure, as well as staff, offender, victim, and public interests.



### Upgrading the Offender Management System

While current appropriated funds allow the TDCJ to maintain the current level of services being offered, there remains a significant gap to ensuring the secure, modern future of corrections in the State of Texas. At the very core of this discussion is the Agency's legacy offender management system that has been in service for over 40 years.



The system was developed in Common Business Oriented Language (COBOL), a programming language that at the time of development was the industry standard for performance, quality, and security. However, after 40 years the existing system is at the end of its useable lifecycle. The current application language, COBOL, is no longer offered in colleges and trade schools and 95% of the current COBOL programmers are "Baby Boomers" who are reaching the end of their careers. It is becoming increasingly difficult to support and secure the system as the COBOL staff rapidly leave the workforce. Currently, the COBOL support staff spend approximately 58% of their time maintaining the antiquated legacy system.



## Texas Department of Criminal Justice's Information Technology (IT) and Cybersecurity Improvements and Modernization

The current offender management system presents significant risks to TDCJ operations regarding sustainability, extensibility, and the tenets of information security, confidentiality, integrity, and availability. The existing system carries a high cost of ownership, is difficult to modify to meet ongoing business demands, requires a legacy skill set that fewer and fewer people possess, and does not adequately meet today's compliance demands. As such, the platform does not have the capability to use the latest functionality and security features available through modern technology. As the business needs of the Agency continue to drive toward the use of new tools, the current system's limited capabilities restrict the interface with products such as O365, remote collaboration systems, business analytics, real-time reporting, handheld technologies, and wireless availability. This limits the Agency's ability to provide the highest levels of technology related services and safety that staff, offenders, victims, and the public expect and deserve.

### Funding of Ongoing IT and Cybersecurity Upgrades

The next strategic step of the ITD Legacy Modernization Plan is focused on the mission-critical legacy offender management system used to process offenders at all phases of incarceration. The Agency began requesting funding for this initiative in the 85th legislative session and ultimately received the requested funding as part of the 86th legislative session.

Upon approval of the \$24.2 million project, the Agency began an aggressive preparation period by building a Request for Purchase, the associated legislative oversight documentation, as well as developing clear and concise process documentation to be prepared for a vendor engagement. The purchasing process resulted in the selection and subsequent Texas Board of Criminal Justice approval to contract with Microsoft, Inc. for the software and services needed to implement their Microsoft Digital Corrections Solution (MDCS), an "off the shelf" system. During this same time frame, the world was dealing with the Coronavirus (COVID-19) pandemic which led to economic instability. In May 2020, all state agencies were directed to submit a plan outlining a 5% reduction to the current FY 2020-21 biennial budget with specific exceptions related to critical government functions. The appropriation for the Corrections Information Technology System (CITS) was offered and accepted as part of this reduction plan. While this project is of the utmost importance, the Agency recognized the gravity of the situation while weighing the primary duty to provide public safety and offender rehabilitation. The Microsoft, Inc. contract was therefore not executed, and the Agency has begun the ongoing task of evaluating technology needs with or without additional funding.

Despite the loss of funding, the TDCJ remains steadfast in its primary job of ensuring the cybersecurity of all Agency assets. Part of the cybersecurity challenge will always be related to the availability of modern technologies. CITS remains the Agency's primary initiative to lay a modern, scalable, and versatile technology foundation for many years to come. CITS is crucial to meeting modern operational and governance needs, while also allowing the Agency to use the most current cybersecurity technologies available. Modernization is critical to the future needs of the people we serve.

The Agency continues to see rising costs in maintaining not only the code, but the mainframe systems that are significantly more costly than modern cloud technologies. The TDCJ will continue to seek funding for CITS through traditional legislative avenues as appropriate, all the while researching all other options that may arise to meet this critical need.





# TEXAS DEPARTMENT OF LICENSING & REGULATION

Executive Office • PO Box 12157 • Austin, Texas 78711 • (512) 463-3173 • Fax (512) 475-2874

[www.tdlr.texas.gov](http://www.tdlr.texas.gov)

September 30, 2020

## **House Appropriations Committee, Subcommittee on Infrastructure, Resiliency, & Investments Formal Request for Information – Charge Two**

During the 86<sup>th</sup> Session, the Texas Legislature appropriated funding to the Texas Department of Licensing and Regulation to develop a unified licensing system, an effort which will also improve and modernize the agency's information technology (IT) and cybersecurity capabilities. This was our top budget priority.

TDLR was the first agency to go through the Texas Department of Information Resources' (DIR) Application Development Decision Framework process (ADDF), which analyzed the current state of our licensing systems and provided an overall look at the various aspects that need to be considered for a major project: culture, finance, business, and technology.

Using this process, TDLR created a strategic plan for a new licensing system and DIR provided important feedback, resulting in a multi-year, two-phased approach. The plan will eliminate nine old computing systems entirely, eliminating those IT tools which no longer work for our agency and our licensees.

Phase I of the IT Licensing Transformation Project is on target to migrate 77% (or 546,000) of TDLR's individual and business licenses, by placing the Massage Therapist, Cosmetologist, Barber and Electrician programs in the new Texas Licensing System (TLS).

TDLR has selected a vendor through the competitive bid process. The vendor is employing the Agile methodology to develop the licensing system, along with a framework, and is working with our subject matter experts to fully understand the requirements and licensing needs for each program. Phase I includes not just the creation of TLS, but a critical educational element so that once the vendor is gone TDLR will be able to make changes to the system as needed in the future.

Lessons learned from the COVID-19 pandemic will be incorporated into the system, ensuring its agility to help respond to future events.

Phase II funding will:

1. Transfer the Towing and Vehicle Storage Facilities from the TOOLS system, which is built on PowerBuilder and difficult to work with, to the new system.
2. Transfer the Driver Education and Safety and Motorcycle and ATV Operator Safety programs, including the Parent-Taught Driver Education manual online ordering system and other older legacy systems, to the new licensing system.



# TEXAS DEPARTMENT OF LICENSING & REGULATION

Executive Office • PO Box 12157 • Austin, Texas 78711 • (512) 463-3173 • Fax (512) 475-2874

[www.tdlr.texas.gov](http://www.tdlr.texas.gov)

3. Transfer the Industrialized Housing and Buildings program from an antiquated Access software system to the new licensing system.
4. Transfer the Speech-Language Pathologists and Audiologists program, which will be the largest remaining program on Versa, to the new licensing system.
5. Develop an elevator permitting and inspections framework to include elevator inspector licensing, searches, and reporting of more than 56,000 elevator inspection reports from third-party inspectors.
6. Develop an inspection module for agency inspectors who perform more than 35,000 inspections a year and assist in routing optimization and risk-based inspection planning.

Once Phase II is complete, TDLR will be positioned to continue any system migrations in order to have one licensing system. In addition, agency staff will continue to modify and maintain TLS to meet changing business needs.

**Amazon Web Services**  
**Response to Formal Request on Interim Charge 2**  
**Texas House Appropriations Committee**  
**Infrastructure, Resiliency, and Investments**  
**September 30, 2020**

Amazon has more than 43,000 employees in the State of Texas. Amazon employees work in 17 fulfillment and sortation centers, ten delivery stations, four air hubs, and three corporate offices in Austin, Houston, and Dallas supporting multiple Amazon business units including Amazon Web Services (AWS), Kindle, Amazon Business, Amazon Prime Video, Whole Foods and others.

Just over 14 years ago, Amazon Web Services (AWS) began offering access to cloud-based infrastructure services based on Amazon's expertise in building and running highly scaled infrastructure and service-oriented software. Today, a vast range of organizations from the smallest start-ups to the largest enterprises and government agencies have taken advantage of this flexible, secure, cost-efficient, and highly efficient way of accessing IT resources.

Before the cloud, businesses and government agencies spent a lot of time and money managing their own datacenters and co-location facilities, and worrying about the security of their physical assets, which meant time *not* spent on their core organizational missions of providing products and services to their customers and citizens

With cloud, organizations in the public sector can focus on critical missions and access virtually unlimited and securable compute power at reasonable and predictable prices, without upfront hardware costs, technical debt, and the worry of defending against the full range of cyber threats. Previously, organizations only had an option of either making massive capital investments to build their own data center and server infrastructure, or of procuring long-term contracts with a vendor for a fixed amount of data center capacity that they might or might not use. Most troubling, organizations had to defend themselves against a complete range of nimble, evolving threats that were difficult to anticipate.

Today, AWS provides agility, cost-savings, and security benefits to millions of active customers in 180 countries, including more than 6,500 government agencies, 11,000 academic institutions and 29,000 nonprofit organizations, including the US Navy, the Department of Homeland Security, the National Geospatial Intelligence Agency, the Federal Aviation Administration, and NASA.

### **Commercial Cloud Efficiencies and Adoption**

Several years ago, there was a certain degree of reluctance to trust the so-called “public” or commercial cloud. This was understandable considering that any time a powerful new innovation appears in the IT industry, it takes time for users to understand and become comfortable with it.

But as customers and IT professionals have learned about the cloud and used its ever-increasing capabilities, organizations and governments at every level highlight how

commercial cloud service providers offer fundamental security *benefits* over traditional IT infrastructure. In fact, at the US federal level, President Trump highlighted the direct link between IT modernization and improving cyber security via his Executive Order in 2017.<sup>1</sup> The President's Executive Order states: "Effective risk management involves more than just protecting IT and data currently in place. It also requires planning so that maintenance, improvements, and modernization occur in a coordinated way and with appropriate regularity."

In May of 2020, the U.S. Government's Cyberspace Solarium Commission led by US Senator Angus King and US Representative Mike Gallagher drafted a white paper citing cybersecurity lessons from the COVID-19 pandemic.<sup>2</sup> Recommendation 4.5.1 in the report notes that the uptake of secure cloud services should be incentivized for state, local, and tribal governments in addition to small and medium sized businesses because the pandemic has produced new requirements that demonstrate the importance of digitizing critical services.

The report goes on to say that "Americans have increasingly relied on federal and state aid programs whose legacy systems have been stressed to the brink of failure...To survive future pandemics or catastrophic cyber incidents, the nation needs secure, remote access to reliable cloud services."

Furthermore, the integration of security policy and compliance with operational security is something that is seldom accomplished in traditional IT systems. Economies of scale also mean that cloud providers can develop and launch new services and security offerings faster than ever before.

Cloud computing is not an IT cure-all but it can be a big help. An organization's security benefits from the cloud provider taking on a major portion of the security "surface area" with continuous monitoring, automation, and logging, which allows customers to refocus their security efforts on a much smaller, more manageable part of the challenge. The cloud also allows for greater visibility into IT operations, giving insight into behavior and functioning of security issues, allowing for in-depth defense and better prevention. With proper planning and configuration, incident response and recovery is also easier and faster in the cloud. Finally, with cost-efficient access to massive amounts of storage and processing capability, our customers use the cloud to withstand many types of attacks and to provide faster remediation of issues when they occur.

In short, the commercial cloud and its inherent capabilities provide a unique opportunity to *enhance* systems security, privacy and cost-efficiency. Customers ranging from major banks to federal government agencies have told us repeatedly that they feel more secure hosting mission-critical and other sensitive data in the cloud than they do in their own data centers. The agility that modern systems like cloud offer provide organizations, especially the

---

<sup>1</sup> <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>

<sup>2</sup> <https://drive.google.com/file/d/1wCHVtIFlw84uZIPOTZe2nkdGau15fLAQ/view>

government, with the ability to move faster, with more capabilities, than the threat. In sum, we believe based on our experience with customers that security should no longer be seen as a *barrier* to cloud adoption, but an argument *in favor* of it.

### **Policy Recommendations for Texas to Take Full Advantage of the Cloud for Cybersecurity**

Across the globe, the cybersecurity threat remains a growing and evolving challenge. Nation-states are motivated to use cyber capacity and cyber tools to attack government data, networks, and systems. Cyber criminals can derive significant profits from their nefarious activities. With the rise of the Internet of Things, using compromised connected devices to launch distributed denial of service (DDoS) attacks are also becoming a common means of disrupting operations for the public and private sector. That said, most cyber breaches are still the result not of sophisticated attacks but of the failure to accomplish very basic security hygiene, such as patching known vulnerabilities in software, enforcing and rotating reasonable passwords, requiring the use of multi-factor authentication, properly configuring their systems when accessible from the Internet, enforcing least-privilege access, and failing to train and protect users from so-called phishing attacks.

Ransomware is malicious code designed by cyber criminals to gain unauthorized access to systems and data and encrypt that data to block access by legitimate users. Once ransomware has locked users out of their systems and encrypted their sensitive data, cyber criminals demand a ransom before providing a decryption key to unlock the blocked systems and decrypt data. If the ransom is not satisfied, organizations risk permanent destruction or public-facing data leaks controlled by the attacker.

Many government organizations are vulnerable due to a combination of shrinking budgets, perceived gaps in security resources, and legacy IT systems with unpatched vulnerabilities. The ransomware threat is serious but smart preparation and ongoing vigilance are effective counters against ransomware. The full armor of data security includes both human and technical factors but there are features of commercial cloud that helps to mitigate against ransomware attacks.

Based on our experience working with the public sector at all levels of government across many different countries around the world, we believe there are actions the Texas state legislature can take to accelerate IT modernization to take full advantage of cloud computing's security, cost-savings, and agility benefits.

In support of the state's strategic IT goals and the legislature's directives, the State of Texas has taken important steps forward to build upon. In 2016, under the leadership by Chair Nelson, the Texas legislature enacted a cloud first directive as part of SB 532. In 2018, HB 3875 authored by Chair Capriglione directed state agencies to ensure that future applications are architected to be cloud-capable. These laws move Texas agencies in the direction of IT modernization and enable greater cloud utilization.

In addition, the Texas Department of Information Resources (DIR) has been working to identify legacy systems and to make it easier for state agencies and local governments in Texas to modernize their IT and to move to the cloud with its reports, guidance, and support for state agencies through policies, security frameworks, and procurements, among other assistance.

AWS is one of several cloud providers offered through DIR's Data Center Services program to support workloads for a variety of State of Texas agencies.

Together, AWS and DIR have also developed a contract vehicle that enables state and local government customers to buy cloud services directly from the cloud service provider,<sup>3</sup> giving state agencies, higher education institutions, and local governments more options to access and utilize cost-effective agile cloud services.

The most important step forward in the effort to secure government communications networks and IT systems is through effective and lasting IT modernization. In the past, government has wrapped fragile security layers around inherently insecure legacy systems. In the private sector, IT modernization is happening because businesses of all sizes, and across all sectors of the economy, are adopting secure DevOps practices and moving their applications and workloads into the commercial cloud.

We hope that the state continues to build on the great work done by the legislature and DIR by enabling more flexible funding and spending models in support of legacy modernization to enhance cybersecurity.

Interim Charge 2 centers on funding appropriated to state agencies for information technology and cybersecurity improvements and modernization. There is a model to follow for additional cost-efficiencies and IT modernization advances. Congress passed and the President signed into law elements of H.R. 2227 the Modernizing Government Technology (MGT) Act authored by Congressman Will Hurd of Texas. Through the use of flexible funding, the MGT Act incentivizes federal agencies to reduce costs on IT *and* modernize aging legacy systems that are most at risk. Federal CIOs are now able to prioritize funding for system upgrades to take advantage of technologies such as commercial cloud, and to also bolster cyber defenses. We believe that states like Texas should look to this as a way to foster regular cycles of modernization of IT systems to lower costs, increase agility, and improve security.

In closing, while work still needs to be done to enable Texas agencies to fully benefit from the financial and security benefits that commercial cloud computing offers, significant progress has been made over the last several years through efforts by the legislature, DIR, and many state agencies. As result, the State of Texas is beginning to reduce costs, providing agencies more agility and flexibility in IT, and critically, is establishing a strong foundation to improve information security in service of all Texans. We should all work to encourage these efforts to modernize the state's IT systems to improve reliability, agility, costs and cybersecurity in Texas.

---

<sup>3</sup> <https://aws.amazon.com/contract-center/cloud-services-for-the-state-of-texas/>

September 30, 2020

House Appropriations Subcommittee on Infrastructure, Resiliency & Investment  
Dear Chair and Members of the Subcommittee,

Thank you for the hard work done by your members and consideration of the following submission on behalf of our company, Hughes Network Systems, relating to Interim Charge #2 on state agency information technology improvements

Hughes, known for its world-leading satellite network technology, applies its deep expertise in optimizing large and complex networks to include terrestrial network technologies to overcome obstacles faced by enterprises and government agencies. Hughes delivers managed wireline, wireless, and satellite broadband services to hundreds of commercial and government customers and has done so for over 15 years. Its approach is anchored by vast supply chain relationships with national and regional service providers that span the range of broadband technologies, such as cable, fiber, DSL, microwave, wireless (4G LTE), and its own market-leading High Throughput Satellite service. The company's HughesON™ managed network services provide complete connectivity solutions employing an optimized mix of satellite and terrestrial technologies and have already resulted in agencies achieving twice the bandwidth at prices between one-third to one-half the cost of dedicated service lines to field offices

### **The Background**

Government agencies are facing a daunting challenge: operating on legacy networks in an era of rapidly changing digital demands. In fact, 67% of federal IT professionals say their legacy network infrastructure is struggling to keep pace with the changing demands of Cloud and hybrid technologies. And 51% say their agency is failing to prioritize the networking aspect of Cloud adoption and overall IT modernization. These challenges are not unlike what IT professionals in other industries cite as critical issues: bandwidth costs, equipment maintenance and updates, and performance between locations.

Given these somewhat universal networking needs, is there a way for agencies to modernize and meet the network demands of today and tomorrow? Indeed, there is. It involves Managed Software Defined Wide Area Networks (SD-WAN). Already widely adopted and proven by commercial enterprises, Managed SD-WAN solutions offer agencies a clear path to network transformation that is proven today and future ready, including cloud readiness, robust branch security, and end-to-end optimization, with substantial performance improvements and cost savings over legacy networks.

### **Transitioning Without Transformation**

#### **Caution: Challenges Ahead**

Agencies have been caught off-guard by the amount of time needed to plan their network modernization and transformation as part of the transition. The challenge grows in magnitude for large distributed agencies with several locations as the larger the network, the more complex it is to manage and secure all endpoints. This creates a natural temptation to transition now, modernize later.

Let's look at the three primary challenges facing agency field offices in which transformation, or lack thereof, will impact: 1) bandwidth, 2) budget, and 3) security.

## **1. Don't Go Chasing Bandwidth**

The networks that many agencies currently have in place are no longer adequate to support today's application demands, particularly at the field office. Cloud technologies, video streaming, teleconferencing, and other bandwidth-hungry applications are congesting traditional telecom infrastructure – and the pressure shows no signs of letting up. Applications that once lived on the desktop now live on the Cloud or in a data center. Imagine building the Mall of America on a two-lane country road without expanding the surrounding road infrastructure in anticipation of higher traffic. That's essentially what happens with T1 lines tasked with carrying heavy Cloud-based application traffic.

As many as 81% of IT professionals expect their networks will require more bandwidth in the next three years. Government leaders understand that what they want to do moving forward is going to require significant amount of bandwidth and the days of annual budget increases to cover that connectivity are over.

A like-for-like network transition all but guarantees the continuation of bandwidth constraints and budget shortages. Networks that are already struggling to support field offices will find no relief without transforming now. Yet to transform, agencies do not need to scrap their existing MPLS networks. Rather, they can build upon what they have in place to create the more resilient, high-performing and Cloud-ready networks of the future. This is done by introducing managed broadband services with an intelligent on-premise routing device.

## **2. Busting Budgets**

Transitioning the same technology adds up to higher costs when compared to a smart network transition. With a like-for-like transition strategy, continuing to maintain an all-MPLS network to dispersed field offices becomes unsustainable due to the distance-sensitive pricing structure. The longer the line, the more expensive the service and access costs; bandwidth demands exceeding existing T1 capacity means adding more MPLS lines and quickly surpassing annual budgets.

Looking at the cost of MPLS T1 lines priced for government procurement (understanding that costs vary greatly by distance), agencies can conservatively expect to pay on average \$400–\$600 per month per line for a whopping 1.5 Mbps download speed. That is not even enough bandwidth to stream a single, standard 1080p HD video.

On the other hand, the average cost of a broadband access line to that same location would fall somewhere between \$100–\$250 per month and likely deliver 25 Mbps to 100 Mbps download speeds per line. For agencies with a number of locations, this becomes a tale of two very different budgets and two very different networks.

Such cost savings not only make broadband access more appealing, they also justify the provisioning of diverse dual-path access for greater network availability and higher application assurance at the field office.



### **3. Securing the Network of the Future**

While dedicated network technology, such as MPLS, delivers lower bandwidth levels to the field offices, it does offer a comforting level of security. Some agency leaders believe introducing broadband opens their networks to cyber hackers who target government agencies daily. This has led to some hesitation regarding transformation, causing some agencies to sacrifice network and application performance for trusted, dedicated network security.

A distributed, broadband network does pose risks. Apps like guest Wi-Fi and digital employee training invite users to access network infrastructure, increasing the risk of a security breach through Internet-based broadband circuits. Hackers often aim to exploit this to attack highly distributed organizations – Gartner estimates more than 30 percent of advanced threats target the distributed branch offices at the edge.

However, to prevent malicious network access, organizations implementing SD-WAN, leveraging broadband for explosive gains in bandwidth and performance, are implementing a proven strategy to offset the risk: an edge-centric security approach to intelligently secure each one of their hundreds or thousands of network endpoints.

#### **Transitioning with Transformation: How to Do Both**

##### **Transforming to Managed SD-WAN**

SD-WAN has now been considered the holy grail of organizational networks for several years. Early commercial enterprise adopters found that when implementing SD-WAN through a proven managed services provider (MSP), many of the complex planning stages, management and optimization processes, and evolving security landscape could be supported or automated by the MSP.

By executing network transformation to SD-WAN via an MSP, agencies can get access to multiple broadband services to most of their locations. This is critical because, if each site has an existing MPLS connection with a broadband access overlay, the MSP can use intelligent routers to prioritize application traffic based on automated policy rules programmed within each branch device. Organizations are better off outsourcing this level of effort to an MSP rather than trying to replicate these capabilities in-house, given the amount of time and resources it would require.

Agencies should take a simpler approach to transforming. Rather than mapping out and designing an entire modernized network under a statement of work to find the most cost-effective provider, agencies can gather the location-by-location SLAs and list them in a statement of objectives. This allows the MSP's network engineering experts to bring forth creative, efficient and lower-cost solutions to allow the agency to pursue the best architecture for the network they need.

##### **Where to Begin: At the Edge with Hybrid Networking**

The biggest opportunity for network transformation for state government agencies exists at the network's edge, where the agency interacts with the citizen and the mission is largely fulfilled. When budgets are tight, it is at the edge that the transformation process imparts the greatest impact.

An edge-first transformation plan provides an outside-in approach that agencies can execute faster and more easily, with minimal operational interruption -- especially when implemented as part of a managed service. By delivering managed broadband services to field offices and automating network traffic using an advanced SD-WAN router, field offices can get the secured bandwidth they need from multiple paths of connectivity. Creating a hybrid architecture -- by adding managed broadband services to existing MPLS networks -- effectively transforms and modernizes agency endpoints in relatively short order.

It's important to note that transition under this edge-first, hybrid approach does not impact the core of an agency's network where most of the existing technology is adequate. Strategically, this approach saves the core to be the last piece of the network to transform, enabling a well-calculated and least-disruptive evolution.

### **Transforming Security**

Accounting for robust security when transforming the agency network is paramount. Fortinet, whose industry leading firewall technology is integrated with Hughes routers, conducted research that indicates 90% of SD-WAN solutions employ only basic security with a stateful firewall. A responsible approach to SD-WAN security mitigates risk while realizing the vast benefits of a Cloud based enterprise network.

An edge-based approach to security creates an inherently distributed security model, removing the risk of a significant breach resulting from a single point-of-failure. Failure within any site or application can result in a major outage. Because edge security is enforced locally at various points in the network, risk is mitigated. Placing security closest to the vulnerabilities also allows scrubbing traffic that is wholly local to the site or which travels from site-to-Internet. This kind of east-west traffic can include anything from gift shop POS transactions to security camera feeds in a sensitive environment. Edge security, on the other hand, scrubs data in both directions, ensuring that bad information or data is kept away from the site and any information that should be protected is either prevented from leaving or secured before it is sent.

Edge-first transformation and security using HughesON Managed SD-WAN is already in place at several federal government cabinet agencies. These agencies were proactive and diligent in their planning -- vetting, testing and examining security and implementation plans and approving the network and security upgrades for hundreds of endpoints. As part of the Hughes proposal, a System Security Plan (SSP) was included; it is updated regularly as the network evolves to ensure the agency field offices remain fully secured from network threats.

### **The Results are Real**

#### **Rapid SD-WAN Adoption Underway**

Transformation that includes SD-WAN moves an agency into a better position to achieve its mission by increasing network availability and application assurance all the way to the edge. There are powerful and proven tools at each agency's disposal that retailers and multi-site enterprises have benefited from for years, including big data analytics, video training, and Cloud storage. Among enterprise organizations, SD-WAN is the dominant networking solution. For agencies without a purpose-built

network to support critical operational functions at every location, application technology will go underutilized--or worse, unused altogether--resulting in additional wasted resources.

Hughes has worked with many government agencies and commercial enterprises to tackle network transformation challenges. To date, Hughes manages more than 30,000 SD-WAN endpoints globally. Several agencies enabled effective network transformation in a concerted effort to save money and optimize network performance immediately. These agencies developed performance objectives for field offices and supplemented dedicated lines with secure managed broadband circuits. On average, these field offices doubled their total throughput and at a third of the recurrent service costs for their legacy technology

#### **Reminder: Transformation Is a Process**

Network transformation is a process; it is not an event. The hybrid network architecture at the edge makes for an ideal phased approach for agencies, leveraging both broadband and existing MPLS transport technologies.

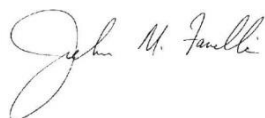
Instead of replacing one network for another, the most effective transformations build upon existing infrastructure as a foundation, enhancing the existing MPLS network with the addition of secure, managed broadband lines and intelligent software-based orchestration of automated multi-path networking. By delivering high-application availability, this approach ends application buffering and choppy VoIP calls and can be fully managed 24/7 by a proven, trusted provider.

Using a single source for network operations centers (NOCs) and security operations centers (SOCs) assures the agency of accountability and coordination across the network, regardless of how many or how widespread the locations. Moreover, a single MSP frees the agency's network team from juggling dozens of agreements across multiple carriers with different terms, conditions, and support channels.

The roadmap to network transformation needs to start now and at the edge with managed SD-WAN solutions that can grow and evolve to meet the agency's network demands -- today and tomorrow.

Thank you for hard work for the State of Texas and for your consideration. Please don't hesitate to reach out for any questions or clarifications I can provide as the subcommittee completes their interim work.

Sincerely,



John Fanelli

Senior Director – Government Solutions  
Hughes Network Systems  
11717 Exploration Lane  
Germantown, MD  
301-548-1953  
[John.fanelli@hughes.com](mailto:John.fanelli@hughes.com)

HOUSE APPROPRIATIONS  
SUBCOMMITTEE ON INFRASTRUCTURE,  
RESILIANCY, AND INVESTMENTS

MIKE SCHROEDER

43 Rainey St, #3003  
Austin, TX 78701  
mike.schroeder@rubrik.com  
512-970-4234

September 29, 2020

Subject "SIRI"

Dear House Appropriations Subcommittee,

Thank you for your leadership and work done by all committee members to ensure the security and availability of online services during this pandemic. We at Rubrik are pleased to submit the following comments regarding the House Appropriations Subcommittee Interim Charge 2, specifically the portion of the Charge tasking the Committee with monitoring the funding of cybersecurity upgrades and modernization, which strengthens the state's online infrastructure against ransomware attacks. Over the past few years many of our Texas institutions have been attacked by cybercriminals utilizing ransomware to encrypt or delete data and backups of that data and demand ransom payments to restore data. There has been a 72% increase in ransomware attacks since the COVID-19 pandemic began targeting our country's state agencies as evidenced by the recent attacks of TxDOT and the Office of Court Administration this year. The FBI also lists a well-timed ransomware attack as one of the biggest threats to our election process for 2020. Gartner has named Rubrik as the leader, with the most completeness of vision in the June 2020 Backup and Recovery Magic Quadrant report citing our Ransomware Protection and Remediation as the main reason. Please consider the attached submission as part of your strategy in support of Interim Charge 2, to provide the funding to protect our state agencies and provide a last line of defense in the event that a ransomware attack occurs.

Sincerely,

Michael Schroeder

# Rubrik For Ransomware Remediation

## Faster Ransomware Recovery From Backups That Cannot Be Compromised

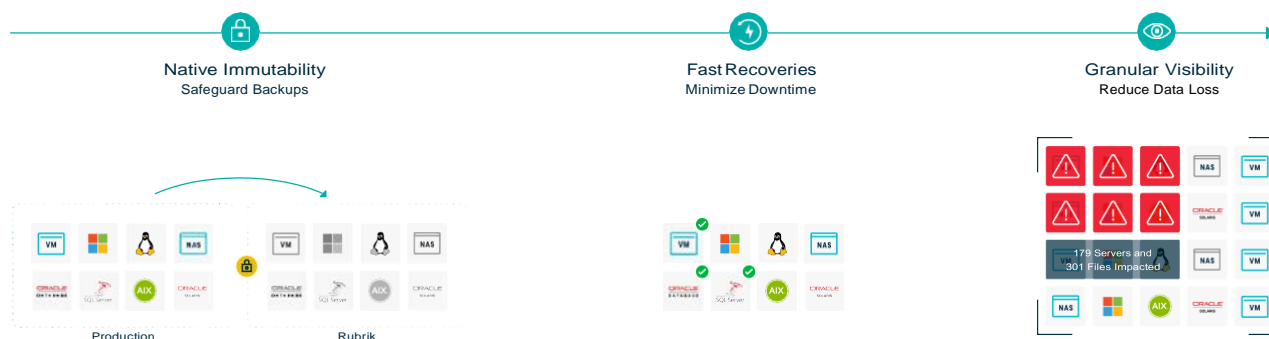
With ransomware attacks continuing to rise, organizations are often forced to trade-off paying the ransom with costly downtime. Even with defense mechanisms in place, extortionists continue to find new mechanisms to encrypt organizations' data.

Backups are one of the most – if not the most – important defense against ransomware. But if subject to corruption, attackers will use it against you. Advanced ransomware is now targeting backups – modifying or completely wiping them out. The importance of cyber resiliency and the need for faster ransomware recoveries from immutable backups that cannot be compromised is more important than ever.

### OUR APPROACH

Often, recovering from a ransomware attack can be complex and time-consuming. Identifying the scope of the attack, locating the most recent clean data, and recovering quickly – all while ensuring your backups have not been deleted or encrypted – can be a significant investment for any organization.

With Rubrik, all of your data is stored in an immutable format, preventing ransomware from ever accessing and encrypting your backups in the first place. In the event of an attack, Rubrik provides fast recovery to the most recent clean state, granular visibility into the scope of the attack, and can alert you to unusual behavior leveraging machine learning.



### NATIVE IMMUTABILITY TO SAFEGUARD BACKUPS

Ensure backups are not compromised by ransomware through built-in immutability. Data managed by Rubrik is never available in a read/write format and cannot be read, modified, or deleted by an external malicious actor.

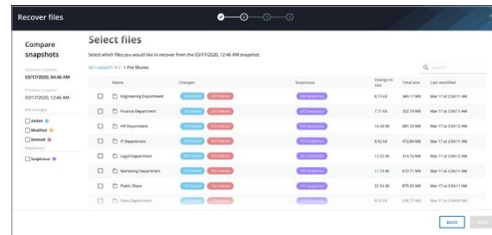
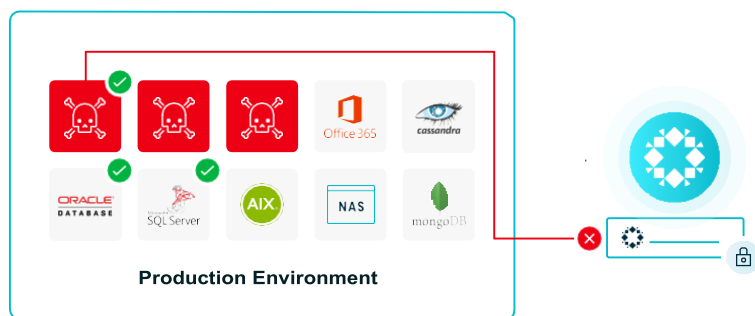
### FAST RECOVERIES TO MINIMIZE DOWNTIME

Easily identify the most recent clean version of data and enable instant, file-level recoveries with Rubrik Live Mount. Plug into automation frameworks such as ServiceNow Incident Response with Rubrik RESTful APIs to further increase operational efficiency.

### GRANULAR VISIBILITY TO REDUCE DATA LOSS

Quickly identify which applications and files were impacted through intuitive data visualizations and roll back with file-level granularity. Minimize the risk of data loss associated with mass restores that include uncompromised data.

## HOW IT WORKS



## KEEP YOUR BACKUPS SAFE

Rubrik combines an immutable filesystem with a zero-trust cluster design in which operations can only be performed through authenticated APIs. This means that once data is written it cannot be read, modified, or deleted. Other data management systems tend to use general-purpose storage that leverages standard protocols such as NFS and SMB. This can leave your backup storage system vulnerable to ransomware.

## RECOVER WITH NEAR-ZERO RTOS

Rubrik's Live Mount delivers near-zero RTOs to accelerate data access for instant recovery. Users can browse and recover files, objects, and tables from VMs as well as physical SQL Server and Oracle databases. Rubrik's Cloud-Scale File System has built-in zero-byte cloning capabilities that minimize storage consumption while allowing any number of mounts to be created.

## UNDERSTAND SCOPE OF DAMAGE

Once you have detected an attack, Polaris Radar compares the post-attack snapshot with the snapshot immediately before to see what was added, deleted, or modified. Rubrik exposes the analysis in the management console, so you can see exactly the scope of the damage, what you need to recover, and where encrypted files are located with file-level granularity. Rubrik can also apply machine learning on application metadata to alert you of unusual activity.

## WHAT OUR CUSTOMERS ARE SAYING

"We were hit with a ransomware attack in June that infiltrated our environment and began encrypting data, rendering it unusable. Rubrik helped us quickly recover 100% of the systems it was protecting."



Craig Witmer  
Chief Technology Officer

"One of the reasons we purchased it [Rubrik] was because it was a backup system that could not be consumed by ransomware."



Kerry Goode  
Chief Information Officer  
and Director of Technology Solutions



Global HQ  
1001 Page Mill Rd., Building 2  
Palo Alto, CA 94304  
United States

1-844-4RUBRIK  
inquiries@rubrik.com  
[www.rubrik.com](http://www.rubrik.com)

Rubrik, the Multi-Cloud Data Control™ Company, enables enterprises to maximize value from data that is increasingly fragmented across data centers and clouds. Rubrik delivers a single, policy-driven platform for data recovery, governance, compliance, and cloud mobility. For more information, visit [www.rubrik.com](http://www.rubrik.com) and follow @rubrikInc on Twitter. © 2020 Rubrik. Rubrik is a registered trademark of Rubrik, Inc. Other marks may be trademarks of their respective owners.