SmartSuite

Framework / Cybersecurity / Other

Texas Cybersecurity Act (HB 8, 2017), Texas Government Code Chapter 2054

The Texas Cybersecurity Act (HB 8, 2017) amended Government Code chapter 2054 to require state agencies to file security plans, assessments and 48-hour incident notices with DIR.



What it is

The Texas Cybersecurity Act is House Bill 8 of the 85th Texas Legislature (Acts 2017, chapter 683), the law that amended Government Code chapter 2054 so that every Texas state agency must plan, assess, test and report its information security to the Department of Information Resources (DIR). The Governor signed it on June 12, 2017, it took effect on September 1, 2017 (Section 18), and the chapter 2054 sections it created have since been amended by the 86th, 87th and 88th Legislatures.

At a glance

PUBLISHER
Texas Legislature (Government Code chapter 2054); administered by the Texas Department of Information Resources (DIR)

TYPE
Regulation

VERSION
HB 8 (2017, Acts ch. 683), Government Code chapter 2054, as amended through the 88th Legislature (2023)

EFFECTIVE
September 1, 2017

DOMAIN
Cybersecurity

FAMILY
Other

REGION
Texas

INDUSTRY
Government & Public Sector

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
Medium

Source: statutes.capitol.texas.gov/Docs/GV/htm/GV.2054.htm

Why it matters

- **Named accountability** Section 2054.133(e) requires a written statement signed by the head of the agency, the chief financial officer and each designated executive manager that they have been made aware of the risks revealed while preparing the information security plan.
- **A fixed filing calendar** The information security plan is due June 1 of even-numbered years (2054.133(c)), the biennial data security plan on the same date (2054.516(a)(1)), the security assessment report by December 1 of the assessment year or within 60 days of completion (2054.515(b)) and contractor training reports by August 31 each year (2054.5192(e)).
- **Confidential filings** The information security plan (2054.133(d)) and the assessment report with its documentation (2054.515(d)) are confidential and exempt from disclosure under the Public Information Act, chapter 552.
- **A 48-hour incident clock** A state agency or local government holding sensitive personal, confidential or legally regulated information notifies DIR, including the chief information security officer, within 48 hours of discovering a breach, suspected breach or ransomware incident (2054.603(b)(2)), then files a cause analysis within 10 business days of eradication, closure and recovery (2054.603(c)).

 © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports TCSA Ch. 2054

Information Security Plan Workspace

Draft and periodically update the 2054.133 plan as a record set: vulnerability report inputs, chapter 2059 services, staff responsibilities, risk measures, DIR best practices or the written explanation, and the signed executive acknowledgment, with the June 1 filing date tracked.

Biennial Security Assessment

Run the 2054.515 assessment of systems, networks, data storage, security measures, vulnerabilities and the data governance program as a scheduled assessment with findings, owners and the report to DIR.

Application Data Security Plans

Register every website and mobile application that processes sensitive personal or confidential information, attach its 2054.516 data security plan and its vulnerability and penetration test, and track remediation of each finding.

Training Completion Tracking

Record annual DIR-certified training for the employees and officers identified under 2054.5191 and for contractors under 2054.5192, with completion percentages ready for DIR's verification form and the August 31 contractor report.

48-Hour Incident Notification

Log a breach, suspected breach or ransomware incident with its discovery time, the 48-hour DIR or Secretary of State notice, Business and Commerce Code 521.053 consumer notices and the 10-business-day cause analysis under 2054.603.

Legacy System Remediation Plan

Maintain the 2054.575 plan: exposure-reduction procedures for personal information on legacy systems, the modernization or disposal approach for each system and the workforce certification analysis.

Common framework mappings

CIS Controls v8.1 · CJIS Security Policy · COBIT 2019 · FedRAMP Rev. 5 · FERPA · GLBA Safeguards Rule (16 CFR Part 314) · HIPAA · ISO 27001:2022 · NIST CSF 2.0 · NIST 800-53 Rev.5

Official resources

HB 8 (2017), enrolled text

The enrolled Texas Cybersecurity Act as passed by the 85th Legislature, with every section of Government Code chapter 2054 it added or amended.

capitol.texas.gov/tlodocs/85R/billtext/html/HB00008F.htm

HB 8 (2017), bill history

Texas Legislature Online's history of HB 8, showing the Governor's signature on June 12, 2017 and the September 1, 2017 effective date.

capitol.texas.gov/BillLookup/History.aspx?LegSess=85R&Bill=HB8

Texas Government Code Chapter 2054

The current text of chapter 2054, Information Resources, including sections 2054.133, 2054.515 to 2054.518, 2054.519 to 2054.5192 and 2054.603.

statutes.capitol.texas.gov/Docs/GV/htm/GV.2054.htm

Texas Administrative Code: Information Security Standards

Official legal text outlining information security standards for Texas state agencies.

texreg.sos.state.tx.us/public/readtac%24ext.ViewTAC?tac_view=5&ti=1&pt=10&ch=202&sch=B&rl=Y

Frequently asked questions

What did the Texas Cybersecurity Act (HB 8) actually change?

HB 8 (85th Legislature, Acts 2017, chapter 683) amended Government Code chapter 2054. It added section 2054.0594 (the information sharing and analysis organization), made the biennial vulnerability report in 2054.077 mandatory, put a 48-hour breach notice to DIR into the statute (now 2054.603), rebuilt the cybersecurity council in 2054.512, added the signed executive risk acknowledgment to the information security plan in 2054.133(e), and added sections 2054.515 to 2054.518 covering the biennial security assessment, data security plans for websites and mobile applications and DIR's statewide risk and incident plan. It took effect September 1, 2017.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

When is the information security plan due, and who signs it?

Under section 2054.133(c) each state agency submits its information security plan to DIR by June 1 of each even-numbered year. Section 2054.133(e) requires the plan to include a written statement, signed by the head of the agency, the chief financial officer and each designated executive manager, that they have been made aware of the risks revealed while the plan was prepared. The plan is confidential under 2054.133(d).

How quickly must a Texas state agency report a security incident?

Section 2054.603(b) requires a state agency or local government to notify DIR, including the chief information security officer, within 48 hours of discovering a security incident, or the Secretary of State if the incident involves election data. A security incident means a breach or suspected breach of system security under Business and Commerce Code 521.053 or the introduction of ransomware. Within 10 business days of eradication, closure and recovery the agency files the details and an analysis of the cause (2054.603(c)).

Who has to complete cybersecurity training under chapter 2054?

Section 2054.5191 requires state employees who use a computer for at least 25 percent of their duties, and every elected or appointed officer of the agency, to complete a DIR-certified cybersecurity training program once a year; local governments apply the same rule to their employees and officials with access to a computer system or database. Section 2054.5192 requires contractors with access to a state system to complete certified training during the contract term, reported to DIR by August 31 each year. DIR certifies at least five programs annually under 2054.519.

Does the Act apply to local governments, universities and school districts?

Partly. Local governments carry the 48-hour security incident notification in 2054.603, the annual training requirement in 2054.5191(a-1) and may join regional cybersecurity working groups under 2054.0594(d). Institutions of higher education follow the website and mobile application security procedures in 2054.517 and take part in the information sharing and analysis organization. School districts are governed instead by Education Code section 11.175 (TX SB 820), and section 17 of HB 8 excludes the Electric Reliability Council of Texas.

License included / downloadable: Yes The Texas Cybersecurity Act and Government Code chapter 2054 are Texas state law, published free on Texas Legislature Online and the Texas Statutes site; the platform links to the enrolled bill and the current chapter text.

Full framework page and mappings: smartsuite.com/frameworks/us-texas-cybersecurity-act-state-cybersecurity-governance-requirements