INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-19 18:59 UTC

Texas Government and Third-Party Ecosystems Under Sustained Attack: 3M+ Records Exposed in Vendor Breach Pattern

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0183
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Texas Parks and Wildlife Department (TPWD), unnamed third-party license system vendor; 3.08 million hunting and fishing license holders
Published	2026-06-19T12:12:41
Discovery Source	Rss

Executive Summary

A third-party vendor breach at Texas Parks and Wildlife Department exposed personally identifiable information for approximately 3.08 million hunting and fishing license holders, including driver's license numbers, passport numbers, and contact information. This incident extends a documented 30-month pattern of successful attacks against Texas government entities and their vendor ecosystems, signaling a systemic third-party risk management failure rather than an isolated event. The exposed dataset creates direct downstream risk for identity fraud, targeted phishing, and credential stuffing campaigns against affected citizens and any organizations they interact with.

Technical Analysis

The breach originated at an unnamed third-party license management system vendor contracted by TPWD. No CVE has been assigned; this is a governance and process failure rather than a discrete software vulnerability. Exposed data confirmed by TPWD includes driver's license numbers, passport numbers, and contact information. Social Security numbers and financial account data were not confirmed compromised. CWE mapping: CWE-359 (unauthorized PII exposure), CWE-284 (improper access control at the vendor layer), CWE-693 (third-party protection mechanism failure), CWE-778 (insufficient logging, likely contributing to delayed detection). MITRE ATT&CK probable activity: T1190 (initial access via public-facing application at the vendor), T1078 (valid accounts), T1213 (data from information repositories), T1048 (exfiltration over alternative protocol). The vendor's identity remains undisclosed, constraining supply chain visibility and limiting the ability of

downstream organizations to assess shared exposure. This incident is contextually linked to a broader Texas government vendor breach pattern including INC Ransom against the State Bar of Texas (April 2025), Play ransomware against Dallas County (October 2023), and ShinyHunters/UNC6395 against TransUnion via Salesforce (July 2025). No patch or vendor advisory is applicable; remediation is procedural and contractual.

Action Checklist

1. Step 1: Containment, Identify all third-party vendors in your environment that hold citizen or employee PII under government contracts. Verify whether any of those vendors also service Texas state agencies or share platform infrastructure with the unnamed TPWD vendor. Suspend data-sharing with any vendor that cannot confirm its incident status (NIST IR-6: Incident Reporting; CIS 1.1: Maintain Enterprise Asset Inventory inclusive of vendor data holders).
2. Step 2: Detection, Review vendor access logs for anomalous data egress patterns over the past 90 days: large bulk exports, off-hours queries against license or PII tables, API calls originating from unexpected IP ranges. Cross-reference AU-2 (Event Logging) to confirm your contracts require vendors to retain and share these logs. If vendor logs are unavailable, treat the gap as a confirmed control failure and escalate (CIS 8.2: Collect Audit Logs).
3. Step 3: Eradication, Enforce contractual data minimization requirements: vendors should hold only the PII fields operationally required, for only the duration required (CWE-284 / NIST AC-3: Access Enforcement; NIST AC-6: Least Privilege). Require the TPWD vendor, and all analogous vendors in your portfolio, to provide a written attestation of current access control configurations, MFA enforcement on administrative accounts, and encryption at rest status. Vendors that cannot attest within 72 hours should be moved to elevated monitoring.
4. Step 4: Recovery, Validate that your vendor contracts include mandatory breach notification timelines, audit rights, and the right to independently verify security controls (NIST AC-20: Use of External Systems). For any vendor confirmed to share infrastructure with the TPWD breach, request forensic attestation before resuming full data-sharing. Monitor for downstream indicators: spikes in phishing attempts targeting your organization using PII consistent with the exposed fields (driver's license numbers, passport numbers) as social engineering hooks.
5. Step 5: Post-Incident, Conduct a third-party risk review using this incident as a trigger case. Map every vendor that holds PII to a risk tier; verify that Tier 1 vendors (high PII volume, government data) have been assessed within the past 12 months (NIST AC-20; CIS 7.1: Vulnerability Management Process). Implement D3-UAP (User Account Permissions) and D3-MFA (Multi-factor Authentication) requirements as mandatory contract terms for new and renewing vendors. Address CWE-778 gaps by requiring vendors to contractually guarantee log retention of no less than 90 days with audit access on demand (NIST AU-11: Audit Record Retention; NIST AU-9: Protection of Audit Information).

IR / Forensic Enrichment

Triage Priority	URGENT

Escalation Criteria	Escalate immediately to legal counsel and executive leadership if any vendor in your portfolio confirms shared infrastructure with the TPWD breach vendor, if PII record counts exposed exceed your state's mandatory breach notification threshold under Texas Business & Commerce Code §521 or equivalent applicable law, or if vendor log unavailability prevents determination of whether your organization's citizen or employee data was accessed.
Recovery Notes	Before resuming data-sharing with any suspended vendor, require a written forensic attestation from a qualified third party confirming that the specific license system platform has been remediated and that no unauthorized access to your organization's data occurred. Monitor inbound phishing attempts, helpdesk social engineering reports, and identity-based fraud indicators — particularly those referencing driver's license or passport numbers consistent with the exposed TPWD fields — for a minimum of 90 days post-incident, as threat actors routinely weaponize breached government PII in follow-on campaigns targeting the same victim population. Update your third-party vendor risk register within 30 days to reflect findings from this incident and schedule Tier 1 vendor reassessments on a 12-month recurring cadence.
Forensic Artifacts	Vendor API gateway or web server access logs (90-day window): filter for requests to hunting and fishing license PII endpoints returning anomalously large response payloads or bulk record counts, originating from IP addresses outside the vendor's declared network ranges — the primary indicator of unauthorized bulk data extraction from a license system. | Database audit logs for the license management system: query logs recording SELECT statements against tables containing driver_license_number, passport_number, date_of_birth, and contact fields, attributed to vendor service accounts — the field-level access record needed to determine exactly which PII was accessible and potentially exfiltrated. | Identity provider and IAM logs for vendor service accounts: authentication events, MFA bypass records, privilege escalation events, and last-access timestamps for all accounts with access to the PII dataset — reveals whether attacker access used compromised vendor credentials or exploited a misconfigured service account. | Outbound NetFlow or firewall egress records: data-volume telemetry on connections from the license system environment to vendor IP ranges or unexpected external destinations, correlated with timestamps of anomalous database queries — quantifies the potential data transfer volume and supports breach scope estimation for regulatory notification. | Inbound phishing and fraud indicators post-disclosure: email gateway logs, helpdesk tickets, and identity fraud reports referencing driver's license numbers or passport numbers from the exposed TPWD population — documents downstream weaponization of the breached PII and informs affected-individual notification scope.

Per-Action IR Details

Step 1: Containment — Identify all third-party vendors in your environment that hold citizen or employee PII under government contracts. Verify whether any of those vendors also service Texas state agencies or share platform infrastructure with the unnamed TPWD vendor. Suspend data-sharing with any vendor that cannot confirm its incident status (NIST IR-6: Incident Reporting; CIS 1.1: Maintain Enterprise Asset Inventory inclusive of vendor data holders).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-20 (Use Of External Systems), NIST IR-4 (Incident Handling), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Export your procurement or contract management system to a spreadsheet and cross-reference vendor names against Texas DIR (Department of Information Resources) registered vendors and any publicly named TPWD technology partners. Use a shared Google Sheet or Notion board to track vendor confirmation status, assigning one analyst to phone/email outreach and one to document responses. Suspend API keys or SFTP credentials for

non-responding vendors by disabling the service account in Active Directory: `Disable-ADAccount -Identity `.

Evidence: Before suspending data-sharing or revoking vendor credentials, capture: (1) current active sessions or API tokens issued to each vendor from your identity provider or API gateway logs — export as CSV with timestamps; (2) the last 90 days of data-transfer logs (SFTP transfer logs, API call logs, or database query logs) showing volume and field-level access by each vendor service account; (3) a point-in-time snapshot of vendor service account permissions from your IAM system. These records establish the pre-containment data-sharing baseline and are essential for breach scope determination and regulatory notification.

Step 2: Detection — Review vendor access logs for anomalous data egress patterns over the past 90 days: large bulk exports, off-hours queries against license or PII tables, API calls originating from unexpected IP ranges. Cross-reference AU-2 (Event Logging) to confirm your contracts require vendors to retain and share these logs. If vendor logs are unavailable, treat the gap as a confirmed control failure and escalate (CIS 8.2: Collect Audit Logs).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-11 (Audit Record Retention), CIS 8.2 (Collect Audit Logs)

Compensating: If your organization owns the database or API layer that feeds the vendor, run the following against your own query logs to surface bulk PII extraction patterns: for PostgreSQL/MySQL, query the slow-query or general log for SELECT statements joining on driver_license, passport_number, or contact fields returning row counts above your defined bulk threshold (e.g., >10,000 rows). For API gateways without a SIEM, pull access logs and run: `awk '{print $1, $7, $9}' access.log | sort | uniq -c | sort -rn | head -50` to rank top IPs by request volume. Flag calls to license or PII endpoints from IPs outside your vendor's declared CIDR ranges. Document every log gap as a formal control deficiency finding.

Evidence: This is a detection and analysis step — it does not alter live state and does not require prior volatile capture. Evidence to collect and preserve during this step: (1) vendor API gateway logs or web server access logs showing requests to hunting/fishing license PII endpoints, filtered for bulk query patterns (row counts, response payload sizes) over the 90-day window; (2) database audit logs (if accessible) recording SELECT queries against tables containing driver_license_number, passport_number, and contact_info fields, with originating application user or service account identity; (3) NetFlow or firewall egress logs showing data volumes transferred to vendor IP ranges, particularly during off-hours windows; (4) authentication logs for vendor service accounts showing logon times, source IPs, and MFA compliance status. Absence of any of these log sources is itself a material finding — document the gap with timestamp and escalate per your third-party risk policy.

Step 3: Eradication — Enforce contractual data minimization requirements: vendors should hold only the PII fields operationally required, for only the duration required (CWE-284 / NIST AC-3: Access Enforcement; NIST AC-6: Least Privilege). Require the TPWD vendor — and all analogous vendors in your portfolio — to provide a written attestation of current access control configurations, MFA enforcement on administrative accounts, and encryption at rest status. Vendors that cannot attest within 72 hours should be moved to elevated monitoring.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 3.3 (Configure Data Access Control Lists), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For vendors where you control the data schema or data-sharing feed: immediately audit the field list in any outbound data extract or API response payload and remove PII fields not required for the vendor's stated function (e.g., strip passport_number from license validation feeds if the vendor only requires license status). Use `diff` or a schema comparison script to compare current field exports against the original data-sharing agreement. For MFA attestation collection, issue a structured questionnaire via encrypted email with a 72-hour deadline, and track responses in a shared incident log. Vendors with no response escalate to vendor suspension per Step 1.

Evidence: Before enforcing data minimization changes or revoking vendor data access: (1) capture the current schema of all data exports or API payloads sent to the vendor — take a production sample (anonymized or hashed) to document exactly which PII fields are currently exposed; (2) export the current access control configuration for vendor service accounts from your IAM or database permission system (e.g., `SHOW GRANTS FOR 'vendor_user'@'%';` in MySQL) — this preserves the pre-remediation state for regulatory and legal review; (3) snapshot vendor account last-access timestamps and MFA enrollment status before any account modifications. These records document the exposure scope and establish that remediation was applied after the baseline was captured, not before.

Step 4: Recovery — Validate that your vendor contracts include mandatory breach notification timelines, audit rights, and the right to independently verify security controls (NIST AC-20: Use of External Systems). For any vendor confirmed to share infrastructure with the TPWD breach, request forensic attestation before resuming full data-sharing. Monitor for downstream indicators: spikes in phishing attempts targeting your organization using PII consistent with the exposed fields (driver's license numbers, passport numbers) as social engineering hooks.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-20 (Use Of External Systems), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For phishing detection without a commercial email security platform: configure mail flow rules in Exchange/M365 or Postfix to flag inbound messages referencing known exposed data patterns (e.g., messages containing 'license renewal' or 'passport verification' combined with sender domains not on your allowlist). For a 2-person team, set a daily 15-minute review of quarantined messages and publish a one-page staff alert describing the specific social engineering risk: attackers may reference recipients' hunting/fishing license details or driver's license numbers to establish false legitimacy. Log all flagged messages and forward to your threat intelligence contact. For forensic attestation of vendors, use a structured security questionnaire aligned to CIS Controls v8 IG1 as a minimum baseline.

Evidence: Before resuming full data-sharing with any suspended vendor: (1) obtain and review the vendor's forensic attestation or third-party IR report confirming the breach scope, affected systems, and remediation actions taken — validate that the license system platform your data transits is explicitly addressed; (2) collect and baseline inbound phishing attempt volumes from your email gateway or mail logs for the 30 days prior to breach disclosure, to establish a pre-event rate for anomaly detection post-recovery; (3) document all contract terms reviewed during this step (notification timelines, audit rights clauses) with the version and date of each contract — this record supports regulatory compliance demonstration if Texas breach notification law (Texas Business & Commerce Code §521) obligations are triggered.

Step 5: Post-Incident — Conduct a third-party risk review using this incident as a trigger case. Map every vendor that holds PII to a risk tier; verify that Tier 1 vendors (high PII volume, government data) have been assessed within the past 12 months (NIST AC-20; CIS 7.1: Vulnerability Management Process). Implement D3-UAP (User Account Permissions) and D3-MFA (Multi-factor Authentication) requirements as mandatory contract terms for new and renewing vendors. Address CWE-778 gaps by requiring vendors to contractually guarantee log retention of no less than 90 days with audit access on demand (NIST AU-11: Audit Record Retention; NIST AU-9: Protection of Audit Information).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-20 (Use Of External Systems), NIST AU-9 (Protection Of Audit Information), NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Build the vendor PII risk tier map in a spreadsheet: columns for vendor name, PII fields held, estimated record count, last assessment date, MFA status, log retention confirmation, and contract renewal date. Prioritize Tier 1 vendors (those holding driver's license numbers, passport numbers, or >50,000 records) for immediate

reassessment using the CIS Controls v8 IG1 self-assessment questionnaire — freely available from CIS. For log retention enforcement, draft a one-paragraph contract addendum requiring 90-day minimum log retention with audit-on-demand rights and attach it to all Tier 1 renewals. Track addendum signature status in the same spreadsheet.

Evidence: No live system state is altered in this post-incident step, so order-of-volatility sequencing does not apply. Evidence to compile and preserve for the lessons-learned record: (1) the complete vendor inventory and risk tier mapping produced during this review, with assessment dates and gaps documented — this becomes the baseline for the next annual review cycle; (2) all written attestations, forensic reports, and questionnaire responses collected from vendors during Steps 3 and 4 — retained as evidence of due diligence for regulatory purposes; (3) a documented timeline of the TPWD breach pattern (the 30-month Texas government vendor breach series) cross-referenced against your own vendor assessment history, to determine whether any of your Tier 1 vendors were assessed before or after known breach events in that pattern; (4) meeting notes or records from the post-incident lessons-learned session, including identified control gaps and assigned remediation owners with target dates — required by NIST 800-61r3 §4 for organizational learning and process improvement.

Detection Guidance

No IOCs have been publicly released for this incident. Detection focus should be behavioral and contractual rather than signature-based. Query your SIEM for bulk PII access events at third-party API integration points: look for single sessions returning more than 1,000 records from license, identity, or permit management systems. Alert on after-hours administrative logins to vendor portals (NIST AU-6: Audit Record Review, Analysis, and Reporting). Cross-reference D3-LAM (Local Account Monitoring) principles: watch for privilege escalation or new account creation events at the vendor access tier. If your organization shares a vendor with TPWD, request the vendor's access logs covering the breach window and run them against your own user population for anomalous access patterns. For downstream phishing detection: watch for inbound emails referencing Texas hunting or fishing license information, TPWD branding, or driver's license verification requests, consistent with T1566 (Phishing) exploitation of the exposed dataset.

Framework Mappings

MITRE-ATTACK

- **T1589** — Gather Victim Identity Information
- **T1567** — Exfiltration Over Web Service
- **T1566** — Phishing
- **T1190** — Exploit Public-Facing Application
- **T1530** — Data from Cloud Storage
- **T1048** — Exfiltration Over Alternative Protocol
- **T1486** — Data Encrypted for Impact
- **T1213** — Data from Information Repositories
- **T1078** — Valid Accounts

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection

- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement
- **IR-4** — Incident Handling
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **15.1** — Establish and Maintain an Inventory of Service Providers
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents
- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training
- **164.308(a)(6)(ii)** — Response and Reporting

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1589	Gather Victim Identity Information	Reconnaissance
T1567	Exfiltration Over Web Service	Exfiltration
T1566	Phishing	Initial-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1530	Data from Cloud Storage	Collection
T1048	Exfiltration Over Alternative Protocol	Exfiltration
T1486	Data Encrypted for Impact	Impact
T1213	Data from Information Repositories	Collection
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/texas-govt-data-brea...	T3
	https://www.bleepingcomputer.com/news/security/transunion-suffers-d...	T3
	https://www.bleepingcomputer.com/news/security/texas-state-bar-warn...	T3
	https://www.bleepingcomputer.com/news/security/dallas-county-data-o...	T3

Source	URL	Tier
Notification of Data Security Incident - Texas Parks and Wildlife	https://tpwd.texas.gov/about/notification-of-data-security-incident	T1

Generated 2026-06-19 18:59 UTC by TJS Security Command Center