DPS Cyber Security Contract Requirements Exhibit

OGC approved 9/1/2021

DPS Cyber Security Contract Requirements Exhibit

Table of Contents

DPS Cyber Security Contract Requirements Exhibit

1. Definitions

These definitions only apply to the Cyber Security Contract Requirements Exhibit.

a. **CISO** means DPS's Chief Information Security Officer.
b. **CJIS** means Criminal Justice Information Services; the FBI and DPS are in charge of overseeing compliance.
c. **Cloud Service Provider (CSP)** means a third-party company offering a cloud-based platform, infrastructure, application, or storage services.
d. **Confidential Data** means Confidential Information as defined in 1 Texas Administrative Code § 202.1(5) that is collected and maintained by DPS. Vendor must protect this data against unauthorized disclosure and the data is not subject to public disclosure under the provisions of applicable state or federal law or other legal agreements.
e. **DPS** means the Department of Public Safety of the State of Texas.
f. **DIR** means the Department of Information Resources.
g. **Enterprise Content Management (ECM)** means technology that provides a means to create, store, manage, secure, distribute, and publish any digital content for enterprise use.
h. **FedRAMP** stands for the Federal Risk and Authorization Management Program
i. **HIPAA** stands for Health Insurance Portability and Accountability Act
j. **Hosted Services** means a combination of traditional IT functions to be provided by Vendor or a third-party such as infrastructure, applications software (including Commercial off the Shelf (COTS) software solutions), security, monitoring, storage, hardware, and hardware maintenance.
k. **PCI DSS** stands for Payment Card Industry Data Security Standard
l. **Regulated Data** means information that is collected and maintained by DPS that requires DPS to implement specific privacy and security safeguards as mandated by federal and state law.
m. **Secure Location** means a facility, conveyance, or area with security controls sufficient to protect sensitive or confidential information and associated information systems.
n. **Security Incident** means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
o. **System/Solution** means a collection of information management techniques involving computer automation (software/hardware/database/network) to support and improve the quality and efficiency of business operations.
p. **System Component** means any individual unit of Hardware or Software which together with other system components make up the System as a whole.

q. **System Failure** means a breakdown of any system hardware, operating system, or application software which prevents the accomplishment of the system's intended function.
r. **TDI** means the Texas Department of Insurance.
s. **TexRAMP** stands for the Texas Risk and Authorization Management Program
t. **United States of America** means the 50 states and the District of Columbia
u. **Wireless Local Area Network (WLAN)** means a wireless computer network that links two or more devices using a wireless distribution method within a limited area.

DPS Cyber Security Contract Requirements Exhibit

2. Cyber Security Standards

Vendor represents and warrants that it will comply with all contract requirements. DPS reserves the right to disqualify or reject Vendor's response or Solution for non-compliance or for failure to meet DPS's desired specifications. DPS may hold Vendor in material breach of contract for noncompliance with these requirements at any time during the life of the Contract.

3. Hosted Services Security

For all Hosted Services:

1. If CJIS data is being processed, stored, or transmitted, or if the solution interfaces with a CJIS system or network, Vendor's and the provider's environment must be CJIS compliant, unless the data remains encrypted per CJIS standards and DPS personnel control the encryption keys. DPS's network is considered a CJIS network.
2. If other Regulated Data is being processed, stored, or transmitted, Vendor's and the provider's environment must be compliant with the applicable regulation (For example: HIPAA or PCI DSS).
3. The environment must comply with the current Cloud Security Alliance's (CSA) Cloud Control Matrix (CCM) incorporated by reference as applicable. Information pertaining to the CSA may be found at https://cloudsecurityalliance.org/ and CCM information may be found at https://cloudsecurityalliance.org/research/cloud-controls-matrix/
4. For all contractor-hosted services proposed (even if Vendor wants to use a third-party provider such as a standardized CSP), Vendor must provide a completed Consensus Assessments Initiative Questionnaire (CAIQ) within its Response. The submitted CAIQ must have been completed within the last year. The CAIQ can be downloaded from this link: https://cloudsecurityalliance.org/research/cloud-controls-matrix/.

For hosted services using a third-party CSP:

1. For all DPS data, the solution must be deployed in an environment authorized by TexRAMP or FedRAMP at the appropriate impact level as determined by DPS, and maintain program compliance and certification throughout the term of the contract. If CJIS data is being processed, stored, or transmitted, the solution must be deployed in a Government Cloud environment.

For hosted services using infrastructure and services owned and operated by Vendor:

1. If the data being processed, stored, or transmitted is classified as non-public, Vendor must provide evidence of a third-party security assessment of the controls identified in the CCM upon request that meets the following requirements:

a. The assessment may not be more than one year old and must target the most recent major release of the product/service that is being provided to DPS.
b. The assessment must be performed by a certified third party. Self-assessments performed by Vendor are not acceptable.

4. User Security

Vendor must:

a. Provide Active Directory based authentication or SAML2 Identity Provider/Service Provider authentication.

b. Establish and administer user accounts in accordance with a role-based scheme and will track and monitor role assignment.

c. Within five business days, notify DPS of personnel additions, personnel changes that affect a user's need-to-know, or if a user is terminated or transferred, or associated accounts are removed, disabled, or otherwise secured.

d. Ensure systems prevent multiple concurrent active sessions for one user identification.

e. Ensure systems enforce a limit of no more than three consecutive invalid access attempts by a user. After three consecutive invalid attempts, automatically lock the account/node for a ten-minute time period unless released by DPS's Administrator.

f. Ensure systems prevent further access by initiating a session lock or termination after a maximum of 30 minutes of inactivity, and the session lock or termination will remain in effect until the user reestablishes access using appropriate identification and authentication procedures.

g. Ensure all users are uniquely identified and prevent the reuse of user identifiers.

h. Require two-factor authentication for public facing application user accounts with elevated or administrative privileges.

i. Ensure systems conduct normal operations without the use of elevated or administrative privileges.

j. Ensure System user functionality is separated from administrator functionality, and require users to establish sessions with administrative privileges to view and access administrator functionality.

k. Force users to follow the secure password attributes, below, to authenticate a user's unique ID. The secure password attributes must:

1) Be a minimum length of 12 characters;
2) Not be a dictionary word or proper name;
3) Not be the same as, or contain, the User ID;
4) Expire within a maximum of 90 calendar days;
5) Not be identical to the previous ten passwords;
6) Not be transmitted in clear text outside the Secure Location;
7) Not be displayed in clear text when entered;
8) Never be stored in plain text, electronically or physically;
9) Never be displayed in clear text on the screen; and
10) Include two numbers as well as two special, two upper, and two lower characters

5. System Security

Vendor must:

a. Provide audit logs that enable tracking of activities taking place on the System.

1) Audit logs will track account creation, modification, disabling, and termination actions.
2) Audit logs will track successful and unsuccessful System log-on attempts.
3) Audit logs will track successful and unsuccessful attempts to access, create, write, delete, or change permission on a user account, file, directory, or other System resource.
4) Audit logs will track successful and unsuccessful attempts to change account passwords.
5) Audit logs will track successful and unsuccessful actions by privileged accounts.
6) Audit logs will track successful and unsuccessful attempts for users to access, modify, or destroy the audit log.

b. Provide the following content to be included with every audited event:

1) Date and time of the event;
2) The component of the System (e.g. software component, hardware component) where the event occurred;
3) IP address;
4) Type of event;
5) User/subject identity; and
6) Outcome (success or failure) of the event.

c. Ensure audit logs are retained for at least one year.

d. Provide real-time alerts to appropriate DPS personnel in the event of an audit processing failure. Alert recipients and delivery methods must be configurable and manageable by DPS System Administrators.

e. Provide real-time alerts to appropriate DPS personnel for audit events that may indicate inappropriate or unusual activity, as defined by DPS.

f. Provide an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of Security Incidents; and does not alter the original content or time ordering of audit records.

g. Ensure audit record time stamps use internal system clocks.

h. Protect audit information and audit tools from unauthorized access, modification, and deletion.

i. Undergo vulnerability scan/penetration testing conducted by DPS or DIR on at least an annual basis or more frequently depending on the system categorization and risk level.

j. Remediate all vulnerabilities reported by DPS Cyber Security or discovered by Vendor in no more than 90 days of the vulnerability finding or sooner depending on the system categorization, risk level, and the severity of the vulnerability as determined by DPS. If this does not occur, at no additional cost to DPS, the System\Solution may not be accepted or may be removed from the DPS network or DPS use until all vulnerability issues are resolved.

k. Display an approved use notification message or banner before granting access to the System. The notification must contain an approved DPS logo and state:

   1) Users are accessing a DPS system;
   2) System usage will be monitored, recorded, and subject to audit;
   3) Unauthorized use of the system is prohibited and subject to criminal and civil penalties;
   4) A description of the authorized use of the system; and
   5) Use of the system indicates consent to monitoring and recording.

l. Implement and use DPS-approved virus protection software and configuration at all System entry and exit points:

   1) The virus protection software must not be disabled or bypassed.
   2) The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.
   3) The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.

m. Implement and use management and maintenance applications and tools, appropriate fraud prevention and detection, and data confidentiality, protection, and encryption technologies for endpoints, servers, and mobile devices. This must include mechanisms to identify vulnerabilities and apply security patches.

n. Implement security testing and flaw remediation during system development to ensure software and firmware security defects are corrected before installation in a production environment.

o. Ensure communication at the external boundary of the system is controlled and monitored to prevent unauthorized connections and protect against or limit the effects of denial of service attacks.

p. Verify the validity of information inputs or implement other controls to prevent the injection of malicious input provided to the System.

q. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.

r. Prevent unauthorized and unintended information transfer via shared system resources, such as registers, main memory, and hard disks.

s. Maintain a separate execution domain for each executing system process, so that one process cannot modify the executing code of another process.

t. Implement mechanisms to safeguard the System's memory from unauthorized code execution.

u. Establish and maintain a continuous security program as part of the Services. The security program will enable DPS (or its selected third party) to:

   1) Define the scope and boundaries, policies, and organizational structure of an information security management system;

2) Conduct periodic risk assessments to identify the specific threats to and vulnerabilities of DPS due to the Services, subject to the terms, conditions and procedures;
3) Implement appropriate mitigating controls and training programs, and manage resources; and
4) Monitor and test the security program to ensure its effectiveness. Vendor must review and adjust the security program in light of any assessed risks.

6. System Maintenance

Vendor must:

a. Schedule, perform, document, and review records of maintenance and repairs on information system components in accordance with manufacturers' specifications or organizational requirements;
b. Submit all maintenance activities for approval by DPS, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;
c. Submit any maintenance tools used for diagnostic or repair actions for approval by DPS;
d. Ensure nonlocal (remote) maintenance sessions are uniquely authenticated, all maintenance and diagnostic activities are logged, and that sessions and network connections are terminated when maintenance is complete.
e. Obtain written approval from DPS for the removal of the information system or system components from the secure hosting location for off-site maintenance or repairs;
f. Sanitize equipment to remove all information from associated media prior to removal from the secure hosting location for off-site maintenance or repairs;
g. Check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions; and
h. Ensure all maintenance personnel are authorized by DPS.

7. System/Solution Assurance

Vendor must:

a. Provide security updates to correct any security defect, vulnerability, or exploit in the System/Solution in accordance with DPS Cyber Security requirements based on the level of risk.

b. Ensure systems will operate with all System/Solution supporting software updates, security updates, and patches.

c. Replace or upgrade systems that are no longer supported by the manufacturer within three months from the official manufacturer end of support date.

d. Complete DPS's System Security Documentation (SSD) at the request of DPS to document the implementation of the System's required security controls as identified in these Cyber Security Contract Requirements, and periodically review and update the information upon request from DPS.

e. Protect DPS's System Security Documentation from unauthorized access, disclosure, or release in accordance with the Subsection entitled "General Confidentiality Requirements."

f. At DPS's request, provide documentation for the System that describes user and administrator guidance regarding the implementation and operation of security controls.

g. Work closely with DPS to ensure all security requirements are met and implemented, or any exceptions formally approved, prior to System acceptance.

8. Physical and Environmental Controls

Vendor must:

a. Restrict physical access to the System containing DPS's data to authorized personnel with appropriate clearances and access authorizations.

b. Enforce physical access authorizations for all physical access points to the facility where the System resides;

c. Verify individual access authorizations before granting access to the facility containing the System;

d. Control entry to the facility containing the System using physical access devices or guards;

e. Change combinations and access devices when access devices are lost, combinations are compromised, or individuals are transferred or terminated;

f. Maintain appropriate environmental controls in the facility containing the System. Environmental controls include maintaining and monitoring heat and humidity levels, fire suppression and detection systems supported by an independent energy source, water shutoff and isolation valves, and

uninterruptable power systems capable of supporting the System in the event of a primary power System Failure; and

g. Collaborate with DPS on security monitoring and incident response, define points of contact on both sides, establish monitoring and response procedures, set escalation thresholds, and conduct training. Vendor must, at the request of DPS or, in the absence of any request from DPS, at least quarterly, provide the DPS's CISO with a report of the incidents that Vendor has identified and taken measures to resolve.

9. Data Security

a. DPS data must be marked, handled, and stored in compliance with the data classification and retention as defined by DPS.

b. If Vendor or any subcontractors require access to DPS's network; DPS's data; or the network processing, transporting, or storing of DPS's data, Vendor will be required to sign the CJIS Security Addendum at DPS's discretion, and all of Vendor's employees requiring access to DPS's network or data will sign the FBI Certification to the CJIS Security Addendum and complete and pass a fingerprint based background check.

c. The System will protect against an employee falsely denying having performed a particular action (non-repudiation).

d. Vendor, its subcontractors, and their staff with access to DPS's data outside of DPS's network will complete and provide proof of DIR certified security awareness training. Security awareness training must be completed annually during the term of the contract and during any renewal period. Refer to Subsection 15.b. for training requirements for individuals with access to DPS's network.

e. Vendor, its subcontractors, and their staff must comply with relevant federal and state statutes and rules, including CJIS requirements.

f. Data may not be exported to a location external to the hosting environment without the written permission of DPS.

g. All DPS data and metadata must remain within the United States of America.

10. Encryption

The System must protect the confidentiality of DPS's information. All data transmitted outside or stored outside the secure network must be encrypted. When cryptography (encryption) is employed within information systems, the System must

perform all cryptographic operations using Federal Information Processing Standards (FIPS) Publication 140-2 or 140-3 validated cryptographic modules with approved modes of operation. The System must produce, control, and distribute cryptographic keys using NIST-approved key management technology and processes. The key management process is subject to audit by DPS.

11. Wireless

a. Wireless: The following requirements specify the minimum set of security measures required on WLAN-enabled portable electronic devices (PEDs) that transmit, receive, process, or store sensitive or confidential information:

1) Personal Firewall: WLAN-enabled PED must use personal firewalls or run a Mobile Device Management system that facilitates the ability to provide firewall services.
2) Anti-Virus Software: Anti-virus software must be used on wireless ECM-capable PEDs or run a Mobile Device Management System that facilitates the ability to provide anti-virus services.
3) Encryption of personal information or Confidential Data-in-transit via WLAN-enabled PEDs, systems and technologies must be implemented in a manner that protects the data end-to-end. All systems components within a WLAN that wirelessly transmit sensitive or confidential information must have cryptographic functionality that is validated under the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program as meeting requirements per Federal Information Processing Standards (FIPS) Publication 140-2. Encryption must be a minimum of 128 bit.
4) Data-at-Rest: Data at rest encryption must be implemented in a manner that protects sensitive and confidential information stored on WLAN enabled PEDs by requiring that the PED must be powered on and credentials successfully authenticated in order for the data to be deciphered. Data-at-rest encryption must include the encryption of individual files, portions of the file system (e.g., directories or partitions), or the entire drive (e.g. hard disks, on-board memory cards, memory expansion cards). In recognition of the increased risk of unauthorized access to sensitive or confidential information in the event that a PED is lost or stolen and the inherently mobile nature of these devices, encryption must be provided for data-at-rest on all WLAN enabled PEDs that is validated as meeting FIPS 140-2.
5) WLAN Infrastructure: WLAN infrastructure systems may be composed of either stand-alone (autonomous) access points or thin Access Points that are centrally controlled by a WLAN controller.
6) Validated Physical Security: Access Points used in the WLANs may not be installed in unprotected environments due to an increased risk of tampering or theft. Vendor is required to periodically check for rogue access points or

force any network connection to be validated in some manner so Vendor is aware of what is connected.

12. Mobile Device Management

The following requirements specify the minimum set of security measures required on mobile devices that transmit, receive, process, or store sensitive or confidential information:

a. Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery. MDM will be implemented and include the following core features:

1) The ability to push security policies to managed devices;
2) The ability to query the device for its configuration information;
3) The ability to modify device configuration as required;
4) Security functionality that ensures the authenticity and integrity of the transaction in the three categories above;
5) Asset management (track/enable/disable) of the mobile devices being managed via the MDM server;
6) The ability to manage proxy access to network resources via the connection of the mobile device to the MDM server;
7) The ability to query devices being managed on the status of security policy compliance and to implement a specified mediation function based on compliance status;
8) The ability to download and store mobile device audit records;
9) The ability to receive alerts and other notifications from managed mobile devices;
10) The ability to generate audit record reports from mobile device audit records;
11) The ability to remotely wipe a device in the event it is lost or stolen; and
12) Application management (application white list) for applications installed on managed mobile devices.

13. Secure Erasure Capability

All equipment provided to DPS by Vendor that is equipped with hard disk drives (e.g., computers, telephones, printers, fax machines, scanners, multifunction devices) as well as all removable storage media (USBs, flash drives, tape drives, etc.) will have the capability to securely erase data written to the hard drive or media device prior to final disposition of such equipment, either at the end of the equipment's useful life or the end of the related services agreement for such equipment, in accordance with 1 Tex. Admin. Code Ch. 202.

DPS Cyber Security Contract Requirements Exhibit

14. Data Center Location Requirements

The data center must be located in the United States of America. See also Section 9.

15. Access to Internal DPS Network and Systems

As a condition of gaining remote access to any internal DPS network and Systems, Vendor must comply with DPS policies and procedures. DPS's remote access request procedures require Vendor to submit a Remote Access Request form for DPS's review and approval.

a. DPS's CISO must approve remote access technologies provided by Vendor.

b. Individuals who are provided with access to DPS's network are required to complete DPS's Security Awareness Training on an annual basis during the term of the contract and during any renewal period.

c. Vendor must secure its own connected systems in a manner consistent with DPS requirements.

d. DPS reserves the right to audit the security measures in effect on Vendor's connected systems without prior warning.

e. DPS also reserves the right to immediately terminate network and system connections not meeting such requirements.

16. DPS Information Protection Requirements

a. Vendor, its employees, and any subcontractors must comply with all applicable requirements that relate to the protection or disclosure of DPS Information. DPS Information includes all data and information:
    1. Submitted to Vendor by or on behalf of DPS;
    2. Obtained, developed, or produced by Vendor in connection with the Contract;
    3. Communicated verbally whether intentionally or unintentionally; or
    4. To which Vendor has access in connection with the Services provided under the Contract.

b. Such DPS Information may include taxpayer, vendor, and other state agency data held by DPS.

c. All waiver requests will be processed in accordance with DPS's Information Protection Policies, Standards & Guidelines, and must be approved by the CISO.

d. DPS reserves the right to take appropriate action to protect DPS's network and information including the immediate termination of System access.

e. Vendor must ensure that any sensitive or confidential DPS Information in the custody of Vendor is properly sanitized or destroyed when the information is no longer required to be retained by DPS or Vendor in accordance with the Contract.

f. Electronic media used for storing any sensitive or confidential DPS Information must be sanitized by clearing, purging, or destroying in accordance with NIST Special Publication 800-88 Guidelines for Media Sanitization. Vendor must maintain a record documenting the removal and completion of all sanitization procedures with the following information:
   1) Date and time of sanitization/destruction;
   2) Description of the item(s) and serial number(s) if applicable;
   3) Inventory number(s); and
   4) Procedures and tools used for sanitization/destruction.

g. No later than 60 calendar days from contract expiration or termination or as otherwise specified in the Contract, Vendor must complete the sanitization and destruction of the data and provide to DPS all sanitization documentation.

17. General Confidentiality Requirements

a. All information provided by DPS to Vendor or created by Vendor in performing the obligations under the Contract is confidential and may not be used by Vendor or disclosed to any person or entity, unless such use or disclosure is required for Vendor to perform work under the Contract. The obligations of this section do not apply to information that Vendor can demonstrate:

   1) Is publicly known at the time of disclosure or subsequently becomes publicly known through no fault of Contractor;
   2) Contractor discovered, learned, or created independently by Contractor or by a rightfully possessing and disclosing third party or by any other legitimate means;
   3) Is required to be disclosed by law or final order of a court of competent jurisdiction or regulatory authority, but Contractor must furnish prompt written notice of such required disclosure and must reasonably cooperate with DPS at DPS's cost and expense, in any effort made by DPS to seek a protection order or other appropriate protection of its confidential information.

b. Vendor must notify DPS in writing of any unauthorized release of confidential information within four hours of when Vendor knows or should have known of such unauthorized release.

c. Contractor must notify affected parties in writing of any unauthorized release of confidential information within two business days of when Contractor knows or should have known of any unauthorized release of confidential information obtained from affected parties

d. Contractor must maintain all confidential information in confidence during the term of the Contract and after the expiration or earlier termination of the Contract.

e. If Contractor has any questions or doubts as to whether particular material or information is confidential information, Contractor must obtain the prior written approval of DPS prior to using, disclosing, or releasing such information.

f. Contractor acknowledges that DPS's confidential information is unique and valuable, and that DPS may have no adequate remedy at law if Contractor does not comply with its confidentiality obligations under the Contract. Therefore, DPS will have the right, in addition to any other rights it may have, to seek in any Travis County court of competent jurisdiction temporary, preliminary, and permanent injunctive relief to restrain any breach, threatened breach, or otherwise to specifically enforce any confidentiality obligations of Contractor if Contractor fails to perform any of its confidentiality obligations under the Contract.

g. Vendor must immediately return to DPS all confidential information when the Contract terminates, at such earlier time as when the information is no longer required for the performance of the Contract or when DPS requests that such information be returned.

h. Information, documentation, and other material in connection with the Contract, including Vendor's proposal, may be subject to public disclosure pursuant to the Texas Government Code Chapter 552.

i. The FBI and DPS have computer security requirements. Vendor's and subcontractor's employees working on this assignment must sign and submit appropriate agreements and abide by these security requirements, within five calendar days of DPS's request.

18. Personal Information

To the extent this subsection does not conflict with the section entitled "General Confidentiality Requirements," Vendor must comply with both sections. To the extent this subsection conflicts with the Subsection entitled "General Confidentiality Requirements," this section entitled "Personal Information" controls. Personal information does not include publicly available information that is lawfully made

available to the public from the federal government or a state or local government. "Personal identifying information" and "Sensitive personal information" are defined by Tex. Bus. & Com. Code Ch. 521. Both are classified as personal information for purposes of this section. Personal information does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.

a. Vendor must implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any personal information collected or maintained by Vendor under the Contract.

b. "Breach of system security" is defined as follows: Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information Vendor maintains under the Contract, including data that is encrypted if Vendor's employee or agent accessing the data has the key required to decrypt the data. Good faith acquisition of personal information by an employee or agent of Vendor for the purposes of performing under the Contract is not a breach of system security unless the employee or agent of Vendor uses or discloses the personal information in an unauthorized manner.

c. Vendor must notify DPS and affected parties of any breach of system security immediately after discovering the breach or receiving notification of the breach, if personal information was, or is reasonably believed to have been, acquired by an unauthorized person. However, Vendor must delay providing notice to the affected parties at DPS's request, if DPS determines that the notification will impede a criminal investigation. Notification to the affected people may be made as soon as DPS determines that it will not compromise any criminal investigation.

d. Vendor must give notice as follows, at Vendor's expense:
    1) Written notice;
    2) Electronic notice, if the notice is provided in accordance with 15 U.S. Code Section 7001;
    3) Notice as follows:
        a) If Vendor demonstrates that the cost of providing notice would exceed $250,000, the number of affected people exceeds 500,000, or Vendor does not have sufficient contact information for the affected people, Vendor may give notice as follows:
            i. Email, if Vendor has an email address for the affected people;
            ii. Conspicuous posting of the notice on Vendor's website;
            iii. Notice published in or broadcast on major statewide media; or

b) If Vendor maintains its own notification procedures (as part of an information security policy for the treatment of personal information) that comply with the timing requirements for notice under this subsection entitled "Personal Information," Vendor may provide notice in accordance with that policy.

e. If this subsection requires Vendor to notify at one time more than 10,000 people of a breach of system security, Vendor must also notify, without unreasonable delay, each consumer reporting agency (as defined by 15 U.S. Code Section 1681a) that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices.

f. In the event of a breach of system security, if personal information was, or is reasonably believed to have been, acquired by an unauthorized person, DPS, an agency of the State of Texas, may assess and enforce, as applicable and without limitation, cyber insurance coverage requirements, indemnification, duty to defend, liquidated damages, actual damages, sanctions, rights, claims, remedies and other amounts against Vendor in accordance with the contract that includes these Cyber Security Contract Requirements, and in accordance with other applicable law. Vendor understands that there may be constitutional and statutory limitations on DPS to enter into certain terms and conditions of the contract that includes these Cyber Security Contract Requirements and that any such terms and conditions will not be binding on DPS except to the extent authorized by the laws and constitution of the State of Texas.

g. Liquidated Damages may be assessed under this Section 18 in the amount of the per capita data breach cost for public sector (government) records as listed in the current Ponemon Institute Research Report Cost of Data Breach Study: United States. The number of affected records will be determined at the time of breach, with a not to exceed Liquidated Damages Cap of 100% of the total contract value.

The Ponemon Institute Research Report Cost of Data Breach Study: United States may be found at: http://www-03.ibm.com/security/data-breach/.

h. Vendor will not be responsible and liquidated damages may not be assessed due to a breach of system security caused entirely by someone other than Vendor, Vendor's subcontractor, or Vendor's agent. (This clause is not to be interpreted that Vendor is absolved of liability with any other sections pertaining to cyber security or data protection).

i. Any liquidated damages assessed under the Contract may, at DPS's option, be deducted from any payments due Vendor. DPS has the right to offset any

liquidated damages payable to DPS, as specified above, against any payments due to Vendor. If insufficient payments are available to offset such liquidated damages, then Vendor will pay to DPS any remaining liquidated damages within 15 calendar days following receipt of written notice of the amount due.

19. Disclosure of Security Incident

Without limitation on any other provision of the Contract regarding information security or security breaches, Vendor must provide notice to DPS's Contract Monitor and the CISO as soon as possible (but no later than 4 hours) following the discovery or reasonable belief that there has been a Security Incident.

a. Within four hours of the discovery or reasonable belief of a known or potential Security Incident, Vendor must provide a written report to the CISO detailing the circumstances of the incident, which includes at a minimum:
   1) A description of the nature of the Security Incident;
   2) The type of DPS information involved;
   3) Who may have obtained DPS information;
   4) What steps Vendor has taken or will take to investigate the Security Incident;
   5) What steps Vendor has taken or will take to mitigate any negative effect of the Security Incident; and
   6) A point of contact for additional information.

b. Each day thereafter until the investigation is complete, Vendor must provide the CISO with a written report regarding the status of the investigation and the following additional information as it becomes available:
   1) Who is known or suspected to have gained unauthorized access to DPS's information;
   2) Whether there is any knowledge if DPS information has been abused or compromised;
   3) What additional steps Vendor has taken or will take to investigate the Security Incident;
   4) What steps Vendor has taken or will take to mitigate any negative effect of the Security Incident; and
   5) What corrective action Vendor has taken or will take to prevent future similar unauthorized use or disclosure.

c. Vendor must confer with the CISO regarding the proper course of the investigation and risk mitigation. DPS reserves the right to conduct an independent investigation of any Security Incident, and should DPS choose to do so, Vendor must cooperate fully by making resources, personnel, and systems access available to DPS and DPS's authorized representatives.

d. Subject to review and approval of the CISO, Vendor must, at its own cost, provide notice that satisfies the requirements of applicable law to individuals whose personal, confidential, or privileged data were compromised or likely compromised as a result of the Security Incident. If DPS, in its sole discretion, elects to send its own separate notice, then all costs associated with preparing and providing notice will be reimbursed to DPS by Vendor. If Vendor does not reimburse such costs within 30 calendar days of DPS's written request, DPS will have the right to collect such costs.

20. Cyber Insurance Requirement

In accordance with the solicitation and any resulting Contract, Vendor must maintain sufficient cyber insurance to cover any losses, security breaches, privacy breaches, unauthorized distributions, or releases or uses of any data transferred to or accessed by Vendor under or as a result of the Contract.

a. This insurance will provide sufficient coverage for Vendor, DPS, and affected third parties for the review, repair, notification, remediation, and other response to such events, including data spillage, breaches, or similar incidents under Texas Business and Commerce Code Chapter 521.

b. DPS may, in its sole discretion, confer with TDI to review such coverage(s) prior to approving them as acceptable under the Contract.

c. Vendor must obtain modified coverage(s) as reasonably requested by DPS within ten calendar days of Vendor's receipt of such request from DPS.

21. Representations and Warranties Related To Software

If any software is provided under the Contract, Vendor represents and warrants each of the following:

a. Vendor has sufficient right, title, and interest in the Software to grant the license required.

b. Contract terms and conditions included in any "clickwrap," "browsewrap," "shrinkwrap," or other license agreement that accompanies any Software (including Software Updates, Software Patch/Fix, or Software Upgrades) provided under the Contract are void and have no effect unless DPS specifically agrees to each licensure term in the fully executed Contract.

c. The Software provided under the Contract does not infringe upon or constitute a misuse or misappropriation of any patent, trademark, copyright, trade secret, or other proprietary right;

d. Software and any Software Updates, Software Maintenance, Software Patch/Fix, and Software Upgrades provided under the Contract must not contain viruses, malware, spyware, key logger, back door, or other covert communications, or any computer code intentionally designed to disrupt, disable, harm, or otherwise impede in any manner, including aesthetical disruptions or distortions, the operation of the computer program, or any other associated software, firmware, hardware, or computer system, (including local area or wide-area networks), in a manner not intended by its creator(s); and

e. Software provided under the Contract does not and must not contain any computer code that would disable the Software or impair in any way its operation based on the elapsing of a period of time, exceeding an authorized number of copies, advancement to a particular date or other numeral, or other similar self-destruct mechanism (sometimes referred to as “time bombs”, “time locks”, or “drop dead” devices) or that would permit Vendor to access the Software to cause such disablement or impairment (sometimes referred to as “trap door” devices).