Exhibit No. F.3

Texas Department of Public Safety

Cyber Security Contract Requirements

Solicitation RFO No.
_________21R0010466___________

Information required as part of a response to a specific Solicitation or required for inclusion as part of a specific Contract (if no Solicitation) or required prior to beginning of work or assignment of employees to the Contract is highlighted in green.

Cyber Security Contract Requirements Exhibit

Contents

Cyber Security Contract Requirements Exhibit

SYSTEM SECURITY AND ACCESS

1. Definitions

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

a. **CISO** means the Department's Chief Information Security Officer.
b. **CJIS Security Addendum** means a document that describes the FBI security related requirements the Department applies to all contractors and subcontractors that work on the Department's contracts. An executed copy of the CJIS Security Addendum is a required part of these contracts. A copy of this form may be found at http://txdps.state.tx.us/SecurityReview/documents.htm.
c. **Contract** means the written agreement with the Contractor that incorporates the Exhibit that includes these Cyber Security Contract Requirements.
d. **Contractor** means the person or entity with which the Department has entered into this Contract. .
e. **Contractor Hosted or Hosted** means a combination of traditional IT functions to be provided by the Contractor such as infrastructure, applications software (including COTS software solution), security, monitoring, storage, and provider of hardware and hardware maintenance.
f. **Cyber Security Division (CSD)** means the Department's Cyber Security Division which is responsible for agency information technology security
g. **Department** means the Texas Department of Public Safety.
h. **Department Hosted** means a combination of traditional IT functions to be provided by the Department such as infrastructure, applications software (including COTS software solution), security, monitoring, storage, provider of hardware and hardware maintenance, and e-mail, over the internet or other Wide Area Networks (WAN).
i. **Department Policies** means all written policies, procedures, standards, guidelines, directives, and manuals of the Public Safety Commission and the Department, applicable to providing the Solution/Services specified under this Contract.
j. **Hardware** means the physical elements of a computing system including the physical components thereof.
k. **Information Technology Division (ITD)** means the Department's Information Technology Division which is responsible for agency technology innovation, maintenance, and support as applicable.
l. **May** means advisory or permissible.
m. **Must** means mandatory.

n. **PII** means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity; this includes any other personal information which is linked or linkable to an individual.

o. **PR** means Pricing Request.

p. **Respondent** means the individual, business entity, or organization that submits an Offer in response to the Solicitation, if any, related to this Contract, with the intent to contract with the Department.

q. **RFQ** means Request for Qualifications.

r. **RFO** means Request for Offers.

s. **RFP** means Request for Proposals

t. **Services** means the furnishing of labor, time, or effort by the Contractor, which may or may not involve the delivery of a specific end product other than reports.

u. **Shall** means mandatory.

v. **Software** means any application programs for exclusive use with the System.

w. **Solicitation** means Request for Proposals (RFP), Request for Offers (RFO), Pricing Request (PR) or Requests for Qualifications (RFQ).

x. **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.

y. **System** 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.

z. **System Backups** means procedures utilized to backup data to protect against data loss in the event of a System outage. Backups will include cold (offline) and hot (online) backups.

aa. **System Component** means any individual unit of Hardware or Software which together with other system components make up the System as a whole.

bb. **System Failure** means a breakdown of any system hardware, operating system, or application software which prevents the accomplishment of the system's intended function.

cc. **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.

2. Cyber Security Standards

The Contractor represents and warrants that it shall comply with all technology, security, assurance, accessibility, warranty, maintenance, confidentiality, testing and other standards, policies and procedures of the Department and the State of Texas that are applicable to the Contractor in its performance of this Contract as such standards, policies, and procedures are amended by the Department or the State throughout the term of this Contract, including any renewal or *optional* periods. The CISO is designated by the Department to assist the Contractor in reviewing these standards, policies and procedures and identifying those that are applicable to the Contractor in its performance of this Contract. The Department reserves the right to disqualify or reject Contractor's Solicitation Response or Solution for non-compliance or for failure to meet the Department's desired specification.

3. Cloud Security

For all Contractor-hosted Service(s) or application(s) that are included as part of the Contractor's solution, the Contractor shall:

a. Comply with the current Cloud Security Alliance's (CSA) Cloud Control Matrix (CCM), RFO/Exhibit J.X or PR Exhibit X; and
b. Provide a completed CSA CCM for the Solution within its Solicitation Response.

Information pertaining to CSA https://cloudsecurityalliance.org/ and CCM information may be found at https://cloudsecurityalliance.org/research/ccm/.

4. User Security

The Contractor shall:

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

b. Account Management: Automatically audit account creations, modifications, disabling and termination actions with notification to the Department's personnel.

c. Prevent multiple concurrent active sessions for one user identification.

d. Enforce a limit of no more than three (3) consecutive invalid access attempts by a user.

e. Automatically lock the account/node for a three (3) minute time period unless released by the Department's Administrator.

f. Prevent further access to the system by initiating a session lock after a maximum of thirty (30) minutes of inactivity, and the session lock will remain in effect until the user reestablishes access using appropriate identification and authentication procedures.

g. Ensure all users will be uniquely identified.

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

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

5. System Assurance

The Contractor shall comply with the following System assurance specifications:

a. Provide periodic security updates to correct any security defect, vulnerability, or exploit in System.

b. Systems will operate with all System supporting software updates, security updates, and patches.

c. Systems that are no longer supported by the manufacturer will be replaced or upgraded within three (3) months from the official manufacturer end of support date.

d. Systems will operate without the use of elevated access privileges.

6. System Security

The Contractor shall:

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

b. Audit logs will track successful and unsuccessful System log-on attempts.

c. 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.

d. Audit logs will track successful and unsuccessful attempts to change account passwords.

e. Audit logs will track successful and unsuccessful actions by privileged accounts.

f. Audit logs will track successful and unsuccessful attempts for users to access, modify, or destroy the audit log.

g. 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.

h. Provide real-time alerts to appropriate Department officials in the event of an audit processing failure. Alert recipients and delivery methods will be configurable and manageable by the Department's system Administrators.

i. Undergo vulnerability scan/penetration testing conducted by the Department or the Texas Department of Information Resources. The Contractor shall remediate legitimate vulnerabilities and the System/Solution will not be accepted until all vulnerability issues are resolved at no additional cost to the Department.

j. Notifications will display an approved use notification message or banner before granting access to the System. The notification will state:

   1) Users are accessing a Department 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; and
   4) A description of the authorized use of the system.

k. The Contractor shall implement and use management and maintenance applications and tools, appropriate fraud prevention and detection, and data confidentiality/protection/encryption technologies for endpoints, servers and mobile devices. This will include mechanisms to identify vulnerabilities and apply security patches.

l. The Contractor shall establish and maintain a continuous security program as part of the Services. The security program will enable the Department (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 the Department 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. The Contractor will review and adjust the security program in light of any assessed risks.

7. Physical Access Controls

The Contractor shall:

a. Restrict physical access to the System containing the Department’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 and guards; and

e. Change combinations and keys when keys are lost, combinations are compromised, or individuals are transferred or terminated.

f. The Department and the Contractor shall collaborate on security monitoring and incident response, define points of contact on both sides, establish monitoring and response procedures, set escalation thresholds, and conduct training. The Contractor shall, at the request of the Department or, in the absence of any request from the Department, at least quarterly, provide the Department with a report of the incidents that it has identified and taken measures to resolve.

8. Data Security

a. If the Contractor or any subcontractors require access to the Department’s network; the Department’s data; or the network processing, transporting, or storing of the Department’s data (may at the Department’s discretion), the Contractor will be required to sign the CJIS Security Addendum, and all of the Contractor’s employees requiring access to the Department’s network will sign the FBI Certification to the CJIS Security Addendum and complete a fingerprint based background check.

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

c. The Contractor, its subcontractors, and their staff shall obtain and provide proof of PII certifications for its employees accessing the Department's data at the request of the Department.

d. The Contractor shall comply with relevant federal and state statutes and rules, and the Department's policies, and standards, including but not limited to CJIS requirements.

e. Data will not be exported to an external location without the permission of the Department.

f. In the event of any impermissible disclosure, loss or destruction of Confidential Information, the receiving Party shall immediately notify the disclosing Party and take all reasonable steps to mitigate any potential harm or further disclosure, loss or destruction of such Confidential Information.

9. Encryption

The System will protect the confidentiality of the Department's information. All data transmitted outside or stored outside the secure network will be encrypted. When cryptography (encryption) is employed within information systems, the System will perform all cryptographic operations using Federal Information Processing Standard (FIPS) PUB140-2 validated cryptographic modules with approved modes of operation. The System will produce, control, and distribute symmetric cryptographic keys using NIST-approved key management technology and processes. The key management process is subject to audit by the Department.

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 PII or confidential information:

1) Personal Firewall: WLAN-enabled PED will 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 will be used on wireless ECMs-capable PEDs or run a Mobile Device Management System that facilitates the ability to provide anti-virus services.
3) Encryption of PII or confidential data-in-transit via WLAN-enabled PEDs, systems and technologies will be implemented in a manner that protects the

data end-to-end. All systems components within a WLAN that wirelessly transmit PII or confidential information will 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 will be a minimum of 128 bit.

4) Data-at-Rest: Data at rest encryption will be implemented in a manner that protects PII 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 will 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 PII or confidential information in the event that a PED is lost or stolen and the inherently mobile nature of these devices, encryption will 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: APs used in the WLANS will not be installed in unprotected environments due to an increased risk of tampering and/or theft.

b. Mobile Device Management Requirement. 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 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) 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 manage mobile devices;

10) The ability to receive alerts and other notifications from managed mobile devices;
11) The ability to generate audit record reports from mobile device audit records; and
12) Application management (application white list) for applications installed on managed mobile devices.

10. Secure Erasure of Hard Disk Capability

All equipment provided to the Department by the Contractor that is equipped with hard disk drives (i.e. computers, telephones, printers, fax machines, scanners, multifunction devices, etc.) will have the capability to securely erase data written to the hard drive 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 TAC §202.

11. Data Center Location Requirements

The data center will be located in the continental United States of America.

12. Access to Internal Department Network and Systems

As a condition of gaining remote access to any internal Department network and Systems, the Contractor shall comply with Department policies and procedures. The Department's remote access request procedures require the Contractor to submit a Remote Access Request form for the Department's review and approval.

a. Remote access technologies provided by the Contractor will be approved by the Department's CISO.

b. Individuals who are provided with access to the Department's network may be required to attend or review the Department's Security Awareness Training on an annual basis.

c. The Contractor shall secure its own connected systems in a manner consistent with Department requirements.

d. The Department reserves the right to audit the security measures in effect on the Contractor's connected systems without prior warning.

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

13. FBI CJIS Security Addendum

The Respondent or proposed Contractor, as appropriate, shall execute an originally signed CJIS Security Addendum which can be downloaded from http://www.txdps.state.tx.us/securityreview. Additionally, a CJIS Security Addendum Certification will be signed by each employee performing duties related to this project prior to final Contract award. Each original Certification will include an original signature of the employee and the Contractor's representative. Non-compliance by the Respondent or proposed Contractor will be cause for termination of contract negotiations and the Department may elect to enter into negotiations with the next highest evaluated Respondent or proposed Contractor.

The Contractor shall, prior to beginning work on this Contract, enter into the CJIS online system all Contractor employees and subcontractors who will work on this Contract (further instructions will be provided to the Contractor prior to execution of this Contract), and have those employees/subcontractors complete the CJIS online training/testing. The Contractor shall meet or exceed all requirements contained in the CJIS Security Policy.

14. Criminal History Background Checks

a. The Contractor's project personnel shall submit to a fingerprint-based Criminal History Background Investigation, if required by the Department, at the Contractor's expense. To facilitate this Criminal History Background Investigation, each person shall complete the Department's Vendor Background Information form (HR-22), which will be provided by the Department.

b. If required under this Contract, the Contractor will not allow personnel who have not submitted to and successfully completed the Department's fingerprint-based Criminal History Background Investigation and who do not otherwise maintain a Department security clearance to work on this Contract. The Department has the right to prevent the Contractor's personnel from gaining access to the Department's building(s) and computer systems if the Department determines that such personnel do not pass the background check or fail to otherwise maintain the Department security clearance.

c. When required, the Contractor's Project Manager will provide the following to the Department's Project Manager within seven (7) calendar days of executing this Contract:

   a) the completed Vendor Background Information form (HR-22) for all proposed personnel; and
   b) Acceptable fingerprints for all proposed personnel.

d. Throughout the term of this Contract, the Department may require the Contractor personnel to submit an annual Department fingerprint-based Criminal History Background Investigation to the Department.

e. Throughout the term of this Contract, the Contractor will promptly notify the Department of any activity or action by the Contractor's personnel that may affect that individual's ability to continue to work under this Contract

15. Department Information Protection Policies, Standards & Guidelines

a. The Contractor, its employees, and any subcontractors shall comply with all applicable Department Information Protection Policies, Standards & Guidelines and any other Department requirements that relate to the protection or disclosure of Department Information. Department Information includes all data and information:
   1. Submitted to the Contractor by or on behalf of the Department;
   2. Obtained, developed, or produced by the Contractor in connection with this Contract;
   3. Communicated verbally whether intentionally or unintentionally; or
   4. To which the Contractor has access in connection with the Services provided under this Contract.

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

c. All waiver requests will be processed in accordance with the Department's Information Protection Policies, Standards & Guidelines Waiver Policy or within Chapter 26 of the TXDPS General Manual.

d. The Department reserves the right to audit the Contractor's compliance with the Department's Information Protection Policies, Standards & Guidelines or within Chapter 26 of the TXDPS General Manual.

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

f. The Contractor will ensure that any confidential Department Information in the custody of the Contractor is properly sanitized or destroyed when the information is no longer required to be retained by the Department or the Contractor in accordance with this Contract.

g. Electronic media used for storing any confidential Department Information will be sanitized by clearing, purging or destroying in accordance with NIST Special Publication 800-88 Guidelines for Media Sanitization. The Contractor will 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.

h. No later than sixty (60) calendar days from contract expiration or termination or as otherwise specified in this Contract, the Contractor shall complete the sanitization and destruction of the data and provide to the Department all sanitization documentation.

16. General Confidentiality Requirements

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

   1) Is publicly available;
   2) The Contractor received from a third party without restriction on disclosure and without breach of contract or other wrongful act;
   3) The Contractor independently developed without regard to the Department confidential information; or
   4) Is required to be disclosed by law or final order of a court of competent jurisdiction or regulatory authority, provided that the Contractor will furnish prompt written notice of such required disclosure and will reasonably cooperate with the Department at the Department’ cost and expense, in any effort made by the Department to seek a protection order or other appropriate protection of its confidential information.

b. The Contractor shall notify the Department in writing of any unauthorized release of confidential information within two (2) business days of when the Contractor knows or should have known of such unauthorized release.

c. The Contractor shall notify sub-recipient in writing of any unauthorized release of confidential information within two (2) business days of when the Contractor knows or should have known of any unauthorized release of confidential information obtained from sub-recipient(s).

d. The Contractor shall maintain all confidential information, regardless whether obtained from the Department or from sub-recipient(s) in confidence during the term of this Contract and after the expiration or earlier termination of this Contract.

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

f. The Contractor acknowledges that the Department's and sub-recipient(s)' confidential information is unique and valuable, and that the Department and sub-recipient(s) may have no adequate remedy at law if the Contractor does not comply with its confidentiality obligations under this Contract. Therefore, the Department 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 the Contractor if the Contractor fails to perform any of its confidentiality obligations under this Contract.

g. The Contractor shall immediately return to the Department all confidential information when this Contract terminates, at such earlier time as when the confidential information is no longer required for the performance of this Contract or when the Department requests that such confidential information be returned.

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

i. The FBI and the Department have computer security requirements. The Contractor's and subcontractor's employees working on this assignment will sign and submit appropriate agreements and abide by these security requirements, within five (5) calendar days of the Department's request.

17. Sensitive Personal Information

To the extent this subsection does not conflict with Subsection 15 herein entitled "General Confidentiality Requirements," the Contractor shall comply with both subsections. To the extent this subsection conflicts with the Subsection 15 herein entitled "General Confidentiality Requirements," this Subsection 17 entitled "Sensitive Personal Information" controls.

a. "Sensitive personal information" is defined as follows:

1) An individual’s first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

    a) Social security number;
    b) Driver’s license number or government-issued identification number; or
    c) Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account; or

2) Information that identifies an individual and relates to:

    a) The physical or mental health or condition of the individual;
    b) The provision of health care to the individual; or
    c) Payment for the provision of health care to the individual.

b. Sensitive 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.

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

d. The Contractor shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the Contractor under this Contract.

e. The Contractor shall notify the Department, any affected sub-recipient and the affected people of any breach of system security immediately after discovering the breach or receiving notification of the breach, if sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. However, the Contractor shall delay providing notice to the affected people and sub-recipients at the Department’s request, if the Department determines that the notification will impede a criminal investigation. Notification to the affected people will be made as soon as the Department determines that it will not compromise any criminal investigation.

f. The Contractor shall give notice as follows, at the Contractor's expense:

1) Written notice;
2) Electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001;
3) Notice as follows:

a) If the Contractor demonstrates that the cost of providing notice would exceed $250,000, the number of affected people exceeds 500,000, or the Contractor does not have sufficient contact information for the affected people, the Contractor may give notice as follows:

i. Electronic mail, if the Contractor has an electronic mail address for the affected people;
ii. Conspicuous posting of the notice on the Contractor's website;
iii. Notice published in or broadcast on major statewide media; or

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

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

h. In the event of a breach of system security, if sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person, the Department , 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 the Contractor in accordance with the contract that includes these Cyber Security Contract Requirements, and in accordance with other applicable law. The Contractor understands that there may be constitutional and statutory limitations on the Department 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 the Department except to the extent authorized by the laws and constitution of the State of Texas.

i. Liquidated Damages may be assessed under this Section 17 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, with a not to exceed Liquidated Damages Cap of XX.X% of the total contract value.

Commented [CD1]: NOTE TO PURCHASER:

XX% will be determined based on contract risk and record 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/.

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

k. Any liquidated damages assessed under this Contract may, at the Department's option, be deducted from any payments due the Contractor. The Department has the right to offset any liquidated damages payable to the Department, as specified above, against any payments due to the Contractor. If insufficient payments are available to offset such liquidated damages, then the Contractor will pay to the Department any remaining liquidated damages within fifteen (15) calendar days following receipt of written notice of the amount due.

18. Disclosure of Security Breach

Without limitation on any other provision of this Contract regarding information security or security breaches, the Contractor shall provide notice to the Department's Project Manager and the CISO as soon as possible following the Department's discovery or reasonable belief that there has been unauthorized exposure, access, disclosure, compromise, or loss of sensitive or confidential Department information ("Security Incident").

a. Within twenty-four (24) hours of the discovery or reasonable belief of a Security Incident, the Contractor shall 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 Department information involved;
3) Who may have obtained the Department information;
4) What steps the Contractor has taken or will take to investigate the Security Incident;
5) What steps the Contractor 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, the Contractor shall 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 the Department's information;
   2) Whether there is any knowledge if the Department information has been abused or compromised;
   3) What additional steps the Contractor has taken or will take to investigate the Security Incident;
   4) What steps the Contractor has taken or will take to mitigate any negative effect of the Security Incident; and
   5) What corrective action the Contractor has taken or will take to prevent future similar unauthorized use or disclosure.

c. The Contractor shall confer with the CISO regarding the proper course of the investigation and risk mitigation. The Department reserves the right to conduct an independent investigation of any Security Incident, and should the Department choose to do so, the Contractor shall cooperate fully by making resources, personnel, and systems access available to the Department and the Department's authorized representative(s).

d. Subject to review and approval of the CISO, the Contractor shall, 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 the Department, in its sole discretion, elects to send its own separate notice, then all costs associated with preparing and providing notice will be reimbursed to the Department by the Contractor. If the Contractor does not reimburse such costs within thirty (30) calendar days of the Department's written request, the Department will have the right to collect such costs.

19. Cyber Insurance Requirement

The Contractor shall maintain sufficient cyber insurance to cover any and all losses, security breaches, privacy breaches, unauthorized distributions, or releases or uses of any data transferred to or accessed by the Contractor under or as a result of this Contract.

a. This insurance will provide sufficient coverage(s) for the Contractor, the Department, and affected third parties for the review, repair, notification, remediation and other response to such events, including but not limited to, breaches or similar incidents under Chapter 521, Texas Business and Commerce Code.

b. The Department may, in its sole discretion, confer with the Texas Department of Insurance to review such coverage(s) prior to approving them as acceptable under this Contract.

c. The Contractor shall obtain modified coverage(s) as reasonably requested by the Department within ten (10) calendar days of the Contractor's receipt of such request from the Department.

20. Representations and Warranties Related To Software

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

a. The Contractor 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 but not limited to Software Updates, Software Patch/Fix, or Software Upgrades, provided under this Contract are void and have no effect unless the Department specifically agrees to each licensure term in this Contract.

c. The Software provided under this 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 this Contract will 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 this Contract does not and will 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 the Contractor to access the Software to cause such disablement or impairment (sometimes referred to as "trap door" devices").

21. Rights to Data, Documents and Computer Software (State Ownership)

a. Any biographic data, demographic data, image data inclusive of fingerprints, photograph and signatures or any other data or metadata in any form acquired or accessed by the Contractor in the performance of its obligations under this Contract will be the exclusive property of the Department and all such data will be delivered to the Department by the Contractor upon completion, termination, or cancellation of this Contract.

b. The Contractor will not use, willingly allow, or cause to have such data used for any purpose other than the performance of the Contractor's obligations under this Contract without the prior written consent of the Department.

c. The ownership rights described herein will include, but not be limited to, the right to copy, publish, display, transfer, prepare derivative works, or otherwise use the works.

d. The Contractor shall provide, at no additional charge, appropriate licenses for the Department to use and access, as necessary for the Department to use and access the turnkey Solution during the term of the lease, the Contractor's pre-existing software or other intellectual or proprietary property that the Contractor determines is necessary to facilitate the performance of the Contractor's obligations under this Contract.