DEPARTMENT OF PUBLIC SAFETY
OF THE STATE OF TEXAS

Request for Information
RFI# CRD202206091531

Mobile Biometrics Identification Devices

1. INTRODUCTION/OBJECTIVE/PURPOSE

The Department of Public Safety (DPS) publishes this Request for Information (RFI) seeking current information related to mobile biometric identification devices (Mobile ID). DPS may use the collected data to determine functionality offerings and build requirements around the needed functions.

1.2 Agency Liability and Confidential Information

This RFI is only a request for information and no contractual obligation on behalf of the DPS whatsoever will arise from the RFI process. It does not constitute a Request for Proposal (RFP), Request for Offer (RFO), Pricing Request (PR), Invitation for Bid (IFB), or other solicitation, nor does it constitute the commitment to issue any solicitation in the future. Therefore, those choosing to respond to this RFI will, merely by virtue of submitting such a response, NOT be deemed to be "bidders" in any sense, and no such respondent will have any preference, special designation, advantage, or disadvantage whatsoever in any subsequent procurement process related to this RFI.

This RFI does not commit the DPS to pay costs incurred in the preparation or submission of any response to the RFI. It is the responsibility of the potential respondent to monitor the Electronic State Business Daily for additional information pertaining to this RFI.

Pursuant to §552.301 (c) of the Public Information Act (PIA), the following email address has been designated for public information requests: OGC.Webmaster@dps.texas.gov. Respondents are advised that materials contained in their response are subject to the aforementioned section of the PIA. **Note:** A request emailed to any other DPS email address does not trigger the requirements of the PIA.

If Respondent asserts that any material in the response is confidential or proprietary information, Respondent must clearly mark the applicable pages of respondent's submission in boldface type to indicate each claim of confidentiality and include the words "confidential" at the top of the page. Additionally, Respondent must include a statement on company letterhead identifying all Response section(s) and specific pages(s) that have been marked as confidential and explain why the information is marked as confidential and excepted from public disclosure under the provisions of the PIA. Merely making a blanket claim that the entire Response is protected from disclosure because it contains some proprietary information is not acceptable and will make the entire Response subject to release under the PIA.

1.3 Background Information

Fingerprint and other biometric comparison technology provide a modern approach to a science that used to involve printing individuals on heavyweight paper and manually comparing those prints to others in a repository looking for a match. Current technology identifies individuals by matching submitted fingerprints and biometrics, primarily captured by Livescan devices in a booking environment to those in the state's fingerprint repository. DPS is requesting information from vendors about the capabilities of mobile identification devices and software that can be used by law enforcement officers during traffic stops or investigations to quickly identify individuals of interest.

This RFI seeks to identify technical specifications and other information as well as unique qualities or benefits of individual devices or systems (solutions). Responses will be reviewed with the goal of developing a solicitation for eventual award by DPS.

2. SCHEDULE OF EVENTS AND TIMELINES

RFI issue date	06/30/2022
Deadline for questions/clarifications to the RFI (Close of Business)	07/06/2022
Deadline for responses to questions/clarifications (Close of Business)	07/08/2022
Deadline for submission of RFI	07/15/2022

To maintain the integrity of the RFI process, all communications with respondents pertaining to this RFI must be referred to and/or coordinated with the DPS point of contact referenced below. Communicating with any other DPS personnel may result in disqualification of the respondent's response.

A. Instructions to Recipients

1. You are requested to provide responsive information related to the general requirements and questions in Section 3. GENERAL REQUIREMENTS below and return it to the address below by 07/15/2022, @ 5:00 P.M. CST.
2. Respondents responding to this RFI may be requested to make a demonstration/presentation of products/services following the deadline for submission upon request by DPS. DPS will not be responsible for expenses incurred by a respondent in the preparation and submission of information. This provision also includes any costs involved in providing an oral presentation/demonstration of product/services**.**
3. Please list the general requirement or question (included below) before each response.
4. All questions/clarifications must be submitted on or before 07/06/2022.

B. Electronic transmission via email is required for questions and clarifications.

DPS is not currently accepting any in-person solicitation responses. DPS will only accept timely emailed responses. DPS will not consider a hard copy response. The response should be submitted to the attention of:

Contract Specialist: Linda Mahan, CTCD, CTCM
Email: Linda.Mahan@dps.texas.gov
Phone: (512) 424-7096

3. GENERAL REQUIREMENTS

A. Devices must be included on the Federal Bureau of Investigation's list of approved devices, https://fbibiospecs.fbi.gov/certifications-1/cpl, and have specifications with 500 pixels per inch (PPI), or have personal identity verification (PIV) specifications. Devices should have a fingerprint acquisition profile (FAP) of 30 or greater. Specifications can be found at https://fbibiospecs.fbi.gov/ebts-1/approved-ebts .

B. Mobile ID should accept, process, and respond to fingerprint identification requests that contain between 2 and 10 images of fingers. The recommended fingers for mobile ID searches are 2 and 7 (the index fingers). General mobile ID information can be found at https://www.dps.texas.gov/section/crime-records-service/mobile-id .

C. Solution must comply with the Federal Bureau of Investigation Criminal Justice Information System (CJIS) Security guidelines, DPS Information Technology Standards and Requirements, and Cyber Security Contract Requirements.

D. Solution must be based on current industry software design principles and architecture that have active support mechanisms, which are not at or near the end of life for support and must be flexible enough to anticipate the growth expectations and complexity of the processes required for law enforcement.

E. DPS is interested in Respondents' input into the possibilities of other technologies and/or services that are not specifically mentioned in this RFI, but which may enhance the implementation or functionality of the Mobile ID solution. This may include an implementation plan that could include your approach/strategy, deliverables, and schedule to reduce overall costs to manage, and/or maintain the new Mobile ID solution.

#	Feature	Description
1	Operating Systems	Must be able to run on iOS, and/or Android, operating systems
2	Retention of data/auto-purge	Rules for records retention and automatic destruction when retention period expires
3	Customized results format	Allow DPS to customize the output format
4	Statistical reports	Provides reports defined by DPS
5	Interfaces	Multiple interface development and maintenance from systems internal to DPS and external, including the criminal history repository.
6	Failure notification	Notify system administrators of any system or program errors or failures.
7	Notifications	System notifications and banners

4. RFI QUESTIONS

DPS is requesting respondents consider the following questions when deciding to respond.

A. How does your solution meet the above general requirements and contain the listed features?
B. How does your device access and maintain connectivity to the internet? These devices will be used in all parts of the state so access in remote areas is a priority.
C. Can the responses be delivered to devices other than the Mobile ID device used for submission (i.e. phones, tablets, laptops, etc.)?
D. How much experience does your company have with a multitude of connections and interfaces? Please explain and/or provide examples of your product in other states.
E. What CJIS security-compliance encryption experience does your company have? What are your system's encryption options?
F. Will additional third-party software be required? If so, do you have access to correct any issues with the software as it pertains to your solution?
G. Are any system or sub-system functions administered by a third party? If so, how do you handle any issues, releases, updates, etc.?
H. Has your system been implemented at local, state, and federal levels? Explain your implementation methodology and experience with each level, including the number of devices deployed.
I. Does the mobile ID device need to be connected to a secondary device to process the fingerprints?
J. Are there any additional hardware, software, or peripherals that are required to utilize your device?

5. TIMETABLE

The respondent's response shall include a timetable that will include product configuration deployment, testing, and acceptance.

6. LIMITATIONS

Changes may occur between the publishing of this RFI and any subsequent RFIs. There also may be differences between this RFI and other relevant documents.

Respondent's staff must be able to pass requisite background checks to participate in the project.

7. INDUSTRY DISCUSSIONS

DPS representatives may or may not choose to meet with potential respondents. Such discussions would only be intended to get further clarification of potential capability to meet the requirements, especially any development and certification risks. Virtual presentations and product demonstrations may be requested from the respondents.

8. SUMMARY

THIS IS A REQUISITION FOR INFORMATION (RFI) ONLY to identify technical specifications and other information as well as unique qualities or benefits of individual systems for Mobile ID. The information provided in this RFI is subject to change and is not binding by the DPS. Any additional forms included with this RFI document are for reference and informational purposes only. DPS has not made a commitment to procure any of the items discussed, and release of this RFI should not be construed as such a commitment or as authorization to incur cost for which reimbursement would be required or sought. All submissions become DPS property and will not be returned.

9. RESPONDENT INFORMATION

Respondents must provide the following:

Company Name:	
Street Address:	
City/State/Zip:	
RFI Point of Contact:	
Title:	
Phone:	
Email:	
Company Web Page Address:	

NOTE: The respondent acknowledges that they have read all instructions carefully. Failure to complete all requirements as outlined in this RFI, sign and submit in accordance with Section 2 Schedule of Events and Timelines may result in disqualification of the respondent's response.

RESPONDENT SIGNATURE(S)

_______________________________________ _________________________ ________

Signature of Authorized Representative Name – Printed Date

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM
Legal Authority for and Purpose and Genesis of the Security Addendum

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

> 1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.
>
> We are therefore proposing to revise 28 CFR 20.33(a) (7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental

> agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.
>
> The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

> § 20.33 Dissemination of criminal history record information.
>
> a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
>
> 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
>
> 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
>
> 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United

> States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director's designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1)under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes.

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Assistant Director
Criminal Justice Information Services Division, FBI
1000 Custer Hollow Road
Clarksburg, West Virginia 26306

DPS INFORMATION TECHNOLOGY (IT) STANDARDS AND REQUIREMENTS

Table of Contents

1.1 DEFINITIONS

A. **API** means Application Programming Interface.

B. **AWS** means Amazon Web Services.

C. **Business Continuity and Disaster Recovery Plan** means a documented set of plans related to preparations and associated activities which are intended to ensure that an organization's critical business functions will either continue to operate despite serious incidents or disasters that might otherwise have interrupted them, or will be recovered to an operational state within a reasonably short period of time.

D. **Change Control Board** means the DPS work group responsible for coordinating any requested change to existing DPS systems.

E. **Change Order** means a document used to capture customer and job information summarizing any labor or materials used to complete the task.

F. **Change Request** means the formal process to initiate and manage the Change Order process.

G. **Cloud Hosted or Cloud Services** means a service available to users on demand through the Internet from a cloud provider's servers or services as opposed to an agency's on-premises servers.

H. **Contract File** means the official DPS set of documents pertaining to the Solicitation, award and monitoring of the awarded contract housed within DPS's Procurement and Contract Services (P&CS) Bureau's official contract repository.

I. **Vendor-Hosted** means a combination of traditional IT functions to be provided by the Vendor such as infrastructure, applications Software (including COTS Software Solution), security, monitoring, storage, and provider of Hardware and Hardware Maintenance.

J. **COTS** means Commercial off the Shelf Software.

K. **Hardware** means the physical elements of a computing system including the physical components thereof.

L. **Hardware Maintenance** means the Hardware is maintained to run efficiently, increase component lifespan, decrease the likelihood of Hardware failure and replace hardware, should it fail.

M. **Hardware Refresh Plan** means the implementation of hardware which has reached end of life and no longer supported that will be replaced.

N. **Information Technology (IT) Division** means the DPS's Division which is responsible for agency technology innovation, maintenance, and support as applicable.

O. **Internet Service Provider (ISP)** means a company that provides Internet services, including personal and business access to the Internet.

P. **Maintenance** means the act of keeping the System in good condition by making repairs, applying updates or upgrades, addressing problems, etc. to ensure that the System continues to meet user requirements in their present operating context.

Q. **Mobile Device Management (MDM) Software** means a type of security Software used by an IT department to monitor, manage and secure employee's mobile devices that are used in the organization.

R. **Performance Standards** means a measurable threshold, requirement, expectation against which actual levels of performance are appraised to gauge efficiency and effectiveness.

S. **Preventive Maintenance** means the care and services by personnel for the purpose of maintaining equipment, and facilities in satisfactory operating condition by providing for systematic inspection, detection, and correction of incipient failures either before they occur or before they develop into major defects.

T. **Publicly owned** (in this context) means desktop or laptop PCs and mobile devices, phones and tablets that are owned by other than DPS or the Vendor.

U. **Recovery Point Objective (RPO)** means the point in time to which data must be recovered after an outage.

V. **Response Time** means the total amount of time it takes to respond to a request for service.

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

X. **Service Level Agreement (SLA)** means an exhibit to the awarded contract that contains performance standards that govern the work under the contract.

Y. **Service Level Standards** means the Performance Standards that govern work under the contract which are interspersed within the contract document itself in the absence of an accompanying SLA Exhibit and include the Basic Service Level Standards as defined in Section 1.4 of this Exhibit.

Z. **Severity Level** means a defining classification scheme for all issues with corresponding resolution times.

AA. **Software (SW)** means any application programs for the exclusive use with the System.

BB. **Software Defect Severity** is defined in five classifications. Each classification and its corresponding definition is as follows:

   a. BLOCKER – When running of test cases is stopped because of the defect or when the application is not working at all.
   b. CRITICAL – When a large number of test cases are affected by the defect or a major application failure has occurred. Example: A new feature is not working at all.
   c. MAJOR – Denotes a defect the affects the overall functioning of a feature. Example: A new feature is not working as specified; or an ungraceful functionality failure.
   d. MINOR – Indicates when the impact of a defect is less important to the overall health of the feature or application but is required to meet the specifications. Example: a usability issue; user interface inconsistency; or an uninformative or missing error message.
   e. TRIVIAL – Indicates a defect of little importance.

CC. **Software Maintenance** means modification of a Software product after it is operational to correct faults, to enhance capabilities, to improve performance or other attributes.

DD. **Software Refresh Plan** means the implementation of software that has either been deprecated, updated or replaced.

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

FF. **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.

GG. **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.

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

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

JJ. **System Failure** means a breakdown of any System Hardware, operating system, or application Software which prevents the accomplishment of the System's intended function.

KK. **System Functionality and Operational Effectiveness** means that the System is performing at the levels specified within this Contract.

LL. **Test Cases** means a specific executable test that examines all aspects including inputs and outputs of a system and then provides a detailed description of the steps that will be taken, the results that will be achieved, and other elements that will be identified.

MM. **DPS-Hosted** means a combination of traditional IT functions to be provided the Department such as infrastructure, applications Software (including COTS Software Solution), security, monitoring, storage, provider of Hardware and Hardware Maintenance, and email, over the internet or other Wide Area Networks (WAN).

NN. **UAT** means User Acceptance Testing.

OO. **Unit Testing** means a Software testing method by which individual units of source code, sets of one or more computer program modules together with associated control data, usage procedures, and operating procedures are tested to determine whether they meet specifications.

PP. **Utility or Utilities** means Software that performs a very specific task that provides an addition to the capabilities provided by the System. Utility Software is designed to help analyze, configure, optimize or maintain a computer or application but is not essential to the operation of the System.

1.2 INFORMATION TECHNOLOGY (IT) STANDARDS AND REQUIREMENTS

The Vendor must comply with the following DPS IT standards and requirements, as applicable to this Contract. The Vendor must also comply with any DPS or state amended standards and requirements throughout the term of this Contract, including any renewal or optional Contract periods.

The Vendor's systems must comply with DPS standards and requirements when there is a need to migrate from a Vendor-hosted infrastructure to a DPS-hosted infrastructure.

All requests for documentation, narratives, diagrams, exceptions, etc., identified in the sections below, must be submitted with the Vendor's Response.

1.2.1 Vendor-Hosted System or DPS-Provided Cloud-Hosted System

A. System and Architectural Documentation

The Vendor must provide, within its Response, documentation for a Vendor-hosted system consisting of the following:

- An overall narrative for any System which is hosted within the Vendor's computing infrastructure or within the DPS provided cloud infrastructure;
- Narratives and detailed diagrams for the following:
    - Product architectural diagram;
    - Security diagram(s) (including security diagrams for database, network, application, etc.);
    - Network diagram;
    - Communications port diagram; and
    - For cloud-hosted, provide an inventory of cloud-based products and services required to support the bulleted items above; and
- An itemized list of any assumed capabilities of DPS IT systems required to access or support the Vendor's proposed product(s) or solution(s).

B. Server, Workstation, Peripheral Documentation

The Vendor must provide, within its Response, an inventory for a Vendor-hosted System for the components listed below.

- Any applicable server Hardware will identify:
    - The processor requirements;
    - The memory requirements;
    - Operating system details and dependencies; and
    - Data storage requirements.
- All workstation requirements will identify:
    - The processor requirements;
    - Display requirements;
    - The memory requirements;
    - Operating system details and dependencies;
    - Data storage requirements; and
    - Any support applications required such as Internet Explorer, Adobe PDF Reader, etc.
- Peripherals required will be identified, including:
    - Printers;
    - Scanners; and
    - Fax.

C. Desktop, Laptop, Mobile Device Documentation

The Vendor must provide, within its Response, how its System will support each of the following items. The Vendor must also document any exceptions.

- DPS-issued desktop or laptop PCs
  - Current Microsoft Enterprise Operating System
  - Current Enterprise Operating Version of Internet Explorer
  - Current Enterprise Operating Version of Microsoft Edge
  - Current Enterprise Operating version of Firefox
  - DPS does not support Google Chrome
- DPS-issued Mobile Devices
  - IOS Smart tablet (latest available for purchase)
  - IOS Smart phone (latest available for purchase)
- Publicly owned desktop or laptop PCs
  - Current Microsoft Enterprise Operating Version
  - Current Enterprise Operating version of Mac OS X
  - Current Enterprise Operating version of Internet Explorer Current Enterprise operating version of Safari
  - Current Enterprise Operating version of Firefox
  - Current Enterprise Operating version of Google Chrome
- Publicly owned mobile devices, phones, and tablets
  - Using Current IOS supported version
  - Using Current Android supported version

1.2.2 DPS-Hosted System

A. System and Architectural Documentation

The Vendor must provide, within its Response, documentation for a DPS-hosted System consisting of the following.

- An overall narrative for any System which is hosted within the DPS-provided infrastructure.
- Narratives and detailed diagrams for the following:
  - Product architectural diagram;
  - Security diagram(s) (including security diagrams for database, network, application, etc.);
  - Network diagram;
  - Communications port diagram; and
  - For cloud-hosted, provide an inventory of products and services required to support the bulleted items above.
- An itemized list of any assumed capabilities of DPS IT systems required to access or support the Vendor's product or System.

B. DPS Standards and Requirements for Software/Hardware

The Vendor must follow the DPS standards and requirements for any Software or Hardware that are to be hosted within the DPS infrastructure. The existing DPS infrastructure framework supports several industry standard products and platforms. All Works for Hire created for DPS as part of this contract must be stored on DPS's local source code management repository, BitBucket. In addition, any application artifacts must be stored in DPS's Artifactory repository. The Vendor will use the agency's CI/CD pipeline and tool chain for build and deployment automation.

The Vendor must identify, within its Response, the products required to properly support the System in the DPS infrastructure.

The Vendor must provide, within its Response, an inventory for the DPS-hosted System consisting of the following.

- Required Hardware platforms and operating system to support the proposed System
  - The processor requirements
  - The memory requirements
  - Operating system details and dependencies
  - Data storage requirements
  - AWS or Azure Cloud services product equivalent, if applicable
- Required application server platforms
  - The processor requirements
  - The memory requirements
  - Operating system details and dependencies
  - Data storage requirements
  - AWS or Azure Cloud services product equivalent, if applicable
- Required web server platforms
  - The processor requirements
  - The memory requirements
  - Operating system details and dependencies
  - Data storage requirements
  - AWS or Azure Cloud services product equivalent, if applicable
- Required support services such as email servers, etc.
  - The processor requirements
  - The memory requirements
  - Operating system details and dependencies
  - Data storage requirements
  - AWS or Azure Cloud services product equivalent, if applicable

The Vendor must provide, within its Response, its ability to support each of the following DPS standards. The Vendor must also document any exceptions to our standards.

- DPS-provided infrastructure only allows the following database platforms.
  - AIX DB2 11 on premise
  - SQL Server 2016 or N-1 (N = current Microsoft SQL release)
  - AWS RDS services and Azure SQL cloud database services
- DPS-provided infrastructure report services use
  - Microsoft SQL Server Reporting Services
  - AWS and Azure Cloud Services reporting tools
- DPS-provided infrastructure platform services use
  - Current VMWare (ESXi) supported version
  - AWS or Azure Cloud services infrastructure products

1.2.3 Intersystem Communication Standards

The System will support integration with other applicable DPS systems using standard web services, provide Application Programming Interface (API) tools that can be incorporated into DPS applications, or secure file transfer protocol with data encryption.

1.2.4 Network Topography

DPS uses a combination of public and private TCP/IP network resources. All internal communications between client resources, other systems, and system services will be through this network. The Vendor's System will use standard TCP/IP network access ports. The System will be accessible on Port 80 for standard web browser access and Port 443 for secure web browser support.

The Vendor must provide, within its Response, documentation on each of the following, as applicable.

- An estimate on the amount of bandwidth or formulas to calculate usage required to support the number of expected internal DPS Users and volume of work.
- For a Vendor-hosted System, the Vendor must provide, within its Response, narrative on how adequate network capacity for DPS Users and External, non-DPS Users will be delivered.

1.2.5 Workstation Software Installation Packaging

The Vendor must provide, within its Response, its level of compliance with the Workstation Software Installation Packaging requirements listed below. The Vendor must also document any exceptions.

If a Software system is client-based and needs to be installed on each computer, the Vendor must provide the client Software in an .msi format, compatible with the current version of Windows Installer (and n-2), which allows for full control over the installer user interface, as defined by Microsoft for Windows-based systems. Any Vendor-supplied .msi will fully support distributed deployment through the System Center Configuration Manager (and n-1) Application Model. OS X applications will support Apple Application installation package standards. Any Software required for mobile devices will be available from the appropriate App store based on the device operating system. Mobile device Software will also be compatible with Mobile Device Management (MDM) Software distribution tools currently used by the Agency.

1.3 MAINTENANCE AND SUPPORT

The Vendor must, within its Response, indicate its level of compliance with each of the following Maintenance and Support standards. The Vendor must also document any exceptions.

The Vendor must provide a Software Maintenance system that includes the following.

Support for the System to include Software changes that the Vendor develops for DPS or makes available to DPS as managed in accordance with this Contract, including any Service Level Agreement (SLA) or Service Level Standards.

Preventive scheduled and unscheduled System diagnosis and correction of faults as well as modification of the Software to maintain the SLA or Service Level Standards.

A web-based support portal for DPS to report minor problems which will be available 24 hours per day, seven days per week, and 365 days a year with a searchable knowledge base for known issues. Response to reported problems will be managed as defined in the SLA or Service Level Standards.

Maintenance services to resolve usability problems to include bugs, security issues, installation of Software updates, and major Software releases.

New Software versions or releases occurring in the normal Maintenance yearly support as referenced in this Solicitation. These Software versions or releases will be provided to DPS at no additional cost.

1.3.1 Software Updates

The Vendor must provide periodic Software updates to incorporate corrections of any defects or implement enhancements to the System's Software.

- Scheduled and unscheduled Software updates released by the Vendor will be installed during periods of the Maintenance window as mutually agreed upon by DPS and the Vendor.

- Updates to documentation or manuals resulting from Software updates will be provided or made available upon DPS request.

1.3.2 Hardware Maintenance

The Vendor must provide Maintenance services for Hardware equipment owned by the Vendor that is installed to support a Vendor's Hosted System.

A. If the Vendor Proposes to Use the DPS Provided Cloud-Hosting Option
This Hardware Maintenance section will not be applicable and should be so noted in the Vendor's response.

B. Scheduled Hardware Maintenance Notification
The Vendor must provide notice to DPS a minimum of ten business days prior to scheduled Maintenance including length of anticipated downtime plus the description or purpose of scheduled Hardware Maintenance.

C. Unscheduled Hardware Maintenance Notification
The Vendor must provide notice to DPS as soon as the Vendor is aware of an issue, prior to unscheduled Hardware Maintenance including length of anticipated downtime plus the description or purpose of unscheduled Maintenance.

D. Preventive Maintenance

1. The Vendor must provide Preventive Maintenance services in order to maintain the System in good condition and working order on a mutually agreed upon, scheduled basis.
2. The Preventive Maintenance schedule is to be based on the Vendor's and DPS's mutual agreement of the particular service required for each System Component, it being understood that this schedule will be oriented to avoid periods when the System is expected to have the heaviest use.
3. During the term of this Contract, DPS may, by providing five calendar days' prior written notice, select any alternative period of Maintenance coverage whether or not such alternative represents an increase or decrease in service.

E. Remedial Maintenance
The Vendor must provide remedial Maintenance to the System on a 24-hours-per day, seven-days-per-week basis, with a Response Time in correspondence with the SLA specified for the system.

1.3.3 Change Control Participation

A. Changes to the System will be subject to the DPS Change Control Board (CCB) process. This requirement is mandatory for Vendor-hosted and DPS-hosted solutions. DPS will initiate and manage the Change Control process. A DPS change coordinator will be assigned as the DPS project representative who is responsible for coordinating and communicating any proposed changes to a production environment.

B. The purpose of DPS IT Change Management (CM) is to ensure that Change Requests (CRs) to DPS IT systems are properly reviewed, authorized, implemented, and tracked with minimum disruption to service levels in order to ensure accountability, communication, transparency, and visibility. The Vendor must submit CR details to the DPS change coordinator detailing in Release Notes what is changing and where it is changing, and why it is changing, along with test plans, test results, and communication processes for before and after a change. DPS reserves the right to delay implementation of a change, stop a change in progress and deny a change to systems. There are two types of change requests.

C. Change of Data Model

1. DPS must approve any changes to Vendor's data model before, during, and after implementation.
2. Vendor-initiated data model changes occurring after original system implementation must be reported to the IT/DPS's Contract Monitor for the contract, and follow the DPS change control process.
3. Vendor agrees to support and comply with any DPS-initiated data model changes.

D. Standard CRs

Standard CRs follow the "normal" change request process. This means these changes will be approved by the DPS CCB prior to being released to a production environment.

E. Emergency CRs

Emergency CRs follow an abbreviated version of the DPS CCB process. The following are examples of what are considered Emergency CRs.

1. Production system down
2. Multiple users/sites affected
3. Misprocessing data
4. Security risk

1.3.4 Service Outage Escalation and Communication Plan

The Vendor must provide, within its Response, a draft Service Outage and Escalation Communication Plan. The draft Communication Plan will specify the service outage notification and escalation process including how DPS is expected to notify the Vendor. Upon contract award, DPS and the Vendor will finalize a Service Outage and Escalation Communication Plan.

1.3.5 Application Outages, Release Rollbacks and Degradation in Performance Reporting

Works for Hire must follow the requirements of this section when a solution has a (1) significant degradation in performance; (2) application outage; or (3) a software release must be rolled back due to defects or issues in the software release.

A significant degradation in performance is defined as a user being unable to use the solution because the performance of the system is degraded to a point to where the application does not perform as defined in the Response Time section of this document.

Application outages are defined as an unplanned disruption of the software solution that prevent the application user from accessing or using the application. This excludes application outages that are due to a network service outage that made it impossible for a user to access the application.

Software release rollbacks are defined as the rollback or removal of a software release or software update that had been previously approved through the Agency Change Control process and deployed into a production environment.

A Vendor must complete the following assessment and send to the Contract Monitor for review and approval.

Outage Event Name: [Type outage event name here]
Outage Date: [Type outage start date and end date here – format MM/DD/YYYY HH:MM – MM/DD/YYYY HH:MM] (Military time please)
Related Change Request: [Type CR number here – format CR ####
Purpose of CR: [Type the purpose of the CR here from the actual CR ticket]
Outage Description: [Type the outage description here – please have enough high-level detail so it makes sense to the potential reader]
Outage details:
[Type a highly-detailed description of what happened during the outage]
Outage Impact:
[Describe the timeline of the outage and the user impact]
Future Prevention Steps:
[Detail the steps for preventing this outage in the future – numbered bullets are preferred if specifically ordered steps are required]

1.4 BASIC SERVICE LEVEL STANDARDS

The purpose of these Basic Service Level Standards, Section 1.4, is to ensure that the proper elements are in place to provide DPS with the optimal level of System performance. These Basic Service Level Standards define the requirements, responsibilities, and obligations of DPS and the Vendor.

Additional standards are located throughout this Exhibit and Solicitation – if any, and include Section 1.3, Maintenance and Support; Section 1.5, System Performance; Section 1.6, System Training Plan for Technical Staff; and Section 1.7, Testing Requirements, Implementation and Acceptance.

1.4.1 System Production Control

The Vendor must schedule production management such as batch processing, job scheduling, automated import/exports, etc. at intervals agreed upon between the Vendor and DPS.

The production control schedule will be mutually agreed upon by both the Vendor and DPS and will be oriented around periods when the System is expected to have the lightest use.

1.4.2 Customer Support

The Vendor must support all Software licensed to DPS for use during the term of this Contract.

The Vendor must provide a toll-free telephone or email accessibility to DPS for the System, Monday through Friday, 7:00 a.m. to 9:00 p.m., Central Time, excluding state or federal holidays. A list of the DPS holiday schedule is available upon request. These days and times may change at the discretion of DPS with 24 hours’ notice. The Vendor must provide the DPS Contract Monitor a means to report trouble outside of normal hours.

A. System support for DPS includes responsibilities such as:

- DPS employee training for the system
- System configuration
- System navigation
- Data query or export procedures
- Search criteria, best practices, parameters, etc.
- Troubleshooting for System Hardware, System Software, network, etc.

B. System support for DPS excludes responsibilities such as:

- Record content
- Record quality
- Record interpretation
- Employee administration (including new accounts, password creation or resets)

- Non-system Software owned, purchased, installed, developed or used by DPS or DPS's Hardware
- DPS's/User's Internet Service Provider (ISP) or other internal method of access.

1.5 SYSTEM PERFORMANCE

1.5.1 Basic Requirements

The Vendor must maintain optimal System performance 24 hours per day, seven days per week, 365 days per year at a rate of 98% (the Rate) as calculated by Calculation of System Performance Rate below.

The Vendor is cautioned to quickly resolve the source or sources of failure. Inability to meet or exceed the Rate in any 12-month period may, at DPS's sole discretion, result in the following actions.

- First Remedy: Verbal warning.
- Second Remedy: Written warning added to the Contract File.
- Continuing Remedy: DPS may begin exercising Contract remedies.

1.5.2 Calculation of System Performance Rate

The Vendor must measure the System performance rate by the amount of time the System is unavailable (downtime) during a calendar month. This metric gauges the System performance as a percentage of available hours tracked to the quarter of an hour (rounded). The rate of System performance will be measured and monitored as follows in this Section.

Available hours equal the total number of hours in a month (24 hours multiplied by the number of days in the month) minus the actual amount of time spent to the quarter of an hour for scheduled Maintenance for the application. Downtime is the total number of hours (rounded to the quarter hour) during which the System is not in operation.

System Performance Rate equals downtime hours divided by available hours.
For example, take the month of January:

Available time per month was 744 hours (31 days X 24 hours);
Downtime per month was 3.75 hours (start 1:00 am - end 4:40 am);
744.00 – 15 = 729; and
729 ÷ 744 = 98%.

1.5.3 Response Time

The Vendor must maintain response times that fall within benchmarks set by industry standards. Response times for Government applications will be between 0.3 seconds and no longer than eight seconds. Response times will be reported as the average of the total response time for a quarterly period. Time period used in calculating the rate will be used to calculate the Response Time average. The Vendor must provide performance metrics based on the applications performance for the period specified.

For Vendor-hosted Systems, the Vendor must provide monitoring tools and reports that DPS can access to verify capacity and throughput.

1.5.4 Data Backups

The Vendor or the System must perform backups on all System records once every 24 hours, seven days per week, and 365 days per year to facilitate data and System restoration in the event of any failures. The data backup schedule will be mutually agreed upon by both the Vendor and DPS and will be performed when the System is expected to have the lightest use. Data and System Backups should be based on the business's recovery point objective (RPO).

The Vendor or the System must be able to restore to development or test environments and must demonstrate the operability of a backup during the testing phase of the project.

1.5.5 Recovery Points

The Vendor must, within its Response, provide Business Continuity Plan (BCP) documentation for each of the following.

A. System Crashes

- System crashes will be resolved within four hours of initial notification.
- Any exceptions to the four-hour resolution requirement will be documented and will require email notifications explaining the reason for any delays to the DPS IT Chief Information Officer (CIO) and the contract monitor.

B. Physical Infrastructure

Vendor must provide DPS with a location-independent restoration plan, including an Information System Contingency Plan (ISCP) that describes the policies, procedures, and processes required to recover a system at the current or alternate location, regardless of its hosted location.

1.5.6 Hardware and Software Refresh Plans

Hardware Refresh Plans will not be applicable for cloud solutions; however, Software refresh plans will need to be addressed as documented below.

Vendor must provide, within its Response, documentation for the following.

A. Vendor-Hosted System

The Vendor must ensure that all operating systems, hardware, software versions, databases, and tools must be kept current, using an "N – 1" model, unless a specific version is specified in the current IT Technology Standards. Such as the current Microsoft Operating System Model, N - 1 refers to the Major Build Number (such as Windows 10, Build 1709, 1605).

The Vendor must provide Hardware and Software Refresh Plans to address end-of-support or end-of-life products. The plan will address System and application patches and implementation methodology and schedule. Refresh of Hardware and Software will be at the sole discretion of DPS.

B. DPS-Hosted System or DPS-Provided Cloud-Hosted System

The Vendor must provide Software refresh plans to address end-of-support or end-of-life products. The plan will address System and application patches and implementation methodology and schedule. Refresh of Software will be at the sole discretion of DPS.

1.5.7 Vendor Business Continuity and Disaster Recovery Plan

Vendor must provide the following to DPS within 30 days or as necessary to update an existing plan:

- Business continuity and disaster recovery plans (BC/DR) to include Information System Contingency Plans (ISCP), a location independent plan that focuses on the procedures needed to recover a system at the current or an alternate location, regardless of hosted location for restoration;
- Appropriate plans, governance and service management to ensure applicable planning, delivery, and support of the organization's IT capabilities supporting business functions, workforce, and customers based on industry acceptable standards (e.g., ITIL v4, COBIT 5, CSA CCM, NIST);
- Evidence that BC/DR plans will be tested at planned intervals (at least once annually) or upon significant organizational or environmental changes; and
- Information system documentation (e.g., administrator and user guides, architecture diagrams) to include the following:
    (a) Configuring, installing, and operating the information system;

(b) Effectively using the system's security features;

(c) Business Continuity and Disaster Recovery Plans (BC/DR) to include a location-independent plan that focuses on the procedures needed to recover a system at current or an alternate location;

(d) Specific actions Vendor will take to meet or exceed DPS's essential functions Recovery Time Objectives (RTO); and

(e) Related artifacts for the methodology, test, training, and exercises (TT&E) used to validate BC/DR plans.

TT&E results and corrective actions identified in annual review of Backup and recovery measures will be incorporated as part of BC/DR and tested accordingly for effectiveness.

The Vendor agrees to meet the SLA or Service Level Standards for all Vendor-provided Services such as:

- Vendor help desk or customer support
- Maintenance services
- Support services (e.g., Software, Hardware)
- Hosting services, if applicable
- Network services, if applicable

1.6 SYSTEM TRAINING PLAN FOR TECHNICAL STAFF

The Vendor must provide, within its Response, a detailed training plan. The plan must explain how the Vendor will train DPS technical staff to support the System. All training will be made available through DPS facilities located in the State of Texas. Training will be interactive so that students have the ability ask the instructor questions during the sessions. The schedule of training sessions will be mutually coordinated and agreed upon by DPS and the Vendor. It is estimated that DPS will receive a negotiated number of training sessions to be conducted during the Base and Renewal Option periods. The requirements of the training plan will address the following.

A. System Administration Training (if applicable)

- Daily operation and Maintenance of the Software
- User administrative duties (e.g., add users, delete users, password administration)
- System configuration
- Monitoring System availability and System status
- System error diagnostics
- System performance monitoring
- Administrative System reports

B. Developer Training (if applicable)

- Skills needed to integrate new data into the Software and to program the Software to develop new capabilities
- How the Software architecture handles various data types
- How the platform scales with users and data
- How the Software features interact with the security model
- How to integrate with internal and external data sources
- Understanding System's APIs to perform common tasks (e.g., exchanging information between the System and other applications)

C. Training Programs

- The Vendor training programs will allow DPS and Vendor to jointly alter the proportion of System Administration and Developer training programs so as to maximize the overall effectiveness of the training for DPS
- The Vendor must scale, detail, and tie training programs to match the System

D. Training Materials

- The Vendor must provide copies for each type of training consisting of the curricula and associated User Guides for acceptance by DPS no less than 15 business days prior to the first training program. The copies will be submitted to the DPS Contract Administrator.
- The Vendor must make available to DPS, video recorded training for each type of training program as a review/refresher resource for DPS personnel who previously completed the live training
- Vendor will transfer ownership of training material to DPS to use internally and with business partners that access Vendor's provided solution.

1.7 TESTING REQUIREMENTS, IMPLEMENTATION AND ACCEPTANCE

All testing activities will include the following.

1.7.1 Implementation and Acceptance

DPS must work closely with the Vendor to ensure requirements are met and completed; however, completion of any one requirement does not constitute full completion and acceptance of the Contract's requirements.

1.7.2 Cloud-Hosted Infrastructure Environment

DPS requires that all Cloud-hosted implementations that are deployed solely for the support of this contract use Infrastructure as Code to allocate cloud resources. The use of Infrastructure as Code is not required for SaaS products that include cloud hosting resources as part of a standard deployment which is used for all customers of the Vendor's SaaS product.

- All cloud service application deployments that are targeted for the cloud service provider's Gov Cloud must be built using the available CJIS templates as a basis.
- All cloud services application deployments that are targeted for the cloud service provider Public Cloud must be built using the available NIST 800-53 templates as a basis.
- The Infrastructure as Code templates must be able to deploy Development, Test, UAT, and Production environments from the same template by submitting multiple iterations with input parameters to specify the unique properties of each environment.
- The Infrastructure as Code template must be kept in a DPS-owned source repository.
- All Infrastructure as Code templates must include all required components required for the proper operation and auditing of the application. This includes:
  - all VPC and network configurations for subnets, route tables and access control lists;
  - all compute resources and load balancers;
  - all applicable Security Groups;
  - any cloud services database services such as RDS or DynamoDB;
  - all storage resources and applicable security policies;
  - all applicable alerts and notifications; and
  - all applicable cloud service Config rules to monitor the account.

DPS requires verification and acceptance as identified in the items below for all Cloud deployments that are specifically built by the Vendor to support the contract. This verification is not required for SaaS products that include cloud services resources as part of a standard deployment that is used for all customers of the Vendor's SaaS product.

- DPS IT resources will be provided all final versions of any Infrastructure as code templates prior to deployment for Production cloud resources. All testing, verification and audit results documentation must be provided to DPS IT prior to the deployment of Production cloud resources.
- DPS resources will perform an audit of deployed production environment to ensure compliance with any applicable regulatory standards prior to loading DPS data.
- DPS resources will perform an audit of any associated cloud services accounts associated with all environments used for DEV, SQA, STG and Production to ensure compliance with any applicable regulatory standards prior to loading DPS data.
- Natural progression of the scripts: Dev, SQA, STG, PROD.

DPS personnel will provide written approval of acceptance of any required Infrastructure as Code templates and cloud services accounts once the auditing and the review process has been completed.

1.7.3 Unit Testing

- The Vendor must provide a listing of Unit Test Cases based on the requirements of this Contract.
- The Vendor must develop automated unit tests in all of its code.
- The Vendor must ensure execution of all units tests in every build.
- The Vendor must also provide DPS with the results of the Unit Test Cases that were executed to completion.
- DPS will be the owner of all automated test cases developed as part of the project.
- Based on the outcome of successful unit testing, the Vendor will advance to the next step of system testing. Successful unit testing will be defined as 100% pass rate of all defined Unit Test Cases with no outstanding issues/defects. The Vendor must perform all these tests in a development environment.

1.7.4 System Testing

- The Vendor must provide to DPS for review and approval by DPS Quality Assurance (QA) testing staff, documented Test Cases that will be performed during Vendor System testing to validate the successful migration and installation of the Software package before any System testing begins.
- The Vendor must perform System testing in the Vendor's QA environment and provide test results to DPS.
- The Vendor must log all defects found during the System testing in the agreed upon defect tracking application.
- The Vendor must investigate any defects found during System testing and participate in defect triage meetings with DPS to determine defect outcome and resolution.
- The Vendor must provide defect fixes in the timeframe as defined in the SLA or Service Level Standards.
- The Vendor must demonstrate all components of the application Software are performing as defined in the System Test Cases and business requirements, including interfaces with other systems (baseline interfaces), in the specified System hardware, operating Software and network environment (system environment).
- Based on the successful outcome of System testing, DPS will advance to Performance Testing. Successful System testing will be defined in the Quality Assurance Test Plan as well as in the Entry and Exit Criteria document, Section 1.8.
- System testing will not be considered successful if outstanding Blocker or Critical defects pending resolution remain, as defined in the agreed upon test plan.

1.7.5 Performance/Load Testing

Performance/Load Testing will be performed by DPS in coordination with the Vendor in instances where internal metrics (network load, etc.) cannot be captured by the Vendor. DPS will help coordinate internal resources to provide oversight and assistance when necessary.

- The Vendor must provide documented Test Cases to DPS that will be performed during Vendor performance and load testing to validate the successful performance of the Software package.
- The Vendor must capture the average data throughput for the System and the maximum number of concurrent users before service degradation to ensure user traffic does not have an adverse effect on the DPS network and will provide these results to DPS.
- The Vendor must be responsible for conducting performance and load testing that will demonstrate the Vendor’s System is capable of meeting metrics as defined by DPS.
- The Vendor must provide performance and load test results to DPS for review and approval.
- Based on the outcome of successful performance and load testing, the Vendor will advance to the next step of System integration testing. Successful performance testing will be defined in the Performance/Load Test Plan documentation created by DPS. The Vendor must perform all these tests in a production-like environment.
- Performance/Load testing will not be considered successful if outstanding Blocker or Critical defects pending resolution remain as defined in the agreed upon test plan.

1.7.6 System Integration Testing

DPS will perform System integration testing independently or jointly with the Vendor following successful completion and documentation of Vendor and DPS System testing.

- The Vendor must provide assistance during the System integration testing process by providing technical and QA resources that will answer questions and will clarify or fix any issues encountered during the System integration testing cycle. This support can be performed remotely or in person at the DPS facility. Remote support will consist of remote server control mechanisms, WebEx review sessions, telephone conference calls and email exchanges. System integration testing will focus on the integration and interaction with other DPS systems, external systems, or third party components and will be based on DPS requirements as well as the Vendor’s System Design Specification.
- The Vendor must provide a User Acceptance Testing environment (STG) upon successful completion of System Integration Testing.

- DPS will log all defects found during the System integration testing in the agreed upon defect tracking application.
- The Vendor must investigate any defects and participate in defect triage meetings with DPS to determine defect outcome and resolution.
- The Vendor must provide a documented response to the documented defect in the agreed upon defect tracking application.
- The Vendor must provide defect fixes in the timeframe as defined in the SLA.
- The Vendor must provide release notes containing an open issues log for each test iteration.
- At DPS's sole discretion, Test Cases may be modified or added to ensure completeness, accuracy and quality of the delivered Software package as defined in business and technical documentation.
- Based on the successful outcome of System integration testing, DPS will advance to User Acceptance Testing (UAT). Successful System integration testing will be defined in the Quality Assurance Test Plan as well as in the Entry and Exit Criteria document, Section 1.8
- System Integration testing will not be considered successful if outstanding Blocker or Critical defects pending resolution remain as defined in the agreed upon test plan.

1.7.7 User Acceptance Testing (UAT)

- Following successful completion of the System integration testing, or System test for Vendor-Hosted Systems, DPS will coordinate and execute UAT in the Vendor's (STG) environment.
- UAT will be performed by DPS end users based on UAT Test Cases created by DPS.
- Based on level of configuration or customization, DPS may require Vendor to be onsite for UAT.
- DPS will notify the Vendor of any defects found during UAT of the Software System.
- The Vendor must investigate any defects and participate in defect triage meetings with DPS to determine defect outcome and resolution.
- The Vendor must provide defect fixes in the timeframe as defined in the SLA or Service Level Standards.
- If the number of defect failures prevents all systems from operating as described above, DPS may reject the entire final Software package.
- If all criteria is not met as defined in the User Acceptance test plan documentation created by DPS, or the Vendor's System does not meet the defined business requirements, DPS may reject the final Software System.

1.7.8 Final Acceptance

The software solution will undergo a stabilization and acceptance period. This stabilization period will not start until the solution is in production. Stabilization period will consist of 30 days of production operations after the final delivery of the Solution to the production environment.

Stabilization will be deemed completed if, at the conclusion of the 30 day period, there are:

1. Zero Blocker outstanding defects;
2. Zero Critical outstanding defects; and
3. No more than 10 Major outstanding defects.

Blocker, Critical, and Major severities are identified during the testing cycle of the Solution with inputs from the business, IT, and Vendor teams.

Final acceptance will be documented in writing, on the Final Acceptance Form and will be executed by DPS and the Vendor.

1.7.9 Failure Resolution

Upon failure of any test within the control of the Vendor, the Vendor must submit report describing the nature of the failure and the actions to be taken to remedy the situation prior to any modification or replacement of the System, within ten business days. DPS will provide written approval or denial within five business days. If a System requires modification, the fault will be corrected and the test repeated until successfully completed.

- Major discrepancies that will substantially delay receipt and acceptance of the System will be sufficient cause for rejection of the System. Failure to satisfy the requirements of any test is considered a defect and the System will be subject to rejection by DPS. Any rejected Software package may be offered again for retest provided all noncompliance has been corrected.
- Resolution of System integration test failure. If the Software package fails the System integration test, Vendor will correct the fault and then DPS will repeat the Systems integration test until successfully completed.
- Resolution of final acceptance test failure. If a defect within the System is detected during the final acceptance test, DPS will document the failure. Vendor will be required to research, document and correct the source of failure. Once corrective measures are taken, DPS will monitor the point of failure until a consecutive 30 calendar day period free of defects is achieved.

1.7.10 Retest

Vendor and DPS will mutually agree to re-test per the Testing Requirements, Implementation, and Acceptance section, as determined by the environment where the issue is to be addressed. If the system downtime exceeds 72 hours or the System does not meet the stability and acceptance criteria defined above, DPS may extend the test period by an amount of time equal to the greater of the downtime in excess of 72 hours or the number of days required to complete the performance requirement of an individual point of failure.

1.8 QA ENTRY AND EXIT CRITERIA

1.8.1 Purpose

Identify and clarify Entrance/Exit Criteria for all initiatives, projects or applications that use the controlled testing environment(s) and processes, commonly referred to as TST, SQA or PRD. The Quality Assurance Team maintains this document and should be referenced in all documents related to software changes that need to be released. This document provides general guidance for requirements, wherein builds, code documents or artifacts are introduced into those environments and processes regarding entry/exit into/from the testing environment(s). This document does not attempt to cover those projects for which the QA Team is serving in an oversight and advisory role.

1.8.2 Scope

Maintain controlled environments and processes to enhance the organization's ability to implement code or applications into the DPS testing and performance environments, and, as result, reducing production defects, trouble tickets or downtime in production.

1.9 GENERAL ENVIRONMENT ENTRY/EXIT CRITERIA AND PROCESS

1.9.1 General Environment Requirements

- Project, Development and Test Leads will engage with Release Manager (RM) for Environment resource. RM should be engaged as early as possible to provide environment review and analysis for all environments.
- Project Lead/Manager, Development Lead and Test Lead must provide documentation sufficient for the RM to complete a testing environment analysis. This information is required to sufficiently gather and identify project resources and requirements for all applications (modified and new), to validate existence of required testing environments.
- RM will assess current environment(s) and identify environment deficiencies, providing feedback to Project Lead/Manager, Development Lead and Test Lead to identify presence or absence of environment(s) and hardware.

- Documentation must include: Deployment steps with roll back strategy (as applicable), version number, be held in source control and be approved by the RM.

1.9.2 Development Environment Entrance/Exit Process/Criteria

- General Environment Requirements (above) have been met.
- Build artifacts must be provided, in advance, to the RM for review, prior to scheduled deployment to Development Environment.
- Depending upon project size and intent (as defined and agreed upon by the Project Team), the items required for entrance, and acceptance, into the Development environment would include the following.
    - Unit, Component and Integration test results
    - Design Document
    - Release Notes, including open issues
- Criteria to exit from Development Environment to QA will be governed by the QA Test Plan and should contain the following.
    - Unit, Component and Integration test results
    - Design Document
    - Defect Report(s)
    - Release Notes

1.9.3 QA Environment Entrance/Exit Process/Criteria

- General Environment Requirements (above) have been met.
- QA Test Plan(s) and test scenarios are reviewed and have approval by project team.
    - The intended functionality of all code changes per business requirements has been documented in test scenarios and these test scenarios have been reviewed and agreed upon within the Test Plan.
- All standard software components, including testing tools, must have been successfully installed and functioning properly.
- Criteria to exit from QA Environment to UAT Environment will be governed by the QA Test Plan, but should contain the following (at a minimum).
    - Test Summary Report (TSR)
    - Test Results
    - Defect Report(s)

1.9.4 UAT Environment Entrance/Exit Process/Criteria

- General Environment Requirements (above) have been met.

- UA Test Plan(s) and test scenarios are reviewed and signed off.
  - The intended functionality of all code changes per business requirements has been documented in test scenarios and these test scenarios have been reviewed and agreed upon within the Test Plan.
- All standard software components, including testing tools, must have been successfully installed and functioning properly.
- Criteria to exit from QA Environment to UAT will be governed by the QA and UA Test Plan, but should contain the following (at a minimum).
  - Test Summary Report (TSR)
  - Test Results
  - Defect Report(s)

1.9.5 PRD Environment Entrance Process/Criteria

- General Environment Requirements (above) have been met.
- Project Lead/Manager, Development Lead and Test Lead must provide documentation sufficient within a Change Request (CR) for the Change Control Coordinator (CCC) to complete a CR analysis. This information is required to sufficiently gather and identify project resources and requirements for all applications (modified and new), to validate existence of required testing environment.
- Project Lead/Manager will schedule official Change Control Board (CCB) meeting when all build and release artifacts are ready for promotion into PRD.
- Build artifacts will be provided in advance for review by the CCC prior to the CCB meeting.
- QA and UA Test Plan(s) have received management approval and test execution complete. Documents have been submitted to the CR.
- Depending upon project size and intent (as defined and agreed upon by the Project Team), the items required for entrance and acceptance into the PRD environment would include the following.
  - Test Summary Report (TSR)
  - Test Plan(s)
  - Test Results
  - Defect Report(s)
  - Release Notes

DPS Cyber Security Contract Requirements

OGC approved 9/1/2021

DPS Cyber Security Contract Requirements

Table of Contents

DPS Cyber Security Contract Requirements

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

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

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).