For the purposes of this form, Vendor means Respondent, Bidder, Applicant, or Contractor as those terms apply throughout the relevant solicitation and contracting process Vendor is participating in or to whom a final contract or purchase order has been awarded. Response means any interested response from the Vendor to DPS for purposes of applying to a solicitation, such as a Proposal, Bid, or Application.

1. Vendor Information

A. Demographics

Company's Legal Name	
Company's DBA if applicable	
Mailing Address	
Physical Address	
DUNS No.	
(Texas) Payee Identification Number	
Federal Taxpayer Identification Number	
Secretary of State Charter No.	
Texas Franchise Tax File No.	
Email for Receipt of Purchase Orders	
Remittance Address if Direct Deposit is Declined	

B. Authorized Representatives and Vendor's Personnel

Complete all fields for each name as requested on this form. All information is necessary.

i. **Vendor's Authorized Representative**

First Name	

Middle Initial/Name	
Last Name	
Title	
Email	
Phone	

ii. Contact for Response Clarifications, Inquiries, and Negotiations

First Name	
Middle Initial/Name	
Last Name	
Title	
Email	
Phone	

iii. Contract/Project Manager

First Name	
Middle Initial/Name	
Last Name	
Title	
Email	
Phone	

C. Historically Underutilized Business (HUB) Representation

Vendor represents and certifies as part of its response that it ☐is or ☐ is not, a VetHUB certified by the Comptroller of Public Accounts' Statewide Procurement Division.

D. Preferences

Check the preferences for which you qualify.

- ☐ Goods produced or offered by a Texas bidder that is owned by a Texas resident service- disabled veteran
- ☐ Goods produced in Texas or offered by a Texas bidder that is not owned by a Texas resident service-disabled veteran
- ☐ Agricultural products grown in Texas
- ☐ Agricultural products offered by a Texas bidder
- ☐ Services offered by a Texas bidder that is owned by a Texas resident service-disabled veteran
- ☐ Services offered by a Texas bidder that is not owned by a Texas resident service disabled veteran
- ☐ Texas vegetation native to the region
- ☐ USA-produced supplies, materials, or equipment
- ☐ Products of persons with mental or physical disabilities
- ☐ Products made of recycled, remanufactured, or environmentally sensitive materials including recycled steel
- ☐ Energy efficient products
- ☐ Rubberized asphalt paving material
- ☐ Recycled motor oil and lubricants
- ☐ Products produced at facilities located on formerly contaminated property
- ☐ Products and services from economically depressed or blighted areas
- ☐ Vendors that meet or exceed air quality standards
- ☐ Recycled or reused computer equipment of other manufacturers
- ☐ Foods of higher nutritional value
- ☐ Commercial production company or advertising agency located in Texas

2. Required Submissions

A. **Child support certification.** Under Texas Family Code §231.006(d) (relating to delinquent child support), Respondent acknowledges that it is not ineligible to receive the specified grant, loan, or payment and acknowledges that this Contract will be terminated and payment will be withheld if this certification is found to be inaccurate. Under Tex. Fam. Code § 231.006(c), responses must include names and Social Security Numbers of each person with at least 25% ownership of the business entity submitting the Response. If any person meets the 25% ownership criteria, failure to provide the required information will result in disqualification of the solicitation. Vendors meeting the criteria must complete the following.

Name	Social Security Number

B. **Certification for former executives.** Under Tex. Gov't Code § 669.003, DPS may not enter into a contract with a person who employs a current or former Executive head of a state agency until four years have passed since that person was the executive head of the state agency. By signing the below acknowledgment, Vendor certifies that it is in compliance with Tex. Gov't Code § 669.003. If Tex. Gov't Code § 669.003 applies, Vendor must complete the following.

Name of Former Executive	
Name of State Agency	
Date of Separation from State Agency	
Date of Employment with Vendor	

C. **Certification for protection of Texas residents and state government**. Under Executive Order GA-48, issued by the Governor of Texas, November 19, 2024, every vendor that submits a bid, proposal, or response with respect to a contract for goods or services to DPS must make the following certification. Vendor certifies that it, and if applicable, any of its holding companies
or subsidiaries, is not:

a. Listed in Section 889 of the 2019 National Defense Authorization Act (NDAA); or
b. Listed in Section 1260H of the 2021 NDAA; or
c. Owned by the government of a country on the U.S. Department of Commerce's foreign adversaries list under 15 C.F.R. § 791.4; or
d. Controlled by any governing or regulatory body located in a country on the U.S. Department of Commerce's foreign adversaries list under 15 C.F.R. § 791.4.

D. Type of Business Organization

Vendor, by checking the applicable box, represents that it operates in Texas as:

☐ A corporation incorporated under the laws of Texas
☐ An individual
☐ A partnership
☐ A non-profit organization
☐ A joint venture; or

If Vendor is a foreign entity, it operates as:

☐ An individual;
☐ A partnership;
☐ A non-profit organization;
☐ A joint venture; or
☐ A corporation, registered for business in _____.

E. Lawsuits (check the applicable paragraph that applies)

i. ☐ Vendor represents and warrants that it is not aware of and has no notice of any court or governmental agency actions, proceedings, or investigations, etc., pending or threatened against Vendor or any related individuals or affiliated entities related to the subject matter of this solicitation or otherwise relevant to DPS's consideration of the response. Vendor represents and warrants that it is not aware of any court or governmental agency actions, proceedings, or investigations, etc. against Vendor or any of these individuals or entities within the five years immediately preceding the submission of the Response to this solicitation. In addition, Vendor represents and warrants that it will notify DPS in writing within five business days of any changes to the representations or warranties in Subsection i and understands that failure to so timely update DPS will constitute breach of contract and may result in immediate termination of the awarded contract.

ii. ☐ Vendor is unable to make the representation and warranty in Subsection i above and instead represents and warranties that it has included as a detailed attachment within its response, which expressly references this Subsection ii, a complete disclosure of any such court or governmental agency actions, proceedings or investigations, etc., and specifically addresses whether any of such past, pending, or threatened actions, proceedings or investigations, etc., would or could (1) impair Vendor's performance under the awarded contract; (2) relate to the solicited or similar goods or services or the awarded contract; or (3) be otherwise relevant to

DPS's consideration of the response. In addition, Vendor represents and warrants that it will notify DPS within five business days of any changes to the representations and warranties in this Subsection ii or attachments in response to Subsection ii and understands that failure to so timely update DPS will constitute breach of contract and may result in immediate termination of the awarded contract.

F. Ethics and Conflict of Interest

Under Tex. Gov't Code § 572.051, any individual who interacts with public purchasers in any capacity is required to adhere to the established guidelines. Tex. Gov't Code § 572.051 outlines the ethical standards required of state officers and employees who interact with public purchasers in the conduct of state business.

Specifically, a DPS employee may not have an interest in, or in any manner be connected with a contract or offer for a purchase of goods or services by an agency of the state; or in any manner, including by rebate or gift, accept or receive from a person to whom a contract may be awarded, directly or indirectly, anything of value or a promise, obligation or contract for future reward or compensation. Entities who are interested in seeking business opportunities with the state must be mindful of these restrictions when interacting with public purchasers of DPS or purchasers of other state agencies. Vendor must also comply with the Conflict of Interest provisions and disclosure requirements as listed in the Texas Procurement and Contract Management Guide.

Vendor represents that it has disclosed to DPS all existing or potential conflicts of interest relative to performance of the Contract or that performance will not constitute an actual or potential conflict of interest or reasonably create an appearance of impropriety.

Vendor must disclose any actual or potential conflict of interest below.

3. Vendor Acknowledgments, Certifications, Assurances, Warranties, and Affirmations

Vendor acknowledges it can meet all requirements as stated and also acknowledges the receipt, review, and acceptance of the Solicitation. Any exceptions to the specifications or statement of work (SOW), terms, requirements, or conditions must be explicitly permitted to be excepted in the solicitation and Vendor must explicitly identify them within Vendor's response in the required format.

Failure to sign and submit this form with the response may disqualify Vendor.

By signing the solicitation and submitting a response to DPS, Vendor certifies its compliance and understanding with the following statements.

By signature and submission, Vendor represents and warrants that the individual signing the documents made part of the submitted Response is authorized to sign such documents on behalf of Vendor and to bind Vendor under any contract which may be awarded from the submission of its response.

By signature and submission, Vendor represents and warrants that all statements and information prepared and submitted in response to this solicitation are true, current, complete, and accurate.

If the circumstances certified by Vendor change or additional information is obtained subsequent to submission of the response, Vendor agrees that it is under a continuing duty to supplement its response under this provision. Vendor must submit updated information as soon as reasonably possible upon learning of any change to its affirmation.

A. Acknowledges that all of its representations and warranties contained in any part of its response and the awarded contract are material and have been relied upon by DPS in selecting Vendor for contract award. Vendor warrants and represents that all of its statements and representations made to DPS prior to contract award, and those made during the negotiation of the contract are material, true and correct. Vendor certifies that it will promptly notify DPS if any representations, certifications, or warranties provided in the awarded contract are no longer true and correct.

B. Certifies it will include without limitation all disclosures, affirmations, guarantees, certifications, statements, and warranties of Vendor in submitting its response to this Solicitation and will become certifications of the Contractor if Vendor is selected for contract award.

C. If a Texas address is shown as the address of Vendor, Vendor qualifies as a Texas Resident Bidder as defined in Tex. Gov't Code § 2155.444(c).

D. Acknowledges its obligation to specifically identify information it contends to be confidential or proprietary, and where Vendor designates substantial portions of or the entire response as confidential or proprietary, the response is subject to being determined to be non-responsive to the Solicitation.

E. Grants a royalty-free, non-revocable limited perpetual license to reproduce any copyrighted portions of the response and subsequent documents to comply with Legislative Budget Board reporting requirements, Texas Public Information Act disclosures, or any other reporting requirements mandated by law or statute. Vendor's response and subsequent documents are subject to the Texas Public Information Act.

F. Certifies that it is exempt or not delinquent in the payment of any franchise taxes owed the State of Texas under Tex. Tax Code Chapter 171.

G. Certifies it is not in default, nor is there any event in existence which, with notice or the passage of time or both, would constitute a default by Vendor under any indenture, mortgage, deed of trust, lease, loan agreement, license, security agreement, contract, governmental license or permit or other agreement or instrument to which it is a party or by which any of its properties are bound and which default would materially and adversely affect Vendor's ability to perform its obligations.

H. Vendor affirms that no person will, on the grounds of race, color, religion, sex, national origin, age, disability, political affiliation, or religious belief, be excluded from the participation in, be denied the benefits of, be subjected to discrimination under, or be denied employment in the administration of, or in connection with, any program or activity funded in whole or in part with funds available under any awarded contract. Vendor must comply with Executive Order 11246, "Equal Employment Opportunity," as amended by Executive Order 11375, "Amending Executive Order 11246 relating to Equal Employment Opportunity," and as supplemented by regulations at 41 C.F.R. Part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity Department of Labor."

I. Certifies that Vendor and its principals are eligible to participate in this transaction and have not been subjected to suspension, debarment, or similar ineligibility determined by any federal, state, or local governmental entity and Vendor is in compliance with the State of Texas statutes and rules relating to procurement and that Vendor is not listed on the federal government's terrorism watch list as described in Executive Order 13224 or debarred on the *Texas Debarred Vendor List*. Entities ineligible for federal procurement are listed at http://www.sam.gov.

J. Affirms compliance with all applicable standards, orders, or regulations issued pursuant to the mandates of the Clean Air Act (42 U.S.C. § 7401 et seq.) and the Federal Water Pollution Control Act, as amended, (33 U.S.C. § 1251 et seq.).

K. Complies with the provisions of the Lobbying Disclosure Act, 2 U.S.C. § 1601 et seq. By submitting a response, Vendor certifies that it will not and has not used federally appropriated funds to pay any person or organization for influencing or attempting to influence any officer or employee of any federal agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any federal contract, grant, or any other award covered by 31 U.S.C. § 1352. It also certifies that Vendor will disclose any lobbying with non-federal funds that takes place in connection with obtaining any federal award by completing and submitting Standard Form LLL.

L. Certifies that it has not given and does not intend to give at any time, any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor, payment, inducement, or service to a public servant or DPS officer, employee, or agent in connection with this transaction. Violation of this requirement may result in the termination of the contract at the discretion of DPS.

M. Under Tex. Gov't Code § 2155.004, Vendor certifies that the individual or business entity named in its response is not ineligible to receive the Contract and acknowledges that the contract may be terminated and payment withheld if this certification is inaccurate. Tex. Gov't Code § 2155.004 prohibits a person or entity from receiving a state contract if that person or entity received compensation for participating in preparing the solicitation or specifications for the Contract.

N. Under Tex. Gov't Code § 2155.006 and 2261.053, Vendor certifies that the individual or business entity named in its response is not ineligible to receive the contract and acknowledges that the contract may be terminated and payment withheld if this certification is inaccurate.

O. Represents and warrants that it has not been the subject of allegations of Deceptive Trade Practices violations under Tex. Bus. & Com. Code Chapter 17 or allegations of any unfair business practice in any administrative hearing or court suit and that Vendor has not been found to be liable for such practices in such proceedings. Vendor certifies that it has no officers who have served as officers of other entities who have been the subject of allegations of Deceptive Trade Practices violations or allegations of any unfair business practices in an administrative hearing or court suit, and that such officers have not been found to be liable for such practices in such proceedings.

P. Represents and warrants that Vendor and Vendor's employees have not been convicted of a felony criminal offense, or that, if such a conviction has occurred, Vendor has fully advised DPS as to the facts and circumstances surrounding the conviction.

Q. Certifies its compliance with Tex. Health & Safety Code Ch. 361, Subchapter Y and Texas Commission on Environmental Quality rules in 30 Tex. Admin. Code Ch. 328, if Vendor is submitting a response for the purchase or lease of computer equipment.

R. Certifies its compliance with Tex. Health & Safety Code Ch. 361 related to the Television Equipment Recycling Program, if Vendor is submitting a response for the purchase or lease of covered television equipment.

S. Certifies, in accordance with Tex. Gov't Code § 2254.033, relating to consulting services, that it does not employ an individual who has been employed by DPS or another agency at any time during the two years preceding the submission of the response, or in the alternative, Vendor has disclosed in its response the following: (1) the nature of the previous employment with DPS or the other agency; (2) the date the employment was terminated; and (3) the annual rate of compensation for the employment at the time of its termination.

T. Represents, if solicitation and Contract is for a professional or consulting service under Tex. Gov't Code Ch. 2254, that none of its employees, including those authorized to provide services under the Contract, were former employees of DPS during the 12 months immediately preceding Contract execution.

U. Certifies, under Tex. Gov't Code § 2155.0061 that it is not ineligible to receive the specified contract and acknowledges that this contract may be terminated and payment withheld if this certification is inaccurate.

V. Certifies that it will comply with Tex. Gov't Code § 2063.104, which requires cybersecurity training. Any Contractor who has access to a state computer system or database must complete a cybersecurity training program certified by DIR and selected by DPS during the initial term of the contract and during any optional renewal period. Contractor must verify completion of the program by sending proof of training to the Contract Monitor upon request.

W. Acknowledges that Tex. Gov't Code Chapter 552, Subchapter J may apply to this solicitation or contract and agrees that DPS may terminate the contract if Contractor or Vendor knowingly or intentionally fails to comply with a requirement of that subchapter.

X. If defined as a company under Tex. Gov't Code § 2270.0152, certifies that it is not (1) engaged in business with Iran, Sudan, or a foreign terrorist organization as prohibited by Tex. Gov't Code § 2252.152, or (2) identified on a list prepared and maintained by the comptroller under Tex. Gov't Code §§ 2270.052, 2270.0102, or 2270.0152.

Y. If defined as an applicable company, certifies that it will comply with Tex. Gov't Code §2271.001 and it does not boycott Israel and will not boycott Israel during the term of any contract resulting from this solicitation. If Vendor cannot make that certification or is not required to do so by law, Vendor must indicate that in its Response and state why the certification is not required.

Z. Certifies, under Tex. Gov't Code § 572.069, that it has not employed and will not employ a former DPS employee or state officer who participated in a procurement or contract

negotiation for DPS involving Vendor before the second anniversary of the date the contract is signed or the procurement is terminated or withdrawn. This certification only applies to former state officers or employees whose state service or employment ceased on or after September 1, 2015.

AA. Certifies that it is not ineligible to receive the Contract under Tex. Health & Safety Code § 161.0085.

BB. Certifies that it, its parent company, any affiliate, or affiliate of its parent are not (1) majority owned or controlled by citizens or governmental entities of China, Iran, North Korea, Russia, or any other country designated by the Governor under Tex. Gov't Code § 2275.0102, or (2) headquartered in any of those countries.

CC. If required to do so under Tex. Gov't Code § 2276.002, verifies that it does not boycott energy companies and will not boycott energy companies during the term of the Contract. If Vendor cannot make that verification, Vendor must indicate that it in its response and state why the verification is not required.

DD. If required to do so under Tex. Gov't Code § 2274.002, verifies that it (1) does not have a practice, policy, guidance, or directive that discriminates against a firearm entity or firearm trade association, and (2) will not discriminate during the Contract term against a firearm entity or firearm trade association. If Vendor cannot make that verification, Vendor must indicate that it in its response and state why the verification is not required.

EE. Vendor certifies that all subcontractors used in performance of this contract are held accountable for all security and contractual requirements, including compliance with all obligations of the Sub-Contracting Plan (SP), including submission and amendments to the SP and Progress Assessment Reports (PARs).

FF. Vendor certifies that it, and if applicable, any of its holding companies or subsidiaries, is not (1) listed in § 889 of the 2019 National Defense Authorization Act (NDAA), or (2) listed in § 1260H of the 2021 NDAA, or (3) owned by the government of a country on the U.S. Department of Commerce's foreign adversaries list under 15 C.F.R. § 791.4, or (4) controlled by any governing or regulatory body located in a country on the U.S. Department of Commerce's foreign adversaries list under 15 C.F.R. § 791.4.

Change Order Request Form

1. Overview

This Change Order Request Form (CORF) defines the detailed requirements of certain incorporated services and enhancements already within the scope of the originally awarded Contract. This CORF will be incorporated by reference into an Amendment or Purchase Order Change Notice (POCN). DPS will not accept any work or pay Contractor for that work without a signed Amendment or an issued POCN.

DPS Project Manager (DPS PM), Contract Monitor, and Contractor will estimate the work effort for this request by completing the fillable sections with information specific to the particular work the Contractor will perform. Contractor may not change this form in any way from what was incorporated into the original Contract. Contractor may only enter data in the fillable fields in Section 2.

2. Scope

DPS requires Contractor to provide the services detailed in this section. Contractor must identify services related to achieving the agreed-upon deliverables. This CORF will address the processes, sub-tasks, itemized costs, and duration for completion of each deliverable, and the pricing will set the associated cost. Tables 1, 2, 3, and 4 are provided as the tools to clearly itemize all identified deliverables.

Services are not complete until all testing is successfully completed and DPS gives final acceptance as defined in the Contact. During the testing and acceptance period, Contractor must capture and document performance issues identified by Contractor or reported by DPS and resolve all hardware, software, and programming defects. Contractor may not bill DPS for time and materials used to resolve defects.

Describe the itemized services and specific business and functional requirements required. This information must match with all tables in this section.

Table 1—Project Points of Contact and Responsibilities				
Organization	**Title and Responsibility**	**Name**	**Phone Number**	**Email Address**
DPS	Project Sponsor			
DPS	Project Manager			
DPS	Technical SME; Hardware			
DPS	Technical SME; Software			

DPS	Technical SME; Data transmission			
DPS	Contract Administrator			
DPS	Contract Monitor			
Organization	**Title and Responsibility**	**Name**	**Phone Number**	**Email Address**
Contractor	Relationship Representative			
Contractor	Project Manager			
Contractor	Programmer			
Contractor	DBA			
Contractor	Technical SME; Hardware			
Contractor	Technical SME; Software			

Table 2—Project Specific Roles and Responsibilities		
Roles and Responsibilities	**Contractor**	**DPS**
Project requirement and dependency #1		
Project requirement and dependency #2		
***primary (P)**		

Table 3—Project Schedule			
No.	**Deliverable Description**	**Due Date**	**Comments**

Table 4—Pricing				
Deliverable Description	**Service Category and Description (e.g., Programmer) and Employee Name**	**Quantity of Hours**	**Hourly Rate in Contract**	**Cost Extension**

3. Risk and Issue Management

If there is no DPS PM associated with this Change Order Request, then the Contract Monitor will be responsible for the DPS PM tasks listed within this section. The following general procedure will be used to manage an active Change Order's issues and risks.

3.1. DPS PM will identify and document project issues (current problems) and risks (potential events that impact the project).

3.2. DPS PM will assess, analyze, and prioritize the impact and determine the highest priority risks and issues that will be managed actively, according to priority, by Contractor.

3.3. Contractor must plan and schedule high-priority risks and issues assigning responsibility for risk management and issue resolution in a documented risks and issues log, as determined by DPS.

3.4. Contractor must track and report the status of risks and issues, and communicate risk mitigation plans and issue resolutions in a documented risks and issues log.

3.5. DPS PM will monitor and control the effectiveness of the risk and issue management actions.

3.6. Active issues and risks will be monitored and reassessed on a weekly basis by DPS PM and Contractor. Mutually agreed upon escalation and risk management processes will be defined at the outset of initiating the CORF.

4. Required Reporting and Communication

Contractor must do the following.

4.1. Create and maintain a documented risks and issues log.

4.2. Provide DPS PM with a weekly written progress report for each in-process Change Order. Reports will be submitted by close of business the following Monday of each week throughout the life of an active Change Order. Contractor may submit the progress report by email.

4.3. Provide one monthly status report; and, if requested by DPS, prepare and lead one status meeting per week of no more than one hour in duration.

4.4. Attend any DPS-required or requested meetings, or submit any DPS-requested documentation.

5. Pricing and Scope

Contractor's scope, pricing, service categories, and employee types must match the Mandatory Pricing Schedule incorporated into the Contract. If Contractor did not specify the specific employees in the Contract, Contractor

must identify the specific employee names in Table 4 of those employees providing the work associated with this specific CORF.

CHANGE ORDER COMPLETION ACCEPTANCE DOCUMENT

TEXAS DEPARTMENT OF PUBLIC SAFETY

Section 1. General Information

Contract # _____

Change Order Name_____ Change Order # _____

Section 2. **Contracto**r Acknowledgement of **Change** Order Completion

The following project deliverables, as required by Section C Scope of Work and as assigned by Subsection Change Order Plan, have been completed.

CO Ref. #	Completed Deliverable Description

This is to acknowledge that _____has completed this Change Order project for the Texas Department of Public Safety.

Contractor Approver Name	Title	Signature	Date

Section 3. TXDPS Acceptance of **Change** Order Completion

This document certifies that the above-referenced services from Change Order Plan #_____ have hereby been tested and accepted by the Texas Department of Public Safety.

TXDPS Approver Name	Title	Signature	Date

FINAL ACCEPTANCE DOCUMENT

TEXAS DEPARTMENT OF PUBLIC SAFETY

DPS IT - Implementation Services Contract

This document certifies that the following services _____ have hereby been tested and accepted by the Department.

Upon execution of this acceptance document, an invoice in the amount of $_____ shall be submitted to the Department.

Final Acceptance was completed on _____.

Approver Name	Title	Signature	Date

DPS INFORMATION TECHNOLOGY (IT) STANDARDS AND REQUIREMENTS

Table of Contents

1.1 DEFINITIONS 4
1.2 INFORMATION TECHNOLOGY (IT) STANDARDS AND REQUIREMENTS 6
1.2.1 Vendor-Hosted System or DPS-Provided Cloud-Hosted System 6
1.2.2 DPS-Hosted System 8
1.2.3 Intersystem Communication Standards 10
1.2.4 Network Topography 10
1.2.5 Workstation Software Installation Packaging 10
1.3 MAINTENANCE AND SUPPORT 10
1.3.1 Software Updates 11
1.3.2 Hardware Maintenance 11
1.3.3 Change Control Participation 12
1.3.4 Service Outage Escalation and Communication Plan 12
1.3.5 Application Outages, Release Rollbacks and Degradation in Performance Reporting 12
1.4 BASIC SERVICE LEVEL STANDARDS 13
1.4.1 System Production Control 14
1.4.2 Vendor Customer and System Support 14
1.5 SYSTEM PERFORMANCE 15
1.5.1 Basic Requirements 15
1.5.2 Calculation of System Performance Rate 16
1.5.3 Response Time 16
1.5.4 Data Backups 16
1.5.5 Recovery Points 17
1.5.6 Hardware and Software Refresh Plans 18
1.5.7 Vendor Business Continuity and Disaster Recovery Plan 18
1.6 SYSTEM TRAINING PLAN FOR TECHNICAL STAFF 20
1.7 TESTING REQUIREMENTS, IMPLEMENTATION AND ACCEPTANCE 21
1.7.1 Implementation and Acceptance 21
1.7.2 Cloud-Hosted Infrastructure Environment 21
1.7.3 Unit Testing 22
1.7.4 System Testing 23
1.7.5 Performance/Load Testing 23

1.7.6 System Integration Testing 24
1.7.7 User Acceptance Testing (UAT) 25
1.7.8 Final Acceptance 25
1.7.9 Failure Resolution 26
1.7.10 Retest 26
1.8 QA ENTRY AND EXIT CRITERIA 26
1.8.1 Purpose 26
1.8.2 Scope 27
1.9 GENERAL ENVIRONMENT ENTRY/EXIT CRITERIA AND PROCESS 27
1.9.1 General Environment Requirements 27
1.9.2 Development Environment Entrance/Exit Process/Criteria 27
1.9.3 QA Environment Entrance/Exit Process/Criteria 28
1.9.4 UAT Environment Entrance/Exit Process/Criteria 28
1.9.5 PRD Environment Entrance Process/Criteria 28

1.1 DEFINITIONS

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

B. **Change Control Board (CCB)** means the DPS work group responsible for coordinating any requested change to existing DPS systems.

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

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

E. **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.

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

G. **ETL** means Extract, Transform, Load and is a process that extracts, transforms, and loads data from multiple sources to a data warehouse or other unified data repository.

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

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

K. **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.

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

M. **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.

N. **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.

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

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

Q. **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.

R. **Service Level Standards** means the Performance Standards that govern work under the contract which are agreed upon by both parties during implementation that defines timeliness or quality of products or service.

S. **Severity Level** means defining the level of impact to the organization
T. **Software (SW)** means any application programs for the exclusive use with the System.
U. **Software Development 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.
V. **Software Refresh Plan** means the implementation of software that has either been deprecated, updated or replaced.
W. **Solicitation** means Pricing Requests (PR), Request for Proposals (RFP), Request for Offers (RFO), Invitation for Bids, or Requests for Qualifications (RFQ).
X. **Solution** means a collection of information management techniques involving computer automation (Software/Hardware/database/network) to support and improve the quality and efficiency of business operations.
Y. **System** means a collection of information management techniques involving computer automation (Software/Hardware/database/network) to support and improve the quality and efficiency of business operations.
Z. **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.
AA. **UAT** means User Acceptance Testing.
BB. **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.
CC. **Vendor-Hosted** means a combination of traditional IT functions to be provided by the Vendor such as infrastructure, applications, Software as a Service, (including COTS Software), Infrastructure as a Service, Platform as a Service, security, monitoring, storage, and provider of Hardware and Hardware Maintenance.

1.2 INFORMATION TECHNOLOGY (IT) STANDARDS AND REQUIREMENTS

The Vendor must comply with the following IT standards and requirements, as applicable to this Contract, including this IT Standards and Requirements Exhibit. 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 this IT Standards and Requirements Exhibit, must be submitted with the Vendor's Response.

If the DPS Cyber Security Contract Requirements Exhibit is also incorporated by reference or included as an exhibit in the Solicitation and the resulting Contract, the Vendor must also comply with those cyber security requirements.

1.2.1 Vendor-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 systems, 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 must be identified.

C. Desktop, Laptop, or Mobile Device Documentation

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

- DPS-issued desktop or laptop PCs
    - Win10 Enterprise OS: 19042 (20h2)
    - Next version Win10 - 19044 (21h2)
    - 14393 (LTSB 2016) - THP incar systems
    - 17763 (LTSC 2019) - THP incar systems imaged after 5/2022
    - Win11 Enterprise OS: Future deployment
    - 22000 (21h2)
    - Browsers:
        - EDGE – 102.0.1245.41
        - Firefox – 91.10.0 esr
        - Chrome- 102.0.5005.63
- Current Enterprise Operating Version of Google Chrome
- Current Enterprise Operating Version of Microsoft Edge
- Current Enterprise Operating version of Firefox
- Splunk
- CrowdStrike
- Sophos
- Bitlocker
- DPS-issued Mobile Devices
- IOS Smart tablet (latest available for purchase)
- IOS Smart phone (latest available for purchase)

- Current Microsoft Enterprise Operating Version
- Current Enterprise Operating version of Mac OS X
- Current Enterprise operating version of Safari
- Current Enterprise Operating version of Firefox
- Current Enterprise Operating version of Google Chrome
- PCs (desktop or laptop), mobile devices, phones, and tablets [used by DPS customers or the general public for DPS information or services]
- 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 (or 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 (or 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
    - 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.

A. 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.
B. 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.
C. 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.
D. Maintenance services to resolve usability problems to include bugs, security issues, installation of Software updates, and major Software releases.
E. 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.

A. 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.
B. 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. 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. DPS reserves the right to delay or reschedule maintenance at its discretion to prevent maintenance from occurring during peak hours.

B. 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.

C. 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.

D. 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

The vendor must inform the contract monitor or the delegated designee of all planned production updates prior to their implementation to ensure that the potential impact is assessed, and will be subject to the DPS Change Management process. This includes the initial deployment and all subsequent updates to the production system.

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 and how the Vendor will notify DPS. Upon contract award, DPS and the Vendor will finalize a Service Outage and Escalation Communication Plan.

1.3.5 System Performance Reporting

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

B. 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.

C. 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.

D. 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.

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

Event Name: [Type event name here]
Event Date: [Type event 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 Change Request: [Type the purpose of the CR here from the actual CR ticket] **Event Description:** [Type the event description here – include high-level details to adequately inform the audience of the change and expected resolution]
Event details: [Type a highly-detailed description of what happened during the event]
Event Impact: [Describe the timeline of the event and the user impact]
Future Prevention Steps: [Detail the steps for preventing this event in the future – numbered bullets are preferred if specifically ordered steps are required]

1.4 BASIC SERVICE LEVEL STANDARDS

These Basic Service Level Standards define the requirements, responsibilities, and obligations of DPS and the Vendor to ensure the Vendor provides DPS with the optimal level of System performance.

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

Please see the following chart for DPS's Severity Level Definitions for the contract:

Severity Level	Description
1. Outage	Mission Critical System Down
2. Critical	Mission Critical System Degraded with Moderate customer impact
3. Urgent	End User Impact initiated
4. Important	Potential for performance impact if not addressed
5. Monitor	Issue addressed but could be impactful in the future
6. Informational	Inquiry for information

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 schedule will likely be oriented around periods when the System is expected to have the lightest use.

1.4.2 Vendor Customer and System Support

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

The Vendor must provide a toll-free telephone number or email accessibility to DPS for the System, 24 hours per day/7 days per week. The Vendor must provide the DPS Contract Monitor a means to report trouble outside of normal business hours.

A. Vendor System support for DPS includes responsibilities such as the following.

- 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.
- Acting as primary support provider of the identified services and ensuring any subcontractors perform any assigned duties
- Informing DPS regarding scheduled and unscheduled service outages due to maintenance, troubleshooting, disruptions or as otherwise necessary that aligns with DPS current change management policy
- Transition responsibilities

B. Vendor System support for DPS excludes responsibilities such as the following.

- Record content
- Record quality
- Assisting in correcting data through an agreed-upon process (such as ETL, providing data updates via code)
- Assisting in modifying the system to reduce the number of data-entry errors (such as using a drop-down selection instead of using a free-form box)
- 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 99% (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.

A. First Remedy: Written warning.
B. Continuing Remedy: DPS may begin exercising Contract breach 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. Vendor must report that information to DPS no later than the third Business Day of the following month. IT leadership will determine if any changes are necessary. 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). Downtime is the total number of hours (rounded to the quarter hour) during which the System is not in operation. Uptime is the actual amount of time the system is available minus downtime. System Performance Rate is equal to uptime.

For example, take the month of January:

Available hours in January: 744 hours (31 days X 24 hours);

Downtime: 1.86 hours per week, or 7.44 downtime hours for the month

Calculation:

744 available hours – 7.44 downtime hours = 736.56 uptime hours; and

736.56 uptime hours ÷ 744 available hours = 99% uptime.

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 (?) Service Levels, Recovery Points, and Target Response

Purpose

The purpose of the Service Level Standards is to specify the requirements of the Vendor's services as regarding the following.

- Requirements for product or service that will be provisioned to DPS
- Agreed service targets
- Criteria for target fulfilment evaluation
- Roles and responsibilities of Vendor
- Duration, Scope and Renewal of service level expectations
- Supporting processes, limitations, exclusions and deviations.

Recovery Points and Times

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 the SLAs noted below.
- Any exceptions to the SLA 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 DPS 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.

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's Business Continuity and Disaster Recovery Plan

The Business Continuity and Disaster Recovery Plan is 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.

Vendor must provide a disaster recovery capability for their disaster recovery planning and recovery efforts in their response to the solicitation by the agency. Vendor must provide the following to DPS within 30 days of contract execution and upon update to an existing plan:

- Business continuity and disaster recovery plans (BC/DRP), a DRP is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency, 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;

- Requirements for business continuity and disaster recovery plans include the following:
    (a) Defined purpose and scope, aligned with relevant dependencies;
    (b) Accessible to and understood by those who will use them;
    (c) Owned by a named person who is responsible for their review, update, and approval;
    (d) Defined lines of communication, roles, and responsibilities;
    (e) Detailed recovery procedures, manual work-around, and reference information;
    (f) Method for plan notification and coordination with DPS; and
    (g) Detailed process by which DPS may declare a disaster recovery necessary for the system and recovery documentation to include DPS user acceptance testing be completed during disaster recovery.
- 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 (such as, ITIL v4, COBIT 5, CSA CCM, NIST);
- Protection measures must be put into place to react to natural and human caused threats;
- 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 (such as 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 Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO); and
    (e) Related artifacts for the methodology, test, training, and exercises (TT&E) used to validate BC/DR plans.
    (f) Provision of disaster recovery, testing or exercise results to DPS, within 30 days of the incident, with an Improvement Plan to include timelines to resolve any issues identified.

TT&E results and Improvement Plan 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 including:

- Vendor's help desk or customer support
- Maintenance services
- Support services (such as, Software or Hardware)
- Hosting services
- 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 Initial Term and Optional Renewal 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 (such as 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 (such as 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 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 government-specific cloud service must be built using the available CJIS templates as a basis.
- All cloud service application deployments that are targeted for the cloud service provider's Public Cloud must be built using the available NIST 800-53, rev. 5 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 unit 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, videoconference 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 DPS 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 Improvement Plan is implemented, 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
    - Release Notes, including open issues

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 the following must be included (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.

  A – Approvals from all relevant parties at DPS
  C – Cyber scans (when required)
  T – Test results
    - Test Summary Report (TSR)
    - Test Plans
    - Test Results
    - Defect Reports
    - Release Notes

  I – Implementation, validation, rollback plans
  O – Operation support manual information (when required)
  N – Notification to users (when the change has downtime or user impact)

DPS Cyber Security Contract Exhibit

OGC APPROVED – 9/11/25

1. Cloud Security Requirements and Certifications

Req ID	Requirement	Response
1.1	Do you (by yourself or through your subcontractor) meet the TX-RAMP requirements for the solution provided in the response at the appropriate level as required by the solicitation and DPS Cyber Security?	☐ Yes ☐ No ☐ N/A (No Cloud Components/On Prem)
If no, please provide the date in which you will obtain the required TX-RAMP Certification. Click or tap here to enter text.		
1.2	Please select the TX-RAMP level obtained for the solution provided in the response. Provide the certification number and expiration date below.	☐ Provisional ☐ TX-RAMP Level 1 ☐ TX-RAMP Level 2
TX-RAMP Certification Number and Expiration Date. If Provisional, please provide the timeframe in which a full TX-RAMP certification will be obtained: Click or tap here to enter text.		
1.3	Do you (by yourself or through your subcontractor) meet the FedRAMP requirements for the solution provided in the response at the appropriate level as required by the solicitation and DPS CJIS Security Office?	☐ Yes ☐ No ☐ N/A (Does Not Interface with CJI Data)
If no, please provide the date in which you will obtain the required FedRAMP Certification. Click or tap here to enter text.		
1.4	Please select the FedRAMP level obtained by the Vendor for the solution provided in the response. Provide the Package ID and most recent annual assessment date below.	☐ FedRAMP Low ☐ FedRAMP Moderate ☐ FedRAMP High
FedRAMP Package ID and Most Recent Annual Assessment Date: Click or tap here to enter text.		
1.5	Are there any additional Cloud Security Certifications that have been obtained for the solution provided in the response (STAR, StateRAMP, etc.)? If so, please provide details below.	☐ Yes ☐ No
If yes, please provide cloud certification details. Click or tap here to enter text.		

2. Identification and Authentication Requirements

Req ID	Requirement	Response
2.1	Is Active Directory based authentication or SAML2 Identity Provider/Service Provider authentication provided?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
2.2	Are user accounts established and administered using a role-based scheme and are those role assignments tracked and monitored?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
2.3	Are users uniquely identified and prevented from establishing multiple concurrent active sessions?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
2.4	Is two-factor authentication required for all user accounts?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
2.5	Is System user functionality separated from administrator functionality, and are users required to establish sessions with administrative privileges to view and access administrator functionality?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		

2.6	Do systems prevent further access by initiating a session lock or termination after a maximum of 30 minutes of inactivity and does the session lock or termination remain in effect until the user reestablishes access using appropriate identification and authentication procedures?	☐ Yes ☐ No

If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement.
Click or tap here to enter text.

2.7	Does the system require reauthentication of the user at least once per 12 hours during an extended usage session?	☐ Yes ☐ No

If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement.
Click or tap here to enter text.

2.8	Does the system enforce a rate-limit of no more than three consecutive invalid access attempts by a user? After three consecutive invalid attempts, does the system automatically lock the account/node for a ten-minute time period unless released by DPS's Administrator?	☐ Yes ☐ No

If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement.
Click or tap here to enter text.

2.9	Does the system adhere to **all** of the following password attributes when creating and authenticating a user's unique ID. If no, please list which attributes are **not** met in the comment box below. a) Passwords must be a minimum of 15 characters up to at least 64 characters maximum and may contain, but are not required to contain any of the following elements: uppercase characters, lowercase characters, numeric characters, special characters (such as $, ^, #, @); b) When passwords are created, passwords must be checked against the following before allowing a password to be used: i. Passwords found in compromised credential databases ii. Previously used passwords iii. Commonly used passwords and passphrases iv. DPS business terms v. Geographical locations; c) Passwords must be continuously monitored to check for evidence of password compromise or breach. Upon discovery, an immediate password change must be forced upon the user; d) Do not force passwords to expire at pre-defined intervals (45, 60, or 90 days); e) Not be transmitted in clear text outside the Secure Location; f) Not be displayed in clear text when entered; g) Passwords must be salted and hashed when stored, and never be stored in plain text, electronically or physically; h) Allow users "paste" functionality when entering password to allow for the use of password managers.	☐ Yes ☐ No

If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement.

Click or tap here to enter text.

3. Audit and Accountability

Req ID	Requirement	Response
3.1	Are audit logs provided that capture **all** of the following system events? If no, please list which system events are **not** met in the comment box below. a) Account creation, modification, disabling, and termination actions b) Successful and unsuccessful System log-on attempts c) Successful and unsuccessful attempts to access, create, write, delete, or change permission on a user account, file, directory, or other System resource d) Successful and unsuccessful attempts to change account passwords e) Successful and unsuccessful actions by privileged accounts f) Successful and unsuccessful attempts for users to access, modify, or destroy the audit log	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
3.2	Is **all** of the following information provided with each audited event? If **no**, please indicate which information is **not** provided in the comment box below. a) Date and time of the event; b) The component of the System (e.g., software component, hardware component) where the event occurred; c) IP address; d) Type of event; e) User/subject identity; and f) Outcome (success or failure) of the event.	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		

3.3	Are audit logs retained for a period of at least one year?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
3.4	Do audit record time stamps use internal system clocks?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
3.5	Are audit records and audit tools protected from unauthorized access, modification, and deletion?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
3.6	Will real-time alerts be provided to appropriate DPS personnel in the event of any inappropriate or unusual activity as defined by DPS, or audit processing failure? Are alert recipients and delivery methods configurable and manageable by DPS System Administrators?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
3.7	Does the solution protect against an individual falsely denying having performed a particular action (non-repudiation)?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		

3.8	Does the system display an approved use notification message or banner before granting access to the System? The notification must contain an approved DPS logo and state: a) Users are accessing a DPS system; b) System usage will be monitored, recorded, and subject to audit; c) Unauthorized use of the system is prohibited and subject to criminal and civil penalties; d) A description of the authorized use of the system; and e) Use of the system indicates consent to monitoring and recording.	☐ Yes ☐ No

If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement.
Click or tap here to enter text.

4. System Security

Req ID	Requirement	Response
4.1	Is DPS-approved virus protection software implemented and configured at all system entry and exit points with the following attributes? a) The virus protection software must not be disabled or bypassed. b) The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software. c) The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
4.2	Are security testing and flaw remediation implemented during system development to ensure software and firmware security defects are corrected before installation in the production environment?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
4.3	Are information inputs validated and controls implemented to prevent the injection of malicious input?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		

4.4	Does the system generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
4.5	Are controls in place to safeguard the system's memory from unauthorized code execution?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
4.6	Is communication at the external boundary of the system controlled and monitored to prevent unauthorized connections and protect against or limit the effects of denial-of-service attacks?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
4.7	Does the system prevent unauthorized and unintended information transfer via shared system resources, such as registers, main memory, and hard disks?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
4.8	Are separate execution domains maintained for each executing system process, so that one process cannot modify the executing code of another process?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		

4.9	Is a continuous security program established and maintained as part of the Services? Will the security program be reviewed and adjusted when a risk is assessed or discovered by the vendor, selected third party, or by DPS? Does the security program enable DPS (or its selected third party) to: a) Define the scope and boundaries, policies, and organizational structure of an information security management system; b) Conduct periodic risk assessments to identify threats and vulnerabilities specific to DPS; c) Receive an unredacted copy of a recent vulnerability scan (no older than 30 days); d) Implement appropriate mitigating controls; e) Implement training programs; f) Manage resources; g) Monitor and test the security program to ensure its effectiveness?	☐ Yes ☐ No

If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement.
Click or tap here to enter text.

5. Maintenance

Req ID	Requirement	Response
5.1	Prior to use, will any maintenance tools used for diagnostic or repair actions be submitted for approval by DPS?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
5.2	Are nonlocal (remote) maintenance sessions uniquely authenticated, all maintenance and diagnostic activities logged, and sessions and network connections terminated when maintenance is complete?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
5.3	Prior to the removal of the information system or system components from the secure hosting location for off-site maintenance or repairs, will written approval be obtained from DPS?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
5.4	Is all equipment sanitized to remove all information from associated media prior to removal from the secure hosting location for off-site maintenance or repairs?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
5.5	Are security controls checked to verify that the controls are still functioning properly following maintenance or repair actions?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		

5.5	Will upgrades, patches, and other maintenance be scheduled with DPS?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
5.6	Will you ensure that all maintenance personnel who maintain the system are authorized by DPS prior to performing maintenance?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		

6. System/Solution Assurance

Req ID	Requirement	Response
6.1	Are security updates applied 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	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
6.2	Will the System/Solution be kept up to date with all supporting software updates, security updates, and patches?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
6.3	Are systems that are no longer supported by the manufacturer replaced or upgraded within three months from the official manufacturer end of support date.	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
6.4	Will the System Security Documentation (SSD) be periodically reviewed and updated upon request from DPS?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
6.5	Will DPS's System Security Documentation be protected from unauthorized access, disclosure, or release in accordance with the Subsection entitled "General Confidentiality Requirements?"	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		

6.6	Will documentation be provided, at the request of DPS, for the System that describes user and administrator guidance regarding the implementation and operation of security controls?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
6.7	Prior to system acceptance, will all security requirements be met and implemented with any exceptions formally approved by DPS?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		

7. Physical and Environmental Protection

Req ID	Requirement	Response
7.1	Is physical access to the System containing DPS's data restricted to authorized personnel with appropriate clearances and access authorizations?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
7.2	Are physical access authorizations enforced for all physical access points, and are all individual access authorizations verified before granting access to the facility where the system resides?	☐ Yes ☐ No
If no, please an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
7.3	Is entry to the facility containing the System controlled using physical access devices or guards?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
7.4	When access devices are lost, combinations are compromised, or individuals are transferred or terminated are combinations and access devices changed?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		

7.5	Are appropriate environmental controls maintained in the facility containing the System? Appropriate 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.	☐ Yes ☐ No
If no, please list which environmental controls are not maintained along with an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
7.6	Will you 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?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
7.7	If requested, will you provide a quarterly report to DPS's CISO of the security incidents that Vendor has identified and taken measures to resolve?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
7.8	If answering **Yes** to the previous question (**7.7**): Will the vendor also provide updates to those security incidents?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		

8. Data Security

Req ID	Requirement	Response
8.1	Is DPS data marked, handled, and stored in compliance with the data classification and retention policy as defined by DPS?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
8.2	Does this System, vendor or any subcontractors require access to DPS's network; DPS's data; or the network processing, transporting, or storing of DPS's data?	☐ Yes ☐ No
If **yes**, please provide an explanation as to what network and data access is required. Click or tap here to enter text.		
8.3	If answering **Yes** to the previous question (**8.2**):	
	Has a CJIS Security Addendum been completed and signed by the vendor?	☐ Yes ☐ No ☐ N/A
	Have all employees requiring access to DPS's network or data signed the FBI Certification to the CJIS Security Addendum and passed a fingerprint-based background check?	☐ Yes ☐ No ☐ N/A
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
8.4	Will the Vendor, its subcontractors, and its staff with access to DPS's data complete and provide proof of DIR certified security awareness training annually for the term of the contract including renewals? This training is mandatory.	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		

8.5	Is all DPS data and metadata maintained within the conterminous United States of America?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
8.6	Is data prevented from being exported to a location external to the hosting environment unless prior written permission from DPS is obtained?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
8.7	Does the solution protect the confidentiality of DPS's information by encrypting all data transmitted outside or stored outside the secure network?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
8.8	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. **Please indicate which FIPS standards are used.**	☐ FIPS 140-2 ☐ FIPS 140-3 ☐ N/A
If cryptographic operations are not FIPS 140-2 or 140-3 compliant, please provide an explanation, and plans to reach compliance with the requirement.		
8.8	When TLS is used, it must be at least version 1.2 **Please indicate which version of TLS is used.**	☐ TLS 1.2 ☐ TLS 1.3 ☐ N/A
If the version of TLS used is below 1.2, please provide an explanation, and plans to reach compliance with the requirement.		

8.9	Does the solution produce, control, and distribute cryptographic keys using NIST-approved key management technology and processes? The key management process is subject to audit by DPS.	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
8.10	Does all equipment provided to DPS by the 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.) 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?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		

9. Wireless Network Security

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.

Req ID	Requirement	Response
9.1	Are personal firewall services in use for all WLAN enabled PEDs?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
9.2	Are antivirus services in use for all WLAN enabled PEDs?	☐ Yes ☐ No
If no, please an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
9.3	Is data-in-transit via WLAN enabled PEDs protected by a minimum 128 bit end-to-end encryption that meets FIPS 140-2 or 140-3?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
9.4	Is FIPS 140-2 or 140-3 compliant data-at-rest encryption enabled on WLAN enabled PEDs in a manner that requires the PED be powered on with credentials successfully authenticated in order for the data to be deciphered?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
9.5	Are wireless access points installed in a protected environment to prevent tampering or theft?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		

9.6	Are wireless network connections periodically checked or validated to prevent against rogue access points?	☐ Yes ☐ No

If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement.

Click or tap here to enter text.

10. Mobile Device Management

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. Mobile devices that transmit, receive, process, or store sensitive or confidential information must have MDM implemented. The MDM solution must include the core features outlined in this section.

Req ID	Requirement	Response
10.1	Does the MDM solution implement the ability to push security policies to managed devices and ensure the authenticity and integrity of the transaction?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
10.2	Does the MDM solution implement the ability to query the device for its configuration information and ensure the authenticity and integrity of the transaction?	☐ Yes ☐ No
If no, please an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
10.3	Does the MDM solution implement the ability to modify device configuration and ensure the authenticity and integrity of the transaction?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
10.4	Does the MDM solution implement asset management (track/enable/disable) for the mobile devices being managed via the MDM server?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		

10.5	Does the MDM solution manage proxy access to network resources via the connection of the mobile device to the MDM server?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
10.6	Does the MDM solution query managed devices on the status of their security policy compliance and implement a specified mediation function based on compliance status?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
10.7	Does the MDM solution generate audit record reports from mobile device audit records?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
10.8	Does the MDM solution maintain the ability to remotely wipe a device in the event it is lost or stolen?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
10.9	Does the MDM solution receive alerts and other notifications from managed mobile devices?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
10.10	Does the MDM solution download and store mobile device audit records?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		

10.11.1	Does the MDM provide application management, including the ability create an allow list, for applications installed on managed mobile devices?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		
10.11.2	Does the MDM solution ensure the authenticity and integrity of the transaction in the three MDM categories mentioned in 10.11.1?	☐ Yes ☐ No
If no, please provide an explanation, any compensating controls, and plans to reach compliance with the requirement. Click or tap here to enter text.		

11. 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, including DPS General Manual Chapter 25 (Cyber Security) and Chapter 26 (Information Resource Policy). 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.

12. 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. DPS will process all waiver requests 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, Vendor must complete the sanitization and destruction of the data and provide to DPS all sanitization documentation.

13. 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 Vendor;
   2) Vendor discovered, learned, or created independently by Vendor 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 Vendor 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 affected parties in writing of any unauthorized release of confidential information:
   1) DPS must be notified immediately (but no later than four hours) when Vendor knows or should have known of such unauthorized release;
   2) Other affected parties must be notified within two business days of when Vendor knows or should have known of such unauthorized release.

c. Vendor must maintain all confidential information in confidence during the term of the Contract and after the expiration or termination of the Contract.

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

e. Vendor acknowledges that DPS's non-public and confidential information is unique and valuable, and that DPS may have no adequate remedy at law if Vendor 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 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 Vendor if Vendor fails to perform any of its confidentiality obligations under the Contract.

f. Vendor must immediately return to DPS all non-public and 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.

g. 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.

h. 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.

14. 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.

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 in Tex. Bus. & Com. Code Sec. 521.053.

c. Vendor must notify DPS and affected parties of any breach of system security immediately (but no later than four hours) 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. Vendor must otherwise comply with all notification requirements in Tex. Bus. & Com. Code Sec. 521.053.

d. 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 may assess and enforce 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 imposed by Vendor that contradict 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.

e. DPS may assess liquidated damages under 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.

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

g. DPS will not hold Vendor responsible or assess liquidated damages due to a breach of system security that DPS determines was 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).

h. 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.

15. 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 four 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 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.

16. Cyber Insurance Requirement

If required by the Contract to get Cyber insurance, 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 must 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.

b. DPS may confer with other state resources such as SORM or 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.

17. Representations and Warranties Related to Software

If any software, that is COTS and not a Work for Hire, 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 does 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

Software provided under the Contract does 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).

Agency Identification

Agency Name	ORI
Agency Address	
City	Zip
Agency Representative (Title and Name)	
Phone Number	Fax Number
Email address	

Contractor Identification

Company Name	Service Providing Agency	
Company Address		
City	State	Zip
Contractor Representative (Title and Name)		
Phone Number	Fax Number	
Email address		

Visit our website www.dps.texas.gov/securityreview for information on submitting vendor/contractor fingerprints.

Email can be sent to: security.committee@dps.texas.gov

Main office number is: (512) 424-5686

Parties may use the following Security Addendum with the Texas Signatory Page or, in their contract, choose to incorporate the Security Addendum by reference. If the Addendum is incorporated by reference into the contract, a copy of the contract must be provided to the TX DPS CJIS Security Office.

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

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM
CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____ _____
Signature of Contractor Employee Date

_____
Printed or Typed Contractor Employee Name

Sex: ____ Race: _____ DOB: _____ State/ID or DL: _____

_____ _____
Signature of Contractor Representative Date

_____
Printed or Typed Name of Contractor Representative

_____
Organization Name and Representative's Title

Texas Signatory Page

The undersigned parties agree that the *Security Addendum* is now a part of the contract between the entities. The parties agree to abide by all requirements of the *Security Addendum* and the *CJIS Security Policy*, and it shall remain in force for the term of the contract. Any violation of this addendum constitutes a breach of the contract.

To the extent there is a conflict between a confidentiality clause in the underlying contract and the *Security Addendum* and/or the *CJIS Security Policy*, the *Security Addendum* and the *CJIS Security Policy* shall govern any information covered by the *Security Addendum* and/or the *CJIS Security Policy*.

(To be signed and dated by the vendor and law enforcement agency representative(s) who signed the original contract, or at least who have authority to bind each entity.)

Printed Name of Agency Representative

Signature of Agency Representative | Title

Agency Name and ORI | Date

Printed Name of Vendor (Contractor) Representative

Signature of Vendor (Contractor) Representative | Title

Vendor Organization Name | Date

Comptroller of Public Accounts FORM 74-176 (Rev.9-21/21) FMX

STATE OF TEXAS

For Comptroller's Use Only

Direct Deposit Authorization

This form may be used by vendors, individual recipients or state employees to receive payments from the state of Texas by direct deposit or to change/cancel existing direct deposit information.

Transaction Types

SECTION 1

1. Select transaction types:

- ☐ New setup *(Sections 2, 3, 5 and 6)*
- ☐ Change financial institution *(Sections 2, 3, 4, 5 and 6)*
- ☐ Change account number *(Sections 2, 3, 4, 5 and 6)*
- ☐ Change account type *(Sections 2, 3, 4, 5 and 6)*
- ☐ Cancellation *(Sections 2 and 6 - Sections 7 and 8 for state agency use)*
- ☐ Change custodial agency ____

Payee Identification

SECTION 2

2. Payee type
- ☐ State employee
- ☐ Vendor or other recipient

3. Identification number
- ☐ Texas Identification Number (TIN)
- ☐ Employer Identification Number (EIN)
- ☐ Social Security number (SSN)*
- ☐ Individual Taxpayer Identification Number (ITIN)

4. Mail code *(If not known, leave blank.)*

5. Payee name

6. Phone *(Area code and number)* ( ) ext.

7. Mailing address *(Street, city, state and ZIP code)*

New Account Information (Setups and Changes) *(Completion by financial institution is recommended)*

SECTION 3

8. Financial institution name

9. City

10. State

11. Routing number *(9 digits)* ____ – ____ – ____

12. Customer account number *(maximum 17 characters)*

13. Account type ☐ Checking ☐ Savings

14. Financial representative name *(optional)*

15. Title *(optional)*

16. Financial representative signature *(optional)*

17. Phone *(Area code and number) (optional)* ( ) ext.

18. Date *(optional)*

Existing Account Information (Changes Only)

SEC 4

19. Routing number *(9 digits)* ____ – ____ – ____

20. Customer account number *(maximum 17 characters)*

21. Account type ☐ Checking ☐ Savings

International Payments Verification *(required)*

SEC 5

22. Will these payments be forwarded to a financial institution outside the United States? ☐ YES ☐ NO

If "YES," also complete the ACH (Direct Deposit) Payment Destination Confirmation (Form 74-227).

Authorization for Setup, Changes or Cancellation *(required)*

SECTION 6

I authorize the state agency that issues my state of Texas payments via the Texas Comptroller of Public Accounts to electronically deposit my payments to my financial institution. I understand that any payments deposited in error to my account will be reversed by the agency that issues my state of Texas payments via the Texas Comptroller of Public Accounts.

I further understand that the agency that issues my state of Texas payments and the Texas Comptroller of Public Accounts will comply at all times with the National Automated Clearing House Association's rules. *(For further information on these rules, please contact your financial institution.)*

sign here 23. Authorized signature

24. Printed name

25. Date

Cancellation by Agency *(for state agency use)*

SEC 7

26. Reason

27. Date

State Agency Contact *(for state agency use)*

SECTION 8

sign here 28. Authorized signature

29. Date

30. Phone *(Area code and number)* ( ) ext.

31. Agency number

32. Agency name

33. Comments

✔

34. ***Please return to the paying agency at the following address:***

** See Federal Privacy Act Statement on page 2.*

Instructions for Direct Deposit Authorization

You have certain rights *under Chapters 552 and 559, Government Code, to review, request and correct information we have on file about you. To request information for review or to request error correction, use the contact information on this form.*

Section 1: Transaction Type(s)

1. Select the appropriate **transaction type(s)** and complete the corresponding sections.

Note: *Requests to change custodial agency number are processed based on Payment Services research and guidelines.*

Section 2: Payee Identification *(Required)*

2. Payee type: Indicate whether the payee is a ***state employee*** or a ***vendor/recipient***.

Note: *Agencies must complete box 34 with the appropriate agency's return address for the selected payee type.*

3. Identification number: Indicate the type of identification number and provide the associated 9- or 11-digit number.
4. Mail code: Enter the 3-digit mail code.
5. Payee name: Enter the payee's name.
6. Phone: Enter the payee's area code, phone number (and extension, if applicable).
7. Mailing address: Enter the payee's mailing address, city, state and ZIP code.

Section 3: New Account Information (Setups and changes) *(Completion by financial institution is recommended)*

8. Financial institution name: Enter the name of the payee's financial institution.
9. City: Enter the city of the payee's financial institution.
10. State: Enter the 2-character abbreviation for state of the payee's financial institution.
11. Routing number: Enter the 9-digit routing number of the payee's financial institution.
12. Customer account number: Enter the payee's account number (maximum 17 characters).
13. Type of account: Indicate whether the payee's account type is a checking account or a savings account.
14. Financial representative name: *(optional)* Enter the name of the financial representative.
15. Title: *(optional)* Enter the title of the financial institution representative.
16. Financial representative signature: *(optional)* Original signature of the financial representative.
17. Phone: *(optional)* Enter the area code, phone number (and extension, if applicable) of the financial representative.
18. Date: *(optional)* Enter the date the financial representative signed the form.

Section 4: Existing Account Information (Changes only)

19. Routing number: Enter the 9-digit ***routing number*** currently on file with the Comptroller's office.
20. Customer account number: Enter the payee's ***account number*** currently on file with the Comptroller's office.
21. Account type: Select the payee's ***account type*** currently on file with the Comptroller's office.

Section 5: International Payments Verification *(Required)*

22. Payment Destination: Select ***YES*** or ***NO*** to indicate if state payments will be forwarded to a financial institution outside the U.S.

Note: *If* ***YES****, the payee must also complete the ACH (Direct Deposit) Payment Destination Confirmation (Form 74-227).*

Section 6: Authorization for Setup, Changes or Cancellation *(Required)*

23. Authorized signature: Original signature of the payee is required.
24. Printed name: Enter or print the name of the payee or vendor/recipient signing the form.
25. Date: Enter or print the date the form was signed.

Section 7: Cancellation by Agency *(for state agency use)*

26. Reason: Enter the reason for cancellation of the payee's direct deposit information.
27. Date: Enter the date the cancellation was determined.

Section 8: State Agency Contact *(for state agency use)*

28. Authorized signature: Original signature of the agency's authorized representative is required.
29. Date: Enter the date the agency's representative signed the form.
30. Phone: Enter the area code, phone number and extension (if applicable) of the agency's representative.
31. Agency number: Enter the 3-digit agency number.
32. Agency name: Enter the agency's name.
33. Comments: *(optional)* Enter comments, if needed.
34. Return to Paying State Agency: This area autopopulates with the name and address of the paying state agency to which this form will be returned.

Questions?

State Employees:	Contact your agency's Human Resource department or payroll staff.
Vendors/Recipients:	Contact the paying agency's accounts payable staff.
State Agencies:	Contact Fiscal Management, Payment Services at 512-936-8138.

***Federal Privacy Act Statement:** Disclosure of your Social Security number is required and authorized under law for the purpose of tax administration and identification of any individual affected by applicable law, 42 U.S.C. § 405(c)(2)(C)(i) and Tex. Gov't Code §§ 403.011, 403.015, 403.055, 403.056 and 403.078. The Public Information Act, Tex. Gov't Code Ch. 522, and applicable federal law shall govern release of information on this form in response to a public information request.*

Form **W-9**
(Rev. March 2024)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

Go to *www.irs.gov/FormW9* for instructions and the latest information.

Give form to the requester. Do not send to the IRS.

Before you begin. For guidance related to the purpose of Form W-9, see *Purpose of Form*, below.

Print or type. See ***Specific Instructions*** on page 3.

1 Name of entity/individual. An entry is required. (For a sole proprietor or disregarded entity, enter the owner's name on line 1, and enter the business/disregarded entity's name on line 2.)

2 Business name/disregarded entity name, if different from above.

3a Check the appropriate box for federal tax classification of the entity/individual whose name is entered on line 1. Check only **one** of the following seven boxes.

☐ Individual/sole proprietor ☐ C corporation ☐ S corporation ☐ Partnership ☐ Trust/estate

☐ LLC. Enter the tax classification (C = C corporation, S = S corporation, P = Partnership) . . . . .

Note: Check the "LLC" box above and, in the entry space, enter the appropriate code (C, S, or P) for the tax classification of the LLC, unless it is a disregarded entity. A disregarded entity should instead check the appropriate box for the tax classification of its owner.

☐ Other (see instructions)

3b If on line 3a you checked "Partnership" or "Trust/estate," or checked "LLC" and entered "P" as its tax classification, and you are providing this form to a partnership, trust, or estate in which you have an ownership interest, check this box if you have any foreign partners, owners, or beneficiaries. See instructions . . . . . ☐

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any)

Exemption from Foreign Account Tax Compliance Act (FATCA) reporting code (if any)

(Applies to accounts maintained outside the United States.)

5 Address (number, street, and apt. or suite no.). See instructions.

Requester's name and address (optional)

6 City, state, and ZIP code

7 List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Note: If the account is in more than one name, see the instructions for line 1. See also *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number

			–			–				

or

Employer identification number

		–							

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
3. I am a U.S. citizen or other U.S. person (defined below); and
4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and, generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here	**Signature of U.S. person**	**Date**

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to *www.irs.gov/FormW9*.

What's New

Line 3a has been modified to clarify how a disregarded entity completes this line. An LLC that is a disregarded entity should check the appropriate box for the tax classification of its owner. Otherwise, it should check the "LLC" box and enter its appropriate tax classification.

New line 3b has been added to this form. A flow-through entity is required to complete this line to indicate that it has direct or indirect foreign partners, owners, or beneficiaries when it provides the Form W-9 to another flow-through entity in which it has an ownership interest. This change is intended to provide a flow-through entity with information regarding the status of its indirect foreign partners, owners, or beneficiaries, so that it can satisfy any applicable reporting requirements. For example, a partnership that has any indirect foreign partners may be required to complete Schedules K-2 and K-3. See the Partnership Instructions for Schedules K-2 and K-3 (Form 1065).

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS is giving you this form because they

must obtain your correct taxpayer identification number (TIN), which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following.

- Form 1099-INT (interest earned or paid).
- Form 1099-DIV (dividends, including those from stocks or mutual funds).
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds).
- Form 1099-NEC (nonemployee compensation).
- Form 1099-B (stock or mutual fund sales and certain other transactions by brokers).
- Form 1099-S (proceeds from real estate transactions).
- Form 1099-K (merchant card and third-party network transactions).
- Form 1098 (home mortgage interest), 1098-E (student loan interest), and 1098-T (tuition).
- Form 1099-C (canceled debt).
- Form 1099-A (acquisition or abandonment of secured property).

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

Caution: If you don't return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See *What is backup withholding*, later.

By signing the filled-out form, you:

1. Certify that the TIN you are giving is correct (or you are waiting for a number to be issued);

2. Certify that you are not subject to backup withholding; or

3. Claim exemption from backup withholding if you are a U.S. exempt payee; and

4. Certify to your non-foreign status for purposes of withholding under chapter 3 or 4 of the Code (if applicable); and

5. Certify that FATCA code(s) entered on this form (if any) indicating that you are exempt from the FATCA reporting is correct. See *What Is FATCA Reporting*, later, for further information.

Note: If you are a U.S. person and a requester gives you a form other than Form W-9 to request your TIN, you must use the requester's form if it is substantially similar to this Form W-9.

Definition of a U.S. person. For federal tax purposes, you are considered a U.S. person if you are:

- An individual who is a U.S. citizen or U.S. resident alien;
- A partnership, corporation, company, or association created or organized in the United States or under the laws of the United States;
- An estate (other than a foreign estate); or
- A domestic trust (as defined in Regulations section 301.7701-7).

Establishing U.S. status for purposes of chapter 3 and chapter 4 withholding. Payments made to foreign persons, including certain distributions, allocations of income, or transfers of sales proceeds, may be subject to withholding under chapter 3 or chapter 4 of the Code (sections 1441–1474). Under those rules, if a Form W-9 or other certification of non-foreign status has not been received, a withholding agent, transferee, or partnership (payor) generally applies presumption rules that may require the payor to withhold applicable tax from the recipient, owner, transferor, or partner (payee). See Pub. 515, Withholding of Tax on Nonresident Aliens and Foreign Entities.

The following persons must provide Form W-9 to the payor for purposes of establishing its non-foreign status.

- In the case of a disregarded entity with a U.S. owner, the U.S. owner of the disregarded entity and not the disregarded entity.
- In the case of a grantor trust with a U.S. grantor or other U.S. owner, generally, the U.S. grantor or other U.S. owner of the grantor trust and not the grantor trust.
- In the case of a U.S. trust (other than a grantor trust), the U.S. trust and not the beneficiaries of the trust.

See Pub. 515 for more information on providing a Form W-9 or a certification of non-foreign status to avoid withholding.

Foreign person. If you are a foreign person or the U.S. branch of a foreign bank that has elected to be treated as a U.S. person (under Regulations section 1.1441-1(b)(2)(iv) or other applicable section for chapter 3 or 4 purposes), do not use Form W-9. Instead, use the appropriate Form W-8 or Form 8233 (see Pub. 515). If you are a qualified foreign pension fund under Regulations section 1.897(l)-1(d), or a partnership that is wholly owned by qualified foreign pension funds, that is treated as a non-foreign person for purposes of section 1445 withholding, do not use Form W-9. Instead, use Form W-8EXP (or other certification of non-foreign status).

Nonresident alien who becomes a resident alien. Generally, only a nonresident alien individual may use the terms of a tax treaty to reduce or eliminate U.S. tax on certain types of income. However, most tax treaties contain a provision known as a saving clause. Exceptions specified in the saving clause may permit an exemption from tax to continue for certain types of income even after the payee has otherwise become a U.S. resident alien for tax purposes.

If you are a U.S. resident alien who is relying on an exception contained in the saving clause of a tax treaty to claim an exemption from U.S. tax on certain types of income, you must attach a statement to Form W-9 that specifies the following five items.

1. The treaty country. Generally, this must be the same treaty under which you claimed exemption from tax as a nonresident alien.

2. The treaty article addressing the income.

3. The article number (or location) in the tax treaty that contains the saving clause and its exceptions.

4. The type and amount of income that qualifies for the exemption from tax.

5. Sufficient facts to justify the exemption from tax under the terms of the treaty article.

Example. Article 20 of the U.S.-China income tax treaty allows an exemption from tax for scholarship income received by a Chinese student temporarily present in the United States. Under U.S. law, this student will become a resident alien for tax purposes if their stay in the United States exceeds 5 calendar years. However, paragraph 2 of the first Protocol to the U.S.-China treaty (dated April 30, 1984) allows the provisions of Article 20 to continue to apply even after the Chinese student becomes a resident alien of the United States. A Chinese student who qualifies for this exception (under paragraph 2 of the first Protocol) and is relying on this exception to claim an exemption from tax on their scholarship or fellowship income would attach to Form W-9 a statement that includes the information described above to support that exemption.

If you are a nonresident alien or a foreign entity, give the requester the appropriate completed Form W-8 or Form 8233.

Backup Withholding

What is backup withholding? Persons making certain payments to you must under certain conditions withhold and pay to the IRS 24% of such payments. This is called "backup withholding." Payments that may be subject to backup withholding include, but are not limited to, interest, tax-exempt interest, dividends, broker and barter exchange transactions, rents, royalties, nonemployee pay, payments made in settlement of payment card and third-party network transactions, and certain payments from fishing boat operators. Real estate transactions are not subject to backup withholding.

You will not be subject to backup withholding on payments you receive if you give the requester your correct TIN, make the proper certifications, and report all your taxable interest and dividends on your tax return.

Payments you receive will be subject to backup withholding if:

1. You do not furnish your TIN to the requester;

2. You do not certify your TIN when required (see the instructions for Part II for details);

3. The IRS tells the requester that you furnished an incorrect TIN;

4. The IRS tells you that you are subject to backup withholding because you did not report all your interest and dividends on your tax return (for reportable interest and dividends only); or

5. You do not certify to the requester that you are not subject to backup withholding, as described in item 4 under "*By signing the filled-out form*" above (for reportable interest and dividend accounts opened after 1983 only).

Certain payees and payments are exempt from backup withholding. See *Exempt payee code*, later, and the separate Instructions for the Requester of Form W-9 for more information.

See also *Establishing U.S. status for purposes of chapter 3 and chapter 4 withholding*, earlier.

What Is FATCA Reporting?

The Foreign Account Tax Compliance Act (FATCA) requires a participating foreign financial institution to report all U.S. account holders that are specified U.S. persons. Certain payees are exempt from FATCA reporting. See *Exemption from FATCA reporting code*, later, and the Instructions for the Requester of Form W-9 for more information.

Updating Your Information

You must provide updated information to any person to whom you claimed to be an exempt payee if you are no longer an exempt payee and anticipate receiving reportable payments in the future from this person. For example, you may need to provide updated information if you are a C corporation that elects to be an S corporation, or if you are no longer tax exempt. In addition, you must furnish a new Form W-9 if the name or TIN changes for the account, for example, if the grantor of a grantor trust dies.

Penalties

Failure to furnish TIN. If you fail to furnish your correct TIN to a requester, you are subject to a penalty of $50 for each such failure unless your failure is due to reasonable cause and not to willful neglect.

Civil penalty for false information with respect to withholding. If you make a false statement with no reasonable basis that results in no backup withholding, you are subject to a $500 penalty.

Criminal penalty for falsifying information. Willfully falsifying certifications or affirmations may subject you to criminal penalties including fines and/or imprisonment.

Misuse of TINs. If the requester discloses or uses TINs in violation of federal law, the requester may be subject to civil and criminal penalties.

Specific Instructions

Line 1

You must enter one of the following on this line; **do not** leave this line blank. The name should match the name on your tax return.

If this Form W-9 is for a joint account (other than an account maintained by a foreign financial institution (FFI)), list first, and then circle, the name of the person or entity whose number you entered in Part I of Form W-9. If you are providing Form W-9 to an FFI to document a joint account, each holder of the account that is a U.S. person must provide a Form W-9.

• **Individual.** Generally, enter the name shown on your tax return. If you have changed your last name without informing the Social Security Administration (SSA) of the name change, enter your first name, the last name as shown on your social security card, and your new last name.

Note for ITIN applicant: Enter your individual name as it was entered on your Form W-7 application, line 1a. This should also be the same as the name you entered on the Form 1040 you filed with your application.

• **Sole proprietor.** Enter your individual name as shown on your Form 1040 on line 1. Enter your business, trade, or "doing business as" (DBA) name on line 2.

• **Partnership, C corporation, S corporation, or LLC, other than a disregarded entity.** Enter the entity's name as shown on the entity's tax return on line 1 and any business, trade, or DBA name on line 2.

• **Other entities.** Enter your name as shown on required U.S. federal tax documents on line 1. This name should match the name shown on the charter or other legal document creating the entity. Enter any business, trade, or DBA name on line 2.

• **Disregarded entity.** In general, a business entity that has a single owner, including an LLC, and is not a corporation, is disregarded as an entity separate from its owner (a disregarded entity). See Regulations section 301.7701-2(c)(2). A disregarded entity should check the appropriate box for the tax classification of its owner. Enter the owner's name on line 1. The name of the owner entered on line 1 should never be a disregarded entity. The name on line 1 should be the name shown on the income tax return on which the income should be reported. For example, if a foreign LLC that is treated as a disregarded entity for U.S. federal tax purposes has a single owner that is a U.S. person, the U.S. owner's name is required to be provided on line 1. If the direct owner of the entity is also a disregarded entity, enter the first owner that is not disregarded for federal tax purposes. Enter the disregarded entity's name on line 2. If the owner of the disregarded entity is a foreign person, the owner must complete an appropriate Form W-8 instead of a Form W-9. This is the case even if the foreign person has a U.S. TIN.

Line 2

If you have a business name, trade name, DBA name, or disregarded entity name, enter it on line 2.

Line 3a

Check the appropriate box on line 3a for the U.S. federal tax classification of the person whose name is entered on line 1. Check only one box on line 3a.

IF the entity/individual on line 1 is a(n) . . .	THEN check the box for . . .
• Corporation	Corporation.
• Individual or • Sole proprietorship	Individual/sole proprietor.
• LLC classified as a partnership for U.S. federal tax purposes or • LLC that has filed Form 8832 or 2553 electing to be taxed as a corporation	Limited liability company and enter the appropriate tax classification: P = Partnership, C = C corporation, or S = S corporation.
• Partnership	Partnership.
• Trust/estate	Trust/estate.

Line 3b

Check this box if you are a partnership (including an LLC classified as a partnership for U.S. federal tax purposes), trust, or estate that has any foreign partners, owners, or beneficiaries, and you are providing this form to a partnership, trust, or estate, in which you have an ownership interest. You must check the box on line 3b if you receive a Form W-8 (or documentary evidence) from any partner, owner, or beneficiary establishing foreign status or if you receive a Form W-9 from any partner, owner, or beneficiary that has checked the box on line 3b.

Note: A partnership that provides a Form W-9 and checks box 3b may be required to complete Schedules K-2 and K-3 (Form 1065). For more information, see the Partnership Instructions for Schedules K-2 and K-3 (Form 1065).

If you are required to complete line 3b but fail to do so, you may not receive the information necessary to file a correct information return with the IRS or furnish a correct payee statement to your partners or beneficiaries. See, for example, sections 6698, 6722, and 6724 for penalties that may apply.

Line 4 Exemptions

If you are exempt from backup withholding and/or FATCA reporting, enter in the appropriate space on line 4 any code(s) that may apply to you.

Exempt payee code.

• Generally, individuals (including sole proprietors) are not exempt from backup withholding.

• Except as provided below, corporations are exempt from backup withholding for certain payments, including interest and dividends.

• Corporations are not exempt from backup withholding for payments made in settlement of payment card or third-party network transactions.

• Corporations are not exempt from backup withholding with respect to attorneys' fees or gross proceeds paid to attorneys, and corporations that provide medical or health care services are not exempt with respect to payments reportable on Form 1099-MISC.

The following codes identify payees that are exempt from backup withholding. Enter the appropriate code in the space on line 4.

1—An organization exempt from tax under section 501(a), any IRA, or a custodial account under section 403(b)(7) if the account satisfies the requirements of section 401(f)(2).

2—The United States or any of its agencies or instrumentalities.

3—A state, the District of Columbia, a U.S. commonwealth or territory, or any of their political subdivisions or instrumentalities.

4—A foreign government or any of its political subdivisions, agencies, or instrumentalities.

5—A corporation.

6—A dealer in securities or commodities required to register in the United States, the District of Columbia, or a U.S. commonwealth or territory.

7—A futures commission merchant registered with the Commodity Futures Trading Commission.

8—A real estate investment trust.

9—An entity registered at all times during the tax year under the Investment Company Act of 1940.

10—A common trust fund operated by a bank under section 584(a).

11—A financial institution as defined under section 581.

12—A middleman known in the investment community as a nominee or custodian.

13—A trust exempt from tax under section 664 or described in section 4947.

The following chart shows types of payments that may be exempt from backup withholding. The chart applies to the exempt payees listed above, 1 through 13.

IF the payment is for . . .	THEN the payment is exempt for . . .
• Interest and dividend payments	All exempt payees except for 7.
• Broker transactions	Exempt payees 1 through 4 and 6 through 11 and all C corporations. S corporations must not enter an exempt payee code because they are exempt only for sales of noncovered securities acquired prior to 2012.
• Barter exchange transactions and patronage dividends	Exempt payees 1 through 4.
• Payments over $600 required to be reported and direct sales over $5,000[1]	Generally, exempt payees 1 through 5.[2]
• Payments made in settlement of payment card or third-party network transactions	Exempt payees 1 through 4.

[1] See Form 1099-MISC, Miscellaneous Information, and its instructions.

[2] However, the following payments made to a corporation and reportable on Form 1099-MISC are not exempt from backup withholding: medical and health care payments, attorneys' fees, gross proceeds paid to an attorney reportable under section 6045(f), and payments for services paid by a federal executive agency.

Exemption from FATCA reporting code. The following codes identify payees that are exempt from reporting under FATCA. These codes apply to persons submitting this form for accounts maintained outside of the United States by certain foreign financial institutions. Therefore, if you are only submitting this form for an account you hold in the United States, you may leave this field blank. Consult with the person requesting this form if you are uncertain if the financial institution is subject to these requirements. A requester may indicate that a code is not required by providing you with a Form W-9 with "Not Applicable" (or any similar indication) entered on the line for a FATCA exemption code.

A—An organization exempt from tax under section 501(a) or any individual retirement plan as defined in section 7701(a)(37).

B—The United States or any of its agencies or instrumentalities.

C—A state, the District of Columbia, a U.S. commonwealth or territory, or any of their political subdivisions or instrumentalities.

D—A corporation the stock of which is regularly traded on one or more established securities markets, as described in Regulations section 1.1472-1(c)(1)(i).

E—A corporation that is a member of the same expanded affiliated group as a corporation described in Regulations section 1.1472-1(c)(1)(i).

F—A dealer in securities, commodities, or derivative financial instruments (including notional principal contracts, futures, forwards, and options) that is registered as such under the laws of the United States or any state.

G—A real estate investment trust.

H—A regulated investment company as defined in section 851 or an entity registered at all times during the tax year under the Investment Company Act of 1940.

I—A common trust fund as defined in section 584(a).

J—A bank as defined in section 581.

K—A broker.

L—A trust exempt from tax under section 664 or described in section 4947(a)(1).

M—A tax-exempt trust under a section 403(b) plan or section 457(g) plan.

Note: You may wish to consult with the financial institution requesting this form to determine whether the FATCA code and/or exempt payee code should be completed.

Line 5

Enter your address (number, street, and apartment or suite number). This is where the requester of this Form W-9 will mail your information returns. If this address differs from the one the requester already has on file, enter "NEW" at the top. If a new address is provided, there is still a chance the old address will be used until the payor changes your address in their records.

Line 6

Enter your city, state, and ZIP code.

Part I. Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. If you are a resident alien and you do not have, and are not eligible to get, an SSN, your TIN is your IRS ITIN. Enter it in the entry space for the Social security number. If you do not have an ITIN, see *How to get a TIN* below.

If you are a sole proprietor and you have an EIN, you may enter either your SSN or EIN.

If you are a single-member LLC that is disregarded as an entity separate from its owner, enter the owner's SSN (or EIN, if the owner has one). If the LLC is classified as a corporation or partnership, enter the entity's EIN.

Note: See *What Name and Number To Give the Requester*, later, for further clarification of name and TIN combinations.

How to get a TIN. If you do not have a TIN, apply for one immediately. To apply for an SSN, get Form SS-5, Application for a Social Security Card, from your local SSA office or get this form online at *www.SSA.gov*. You may also get this form by calling 800-772-1213. Use Form W-7, Application for IRS Individual Taxpayer Identification Number, to apply for an ITIN, or Form SS-4, Application for Employer Identification Number, to apply for an EIN. You can apply for an EIN online by accessing the IRS website at *www.irs.gov/EIN*. Go to *www.irs.gov/Forms* to view, download, or print Form W-7 and/or Form SS-4. Or, you can go to *www.irs.gov/OrderForms* to place an order and have Form W-7 and/or Form SS-4 mailed to you within 15 business days.

If you are asked to complete Form W-9 but do not have a TIN, apply for a TIN and enter "Applied For" in the space for the TIN, sign and date the form, and give it to the requester. For interest and dividend payments, and certain payments made with respect to readily tradable instruments, you will generally have 60 days to get a TIN and give it to the requester before you are subject to backup withholding on payments. The 60-day rule does not apply to other types of payments. You will be subject to backup withholding on all such payments until you provide your TIN to the requester.

Note: Entering "Applied For" means that you have already applied for a TIN or that you intend to apply for one soon. See also *Establishing U.S. status for purposes of chapter 3 and chapter 4 withholding*, earlier, for when you may instead be subject to withholding under chapter 3 or 4 of the Code.

Caution: A disregarded U.S. entity that has a foreign owner must use the appropriate Form W-8.

Part II. Certification

To establish to the withholding agent that you are a U.S. person, or resident alien, sign Form W-9. You may be requested to sign by the withholding agent even if item 1, 4, or 5 below indicates otherwise.

For a joint account, only the person whose TIN is shown in Part I should sign (when required). In the case of a disregarded entity, the person identified on line 1 must sign. Exempt payees, see *Exempt payee code*, earlier.

Signature requirements. Complete the certification as indicated in items 1 through 5 below.

1. Interest, dividend, and barter exchange accounts opened before 1984 and broker accounts considered active during 1983. You must give your correct TIN, but you do not have to sign the certification.

2. Interest, dividend, broker, and barter exchange accounts opened after 1983 and broker accounts considered inactive during 1983. You must sign the certification or backup withholding will apply. If you are subject to backup withholding and you are merely providing your correct TIN to the requester, you must cross out item 2 in the certification before signing the form.

3. Real estate transactions. You must sign the certification. You may cross out item 2 of the certification.

4. Other payments. You must give your correct TIN, but you do not have to sign the certification unless you have been notified that you have previously given an incorrect TIN. "Other payments" include payments made in the course of the requester's trade or business for rents, royalties, goods (other than bills for merchandise), medical and health care services (including payments to corporations), payments to a nonemployee for services, payments made in settlement of payment card and third-party network transactions, payments to certain fishing boat crew members and fishermen, and gross proceeds paid to attorneys (including payments to corporations).

5. Mortgage interest paid by you, acquisition or abandonment of secured property, cancellation of debt, qualified tuition program payments (under section 529), ABLE accounts (under section 529A), IRA, Coverdell ESA, Archer MSA or HSA contributions or distributions, and pension distributions. You must give your correct TIN, but you do not have to sign the certification.

What Name and Number To Give the Requester

For this type of account:	Give name and SSN of:
1. Individual	The individual
2. Two or more individuals (joint account) other than an account maintained by an FFI	The actual owner of the account or, if combined funds, the first individual on the account[1]
3. Two or more U.S. persons (joint account maintained by an FFI)	Each holder of the account
4. Custodial account of a minor (Uniform Gift to Minors Act)	The minor[2]
5. a. The usual revocable savings trust (grantor is also trustee)	The grantor-trustee[1]
b. So-called trust account that is not a legal or valid trust under state law	The actual owner[1]
6. Sole proprietorship or disregarded entity owned by an individual	The owner[3]
7. Grantor trust filing under Optional Filing Method 1 (see Regulations section 1.671-4(b)(2)(i)(A))**	The grantor*
8. Disregarded entity not owned by an individual	The owner
9. A valid trust, estate, or pension trust	Legal entity[4]
10. Corporation or LLC electing corporate status on Form 8832 or Form 2553	The corporation
11. Association, club, religious, charitable, educational, or other tax-exempt organization	The organization
12. Partnership or multi-member LLC	The partnership
13. A broker or registered nominee	The broker or nominee
14. Account with the Department of Agriculture in the name of a public entity (such as a state or local government, school district, or prison) that receives agricultural program payments	The public entity
15. Grantor trust filing Form 1041 or under the Optional Filing Method 2, requiring Form 1099 (see Regulations section 1.671-4(b)(2)(i)(B))**	The trust

[1] List first and circle the name of the person whose number you furnish. If only one person on a joint account has an SSN, that person's number must be furnished.

[2] Circle the minor's name and furnish the minor's SSN.

[3] You must show your individual name on line 1, and enter your business or DBA name, if any, on line 2. You may use either your SSN or EIN (if you have one), but the IRS encourages you to use your SSN.

[4] List first and circle the name of the trust, estate, or pension trust. (Do not furnish the TIN of the personal representative or trustee unless the legal entity itself is not designated in the account title.)

* **Note:** The grantor must also provide a Form W-9 to the trustee of the trust.

** For more information on optional filing methods for grantor trusts, see the Instructions for Form 1041.

Note: If no name is circled when more than one name is listed, the number will be considered to be that of the first name listed.

Secure Your Tax Records From Identity Theft

Identity theft occurs when someone uses your personal information, such as your name, SSN, or other identifying information, without your permission to commit fraud or other crimes. An identity thief may use your SSN to get a job or may file a tax return using your SSN to receive a refund.

To reduce your risk:

- Protect your SSN,
- Ensure your employer is protecting your SSN, and
- Be careful when choosing a tax return preparer.

If your tax records are affected by identity theft and you receive a notice from the IRS, respond right away to the name and phone number printed on the IRS notice or letter.

If your tax records are not currently affected by identity theft but you think you are at risk due to a lost or stolen purse or wallet, questionable credit card activity, or a questionable credit report, contact the IRS Identity Theft Hotline at 800-908-4490 or submit Form 14039.

For more information, see Pub. 5027, Identity Theft Information for Taxpayers.

Victims of identity theft who are experiencing economic harm or a systemic problem, or are seeking help in resolving tax problems that have not been resolved through normal channels, may be eligible for Taxpayer Advocate Service (TAS) assistance. You can reach TAS by calling the TAS toll-free case intake line at 877-777-4778 or TTY/TDD 800-829-4059.

Protect yourself from suspicious emails or phishing schemes. Phishing is the creation and use of email and websites designed to mimic legitimate business emails and websites. The most common act is sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

The IRS does not initiate contacts with taxpayers via emails. Also, the IRS does not request personal detailed information through email or ask taxpayers for the PIN numbers, passwords, or similar secret access information for their credit card, bank, or other financial accounts.

If you receive an unsolicited email claiming to be from the IRS, forward this message to *phishing@irs.gov*. You may also report misuse of the IRS name, logo, or other IRS property to the Treasury Inspector General for Tax Administration (TIGTA) at 800-366-4484. You can forward suspicious emails to the Federal Trade Commission at *spam@uce.gov* or report them at *www.ftc.gov/complaint*. You can contact the FTC at *www.ftc.gov/idtheft* or 877-IDTHEFT (877-438-4338). If you have been the victim of identity theft, see *www.IdentityTheft.gov* and Pub. 5027.

Go to *www.irs.gov/IdentityTheft* to learn more about identity theft and how to reduce your risk.

Privacy Act Notice

Section 6109 of the Internal Revenue Code requires you to provide your correct TIN to persons (including federal agencies) who are required to file information returns with the IRS to report interest, dividends, or certain other income paid to you; mortgage interest you paid; the acquisition or abandonment of secured property; the cancellation of debt; or contributions you made to an IRA, Archer MSA, or HSA. The person collecting this form uses the information on the form to file information returns with the IRS, reporting the above information. Routine uses of this information include giving it to the Department of Justice for civil and criminal litigation and to cities, states, the District of Columbia, and U.S. commonwealths and territories for use in administering their laws. The information may also be disclosed to other countries under a treaty, to federal and state agencies to enforce civil and criminal laws, or to federal law enforcement and intelligence agencies to combat terrorism. You must provide your TIN whether or not you are required to file a tax return. Under section 3406, payors must generally withhold a percentage of taxable interest, dividends, and certain other payments to a payee who does not give a TIN to the payor. Certain penalties may also apply for providing false or fraudulent information.

Vendor Exceptions Form

List and clearly explain any exceptions that you propose to DPS's Standard Terms and Conditions in the table below and in the exact format required. If not in the exact format required, Vendor will be deemed as waiving the exception and DPS will reject it.

Section Number	Language	Language that you propose in the alternative (delete by strikethrough and add by underline)	Reason for Requesting Exception to DPS's Standard Terms and Conditions

DPS Online Bid Room Vendor Information

Responses for this solicitation may be submitted electronically using the DPS Online Bid Room or any other method identified in the solicitation. Use of the DPS Online Bid Room is optional and is subject to all terms and conditions, affirmations, and other solicitation requirements as any other response submission method.

Read and review the solicitation package, including all exhibits, carefully before completing and submitting a response in the form and manner described in the solicitation package.

Questions the DPS point of contact in the solicitation package must address questions regarding the solicitation. The Point of Contact is identified in the solicitation package.

Submit the solicitation response in the form and manner described in the solicitation package on or before the response due date and time.

IMPORTANT: The solicitation package will identify the specific form and method of delivery. Failure to adhere to the requirements in the solicitation package may result in disqualification.

Access to the DPS Online Bid Room is a two-step process.

Step 1: Register as a vendor for the Online Bid Room at https://texasdps.appianportalsgov.com/vendor-management. It can take up to two business days to receive your username and password. If you do not receive this information within two days, Contact DPS-Online Bid Room Vendor Support

Step 2: Registered. You will receive your login credentials via email, and you can gain access to the DPS Online Bid Room to review solicitation opportunities and submit your response to the solicitation electronically.

View the DPS Online Bid Room Vendor Forms and Resources to help you navigate the site, be informed, and learn how to reach out for assistance. Online Bid Room Vendor Tutorial, Vendor User Guide, Frequently Asked Questions, Contact DPS-Online Bid Room Vendor Support

IMPORTANT: Allow enough time for the registration process to submit your bid by the response due date. **Late solicitation responses are not accepted.**

The optional use of the DPS Online Bid Room and any resulting technical difficulties that may prevent a successful, responsive electronic submission of a solicitation response do not constitute a sufficient basis for a protest of a contract award. ***Submissions via the DPS Online Bid Room will receive submission confirmation through the system. If confirmation is received through the DPS Online Bid Room, no additional confirmation of receipt is required.***