



REQUEST FOR QUALIFICATIONS
FOR
MOBILITY & INFRASTRUCTURE CONSULTING

WORKFORCE SOLUTIONS CAPITAL AREA

Release Date: February 10, 2023 - 1:00 PM (CST)
Response Due: February 27, 2023 - 1:00 PM (CST)

9001 N I-35, Suite 110E
Austin, Texas 78753
(512) 597-7100

www.wfscapitalarea.com


A proud partner of the  **americanjobcenter** network
Workforce Solutions Capital Area is an Equal Opportunity Employer/Program.
Auxiliary aids and services are available, upon request, to persons with disabilities.
Relay Texas: 1.800.735.2989 (TDD) / 711 (Voice)

Table of Contents

SECTION I – GENERAL INFORMATION	5
A. BACKGROUND INFORMATION.....	5
B. ELIGIBLE PROPOSERS	5
C. QUALIFICATIONS.....	5
D. SCOPE OF WORK.....	6
E. NARRATIVE INSTRUCTIONS	6
F. PROCUREMENT STANDARD.....	6
SECTION II – CONTRACT INFORMATION.....	6
A. AWARD	6
B. CONTRACT PERIOD	6
C. FUNDING CLAUSE	7
SECTION III – SUBMISSION INFORMATION.....	7
A. SUBMISSION	7
B. PROCUREMENT SCHEDULE*	7
C. TECHNICAL ASSISTANCE	7
D. AVAILABILITY OF RFQ.....	7
E. PROPRIETARY INFORMATION AND THE TEXAS PUBLIC INFORMATION ACT	8
SECTION IV – PROPOSAL RESPONSE REQUIREMENTS.....	8
A. PROPOSAL FORMAT.....	8
B. SUBMISSION ORDER.....	8
C. VALIDITY PERIOD	8
HISTORICALLY UNDERUTILIZED BUSINESS.....	9
SECTION V – EVALUATION PROCESS	9
EVALUATION CRITERIA	9
SECTION VI – RFQ GENERAL INFORMATION.....	10
A. PROCESS TO PROTEST.....	10
B. EQUAL OPPORTUNITY/NON-DISCRIMINATION	12
C. OPEN RECORDS.....	13
ATTACHMENT A - COVER SHEET	14
ATTACHMENT B - CERTIFICATION OF PROPOSER.....	15
ATTACHMENT C - CERTIFICATONS REGARDING LOBBYING, DEBARMENT, SUSPENSION AND OTHER RESPONSIBILITY MATTERS, AND DRUG-FREE WORKPLACE REQUIREMENTS	16
ATTACHMENT D - TEXAS CORPORATE FRANCHISE TAX CERTIFICATION	19

ATTACHMENT E - STATE ASSESSMENT CERTIFICATION.....	20
ATTACHMENT F – CERTIFICATION REGARDING CONFLICT OF INTEREST	21
ATTACHMENT G - CERTIFICATION OF LEGAL AND SIGNATORY AUTHORITY	22
ATTACHMENT H - CERTIFICATION REGARDING IMPLEMENTATION OF THE NON-DISCRIMINATION & EQUAL OPPORTUNITY PROVISIONS AND THE WORKFORCE INNOVATION AND OPPORTUNITY ACT (WIOA)	23
ATTACHMENT I - UNDOCUMENTED WORKER CERTIFICATION	24
EXHIBIT 1.....	25
Safeguards for TWC Information	25
EXHIBIT 2.....	31
Board Guidelines for Security	31
Section 1. Identify	33
1.1. Privacy and Confidentiality	33
1.2. Data Classification	33
1.3. Critical Information Asset Inventory	33
1.4. Enterprise Security Policy, Standards and Guidelines	33
1.4.1 Acceptable Use	33
1.4.2 Data Security Guidelines.....	33
1.5. Control Oversight and Safeguard Assurance.....	33
1.6. Information Security Risk Management.....	34
1.7. Security Oversight and Governance	34
1.8. Security Compliance and Regulatory Requirements Management	34
1.9. Cloud Usage and Security	34
1.10.Security Assessment and Authorization / Technology Risk Assessments	34
1.11.External Vendors and Third-Party Providers	34
Section 2. Protect.....	34
2.1. Enterprise Architecture, Roadmap and Emerging Technology	35
2.2. Secure System Services, Acquisition and Development.....	35
2.3. Security Awareness and Training.....	35
2.4. Privacy Awareness and Training	35
2.5. Cryptography	35
2.6. Secure Configuration Management	35
2.7. Change Management	35
2.8. Contingency Planning	35
2.9. Media.....	36
2.9.1 Removable Media.....	36
2.10. Physical and Environmental Protection.....	36
2.11. Personnel Security	36

2.12.	Third-Party Personnel Security	36
2.13.	System Configuration Hardening and Patch Management	36
2.13.1	System Configuration Hardening	36
2.13.2	Patch Management	37
2.14	Access Control	37
2.15	Account Management	37
2.15.1	User Verification	37
2.16	Security Systems Management	38
2.17	Network Access and Perimeter Controls	38
2.18	Internet Content Filtering	38
2.19	Data Loss Prevention	38
2.20	Identification and Authentication	38
2.21	Spam Filtering	39
2.22	Portable and Remote Computing	39
2.23	System Communications Protection	39
Section 3.	Detect	39
3.1	Vulnerability Assessment	39
3.2	Malware Protection	39
3.3	Security Monitoring and Event Analysis	39
Section 4.	Respond	40
4.1	Cybersecurity Incident Response	40
4.2	Privacy Incident Response	40
Section 5.	Recover	40
5.1	Disaster Recovery Procedures	40
EXHIBIT 3 -	Security Management and Texas Cybersecurity Framework	41
	Security Management	47
	Texas Cybersecurity Framework	47

SECTION I – GENERAL INFORMATION

PURPOSE OF REQUEST FOR QUALIFICATIONS (RFQ)

Workforce Solutions is seeking consultative services from an individual or agency until it is able to secure the services of a full-time personnel to lead the efforts internally. Upon selection of internal personnel, the consultant will provide transition training to ensure a smooth transition.

Further, the consultant may be engaged for continued services if the budget and scope of work allow.

A. BACKGROUND INFORMATION

The Workforce Solutions Capital Area Workforce Board (hereinafter, “WFS”, “the Board”, “Workforce Solutions”) serves as the leadership and governing body for the Austin/Travis County workforce system. The Board administers workforce development services/programs with its Board of Directors representing business, education, labor, economic development, community-based organizations, and public entities.

The Board was organized in 1984 as a non-profit corporation in the State of Texas, with tax-exempt status under IRS code 501(c)(3). It is part of the Texas Workforce Solutions Network – comprised of the Texas Workforce Commission (TWC) and twenty-eight (28) local workforce boards.

The Board also serves as the designated grant recipient and administrative entity for workforce development program funds allocated to the Austin/Travis County area.

B. ELIGIBLE PROPOSERS

Organizations and individuals possessing the capacity and demonstrated ability to perform successfully under the terms and conditions of a contract with the Board may respond to this RFQ. Eligible individuals include those who can demonstrate experience and expertise of similar scope as this RFQ. Eligible firms/brokers include public entities, community-based organizations, faith-based organizations, non-profit organizations, private for-profit corporations, and other qualified individuals. Minority, disadvantaged, veteran and/or women-owned businesses are encouraged to respond to this RFQ.

Entities that are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any federal department or agency are not eligible to respond to this RFQ or receive a contract.

C. QUALIFICATIONS

Individuals and entities with industry sector business development support experience, including but not limited to experience with public sector entities such as CapMetro, the City of Austin, or similar public entities charged with mobility and transit planning. A list of any related credentials may be attached to the Respondent’s submission.

D. SCOPE OF WORK

Individuals and/or entities selected for this work will provide consultative and project management services related to:

- 1) Representing Workforce Solutions Capital Area in mobility and transit initiatives. This activity includes serving as the public workforce system representative in discussions with CapMetro, Austin Transit Partnership, the Austin Airport, etc. in pursuit of talent development and talent sourcing solutions. The work will include organizing and leading committees and/or work groups as part of year one of setting up a Mobility and Infrastructure Industry Partnership.
- 2) Leading the Data Research Project to analyze the Regional Supply and Demand for mobility workforce. This activity will support the TWC TIP grant and other research-focused funding to analyze the mobility and infrastructure ecosystem. The research project will be procured separately, but the consultant will oversee the work.
- 3) Educating local leaders on the value and necessity of workforce programming in mobility and infrastructure projects. This activity may include making presentations to internal and external stakeholders, and creating briefing pieces for leadership related to infrastructure workforce needs.
- 4) Identifying and recommending available resources. This activity will support WFS leadership in identifying possible additional partnerships and funding sources to support the mobility and infrastructure work, as well as ensuring that those additions are included in the new Mobility and Infrastructure Industry Partnership.
- 5) Creating a work plan based on the results of the research project (#2) and other contributing factors resulting from discussions with stakeholders in the mobility, transit, and infrastructure industries.

E. NARRATIVE INSTRUCTIONS

Proposers should submit a proposal that demonstrates experience providing services such as those outlined in the above Scope of Work. Proposers should describe the process and expected timeline, including time requirements for participants, as well as expected outcomes. The proposer may include other relevant information to demonstrate what is reflected in this RFQ.

F. PROCUREMENT STANDARD

It is the policy of the Board to conduct procurement in a manner that provides for full and open competition. An award will be made only to an organization possessing the qualifications and demonstrated ability to perform successfully under the terms and conditions of a contract. The services solicited under this RFQ are procured under the methods outlined in the TWC Financial Manual for Grants and Contracts (FMGC).

SECTION II – CONTRACT INFORMATION

A. AWARD

The proposal most advantageous to the Board in terms of proposer's qualifications and quality of the proposal will be recommended for contract negotiations.

B. CONTRACT PERIOD

The contract period for the awarded entity is expected to commence upon signature, through December 31, 2023. Contract period may allow renewable for up to one (1) year based on vendor performance, WFS need, and funding availability. If additional funding is secured, the contract scope and budget may be negotiated and increased so long as the primary scope of work outlined remains in effect. The contract for the awarded entity may be terminated by either party with a 30-day written notice.

C. FUNDING CLAUSE

Workforce Solutions reserves the right to negotiate fees and costs with any vendor who is qualified per the evaluation criteria.

SECTION III – SUBMISSION INFORMATION

A. SUBMISSION

Electronic copy must be emailed to **WFS Procurements** at wfs.procurements@wfscapitalarea.com by Response Deadline, **1:00PM (CST) on February 10, 2023**. Proposals received after the due date and time will not be accepted or considered under this procurement. No exceptions will be made to this requirement for any reason.

B. PROCUREMENT SCHEDULE*

RFQ Release Date	February 10, 2023 by 1:00PM (CST)
Response Deadline	February 27, 2023 by 1:00PM (CST)
Electronic Submission Email	wfs.procurements@wfscapitalarea.com
Estimated Contract Start Date	Upon Signing through no later than December 31, 2023*
Proposers Questions Deadline	February 16, 2023 by 1:00PM (CST)
WFS Response to Questions no later than;	February 22, 2023 by 1:00PM (CST)

** Dates are subject to change*

C. TECHNICAL ASSISTANCE

No bidder's conference related to this RFQ will be held.

Proposals may be withdrawn upon written request if made before the response deadline. The cost of submissions or returning proposals that are withdrawn shall be the responsibility of the proposer. Once the response deadline is passed, all proposals will become the property of Workforce Solutions and will not be returned.

D. AVAILABILITY OF RFQ

The RFQ will be posted on The Board's website at <https://www.wfscapitalarea.com/procurements/> and the Electronic State Business Daily Search at <http://www.txsmartbuy.com/esbd>

E. PROPRIETARY INFORMATION AND THE TEXAS PUBLIC INFORMATION ACT

Proposer is hereby notified that the Board strictly adheres to all statutes, court decisions and the opinions of the Texas Attorney General with respect to disclosure of public information. The Board may seek to protect from disclosure all information submitted in response to this RFQ until a final agreement is executed. Upon execution of a final agreement, the Board will consider all information, documentation, and other materials requested to be submitted in response to this RFQ to be of a non-confidential and non-propriety nature; therefore, subject to public disclosure under Chapter 552.001. Proposer will be advised of a request for public information that applies to their materials and will have the opportunity to raise any objections to disclosure to the Texas Attorney General. Certain information that may be protected from release is noted in Sections 552.101, 552.110, 552.113 and 552.131 of the Government Code.

SECTION IV – PROPOSAL RESPONSE REQUIREMENTS

Proposals will become the Board's property and will not be returned.

A. PROPOSAL FORMAT

1. Each proposal must be accompanied by a complete proposal Cover Sheet (Attachment A);
2. Signatures are required for submission.
3. Proposals must contain all required elements in the order prescribed; and
4. Proposals that do not conform to the SUBMISSION ORDER may be considered non-responsive and excluded from consideration under this procurement.
5. Narrative Response must be included in the submission.

B. SUBMISSION ORDER

1. Cover Sheet (Attachment A)
2. Narrative Response
3. Proposed hourly rate for consultative services, as well as an approximate number of hours per month dedicated to this project.
4. Reference names and email addresses for 3 previous public sector entities you have provided services
5. Resumes of individual(s) providing the consulting services
6. Certification of Proposer (Attachment B)
7. Certifications Regarding Lobbying, Debarment and Drug-Free Workplace (Attachment C)
8. Texas Corporate Franchise Tax Certification (Attachment D)
9. State Assessment Certification (Attachment E)
10. Certification Regarding Conflict of Interest (Attachment F)
11. Certification of Legal and Signatory Authority (Attachment G)
12. Certification of Non-Discrimination & Equal Opportunity Provisions and the WIOA (Attachment H)
13. Undocumented Worker Certification (Attachment I)
14. Security Management and Texas Cybersecurity Framework Responses (EXHIBIT 3)
15. HUB Certificate (if, applicable)

C. VALIDITY PERIOD

Each response will remain valid for the Board's acceptance for a minimum of ninety (90) days after the submittal deadline, to allow for evaluation, selection, and Board action, if applicable.

HISTORICALLY UNDERUTILIZED BUSINESS

A "Historically Underutilized Business" is an entity with its principal place of business in Texas and is at least 51% owned by an Asian Pacific American, Black American, Hispanic American, Native American and/or American woman who reside in Texas and have a proportionate interest and demonstrate active participation in the control, operations, and management of the entity's affairs.

Five (5) bonus points will be awarded to responsive proposals submitted by a HUB certified by the Texas Comptroller of Public Accounts, or another bona fide certifying agency. **HUBs must identify their certifying agency on the cover sheet and attach a copy of the notice of certification to be eligible for points awarded under this section.** Certifications that are expired or do not meet the criteria specified shall not be considered for the five additional points.

Note: Finalists may be asked to provide a list of specific references. Finalists may also be asked to make a presentation of proposal strategies to WFSCA Board staff via Zoom.

SECTION V – EVALUATION PROCESS

EVALUATION CRITERIA

Qualifications will be evaluated to determine if the respondent has the organizational capability, demonstrated experience, and reasonableness in cost to perform the scope of work in this RFQ. Qualifiers must achieve an overall score of **at least 70 points** (excluding HUB/SWMBE bonus points) to be considered for selection and contract award. WFSCA will base the review and evaluation of qualifications upon the following criteria:

I.	Respondent's Past Performance	15 Points
II.	Overall Experience/Qualifications	25 Points
III.	Proposed Plan for Requested Services	30 Points
IV.	Hourly cost rate	30 Points

Historically Underutilized Business (HUB)

5 Bonus Points

A current copy of HUB certification certificate must be included in the submission.

TOTAL POSSIBLE POINTS FOR PROPOSAL RESPONSE

105 POINTS

SECTION VI – RFQ GENERAL INFORMATION

A. PROCESS TO PROTEST

Proposers who wish to protest a decision must utilize the following process:

Step 1. Requests for Debriefing – Proposers not selected by this procurement process may appeal the Board decision by submitting a request for debriefing to obtain information on the procurement process and how their proposal or offer was received and ranked within fifteen (15) working days of the receipt of the Board notification of the procurement decision.

The request for debriefing may be sent electronically to wfs.procurements@wfscapitalarea.com.

Registered mail **or** hand delivered is permissive for this RFQ, and will need to identify externally as “Dated Material” and addressed to:

Tamara Atkinson, Chief Executive Officer
Workforce Solutions Capital Area
9001 N IH35, Ste 110E
Austin, TX 78753

The Board shall acknowledge receipt of the request for debriefing in writing within three (3) days of receipt, along with the date and time of the scheduled debriefing. The debriefing shall be scheduled, as soon as possible, and no later than fifteen (15) working days from the receipt of the request for debriefing.

Step 2. Debriefing – The purpose of the debriefing is to promote the exchange of information, explain the Board proposal evaluation system, and help unsuccessful proposers understand why they were not selected. In the debriefing the respondent will obtain information on the procurement process, including the proposal evaluation process. Materials provided in the debriefing include a blank copy of the proposal scoring sheet used by readers, spread sheet of rankings provided to the Board of Directors, and written evaluators’ comments. Board staff will meet with the appealing party and review how the appealing party’s proposal or bid was scored or ranked. Bidders and proposers can gain a better understanding of the Board procurement processes and how to improve their bids or proposals. The debriefing is an educational opportunity for proposers, which hopefully will help them to improve the quality of any future proposals.

Step 3. Written Notice of Appeal – If, after the debriefing, the appealing party wishes to initiate the appeals process, they must submit to the Board a Notice of Appeal. This written notice must clearly state that it is an appeal and identify the funding decision being appealed (i.e. specific date of the RFQ, or the Workforce Board of Directors’ action); the name, address, and phone number of the appealing party(s); and specify the grounds of the appeal, including evidence to substantiate the grounds.

A Notice of Appeal must be received by the Board within ten (10) days of receipt of the Board debriefing meeting. **All appeals must be filed with and received by the Office of the CEO of the Board during normal business hours (Monday through Friday, 8:00 a.m. to 5:00 p.m., CST). Any appeal received after 5:00 p.m. (CST) shall be deemed filed on the next business day.** The failure of a bidder to file a timely appeal in accordance with this policy shall be deemed as a waiver of the Bidder’s right to appeal or otherwise challenge

any action or decision of the Board and the action or decision of the Board shall be deemed final in all respects.

The Notice of Appeal must be sent by registered mail or hand delivered (please request a receipt) clearly identified externally as “Dated Material” and addressed to:

Tamara Atkinson, Chief Executive Officer
Workforce Solutions Capital Area
9001 N IH35, Ste 110E
Austin, TX 78753

Telefax, Facsimile, or E-mail notices will not be accepted at any stage of the appeals process. The appealing party is solely responsible for the timely submission/receipt of the notice of appeal to the Board. Failure to follow the requirements of this policy shall be deemed as a waiver of the appealing party’s right to an appeal and the action or decision of the Board shall be deemed final in all respects.

All Appeals must contain the following information:

1. Identification of the specific procurement being appealed;
2. The contact name, address, phone, and e-mail address of the appealing party;
3. The specific grounds for the appeal;
4. A detailed statement of all disputed issues of material and relevant facts surrounding the action/decision taken and the alleged violations as a result of such action/decision;
5. A copy of any documents(s) upon which the Bidder relies to support their contention that the action/decision of the Board should be reversed or modified;
6. A request for a hearing; and
7. A statement of relief sought by the Bidder.

Written acknowledgement of receipt of the Notice of Appeal will be provided to the appealing party within ten (10) working days of the receipt of the Notice of Appeal. The Board shall provide the appealing party with the date and time of the next step, the Informal Hearing.

Step 4. Informal Hearing – An Informal Hearing will be held at the offices of Workforce Solutions Capital Area within fifteen (15) working days of the receipt of the Notice of Appeal. The CEO’s designee shall act as the Hearings Officer and will meet with the appealing party to discuss specific concerns and grounds for the appeal that were identified in the Notice of Appeal. The Board and the appealing party shall seek in good faith to resolve any or all the issues identified in the appeal. Failure of the appealing party to attend or participate in good faith in the Informal Hearing shall be deemed as a waiver of the appealing party’s right to a Formal Hearing and the action or decision of the Board shall be deemed final in all respects. The Hearing Officer may recommend to the Board’s CEO any appropriate actions allowable under applicable rules and regulations and consistent with agency policies to resolve issues raised at the Informal Hearing. If the appealing party agrees in writing with the decision/action of the Hearing Officer, the appeal shall be ended at this point.

Step 5. Request for a Formal Hearing – If the appealing party is not satisfied with the results of the Informal Hearing, they must inform the Hearing Officer, in writing, no later than fifteen (15) working days from the date of the Informal Hearing of the intent to proceed with the appeal. A request for a Formal Hearing must be made in writing and delivered to the Board pursuant to the instructions for submitting written notices of appeals in Step 3 above. The Request for Formal Appeal must state the specific grounds for the appeal and the remedy(ies) requested. Within fifteen (15) working days of the receipt of this written request, the

Hearing Officer will respond, in writing, to inform the appealing party of the time, date and place of the next step – the Formal Hearing.

Step 6. Formal Hearing – The Formal Hearing shall be conducted within fifteen (15) working days of the date of the Request for Formal Hearing. An independent Hearing Officer selected by the CEO will conduct the Formal Hearing of the appeal. The Hearing Office will deal only with those issues identified in the original notice of appeal. The Hearing Officer will consider the facts presented as the grounds for the appeal and remedies requested. The Hearing Officer may request additional information from Board staff or the appealing party. After full review, the Hearing Officer will render his/her decision not later than fifteen (15) working days from the date of the Formal Hearing. The Hearing Officer’s decision shall be provided to both parties in writing.

The recommendation/decision of the Hearing Officer shall be presented to the Workforce Solutions Capital Area Board of Directors for consideration and possible action at its next scheduled meeting, in the event the Hearing Officer sides with the appealing party. The Board is NOT obligated to accept the Hearing Officer’s decision and/or recommendations. The Board’s decision shall be considered final, and the end of the appeals process at the local level.

A postponement or continuance of the Informal Resolution Conference and/or Formal Hearing may be granted to the appealing party only upon written request filed with the Office of the CEO of the Board not less than three (3) calendar days (unless in cases of emergency) prior to the scheduled date of the Informal Resolution Conference and/or Formal Hearing. Such a request shall specify the reason(s) for the request for postponement or continuance. Requests for a postponement or continuance may be submitted in person, by fax or e-mail to the Office of the CEO of the Board. If a postponement or continuance is granted, the Informal Resolution Conference and/or Formal Hearing will be rescheduled at a date acceptable to the Hearing Officer, the Board, and the appealing party.

The outcome of an appeal at the local level shall be disclosed to the Texas Workforce Commission (TWC).

Miscellaneous – In all instances, information regarding protest/dispute will be disclosed to the Texas Workforce Commission (TWC). TWC’s Financial Manual for Grants and Contracts provides for limited appeals of any local decision.

B. EQUAL OPPORTUNITY/NON-DISCRIMINATION

As a condition of the award of financial assistance from the Department of Labor under Title I of WIOA, the grant applicant assures that it will comply fully with the nondiscrimination and equal opportunity provisions of the following laws:

- Section 188 of the Workforce Innovation and Opportunity Act of 2014 (WIOA), which prohibits discrimination against all individuals in the United States based on race, color, religion, sex, national origin, age, disability, political affiliation, or belief, and against beneficiaries based on either citizenship/status as a lawfully admitted immigrant authorized to work in United States or participation in any WIOA Title I financially assisted program or activity.
- Title VI of the Civil Rights Act of 1964, as amended, which prohibits discrimination on the bases of race, color, and national origin.
- Section 504 of the Rehabilitation Act of 1973, as amended, which prohibits discrimination against qualified individuals with disabilities.
- The Age Discrimination Act of 1975, as amended, which prohibits discrimination based on age.
- Title IX of the Education Amendments of 1972, as amended, which prohibits discrimination of the basis of sex in education programs.

The proposer also assures that it will comply with 29 CFR Part 37 and all other regulations implementing the laws listed above. This assurance applies to the grant applicant's operation of the WIOA Title I financially assisted program or activity, and to all agreements the grant applicant makes to carry out the WIOA Title financially assisted program or activity.

In addition, the proposers' assurance that it will fully comply with the nondiscrimination and equal opportunity provisions of the following:

- The Americans with Disabilities Act of 1990, as amended.
- The Non-Traditional Employment for Women Act of 1991, as amended.

C. OPEN RECORDS

Proposer is hereby notified that the Board strictly adheres to all statutes, court decisions, and the opinions of the Texas Attorney General with respect to disclosure of public information. Proposals submitted in response to this RFQ are subject to the Texas Public Information Act, Government Code Chapter 552, and may be disclosed to the public upon request. Therefore, any confidential or proprietary information contained within a proposal must be clearly identified by the proposer in the proposal itself (each applicable page clearly marked as confidential). Such information will be kept confidential by WFS to the extent that State law permits.

REQUEST FOR QUALIFICATIONS

MOBILITY & INFRASTRUCTURE CONSULTING

Legal Name of Proposing Entity	
Mailing Address	
Authorized Contact/Signatory Authority	
Phone Number	
E-Mail	
Type of Organization	<input type="checkbox"/> Private for-profit <input type="checkbox"/> Private non-profit <input type="checkbox"/> Government Agency <input type="checkbox"/> Partnership <input type="checkbox"/> Sole Proprietor <input type="checkbox"/> Other (specify)
Date Established	
Federal EIN	
Texas State Comptroller ID Number	
Historically Underutilized Business?	<input type="checkbox"/> Yes (if yes, attached current certificate is required) <input type="checkbox"/> No
Typed Name & title of Authorized Signatory	
Signature	

ATTACHMENT B - CERTIFICATION OF PROPOSER

I hereby certify that the information contained in this proposal and any attachments is true and correct and may be viewed as an accurate representation of proposed services to be provided and the administrative, management and financial systems of this organization. I certify that no employee of Workforce Solutions has assisted in the preparation of this proposal.

I acknowledge that I have read and understand the requirements and provisions of the RFQ and that the organization will comply with applicable local, state, and federal regulations and directives in the implementation of the program. I also certify that I have read and understand the Limitations and Condition section presented in this RFQ and will comply with the terms.

This proposal is a firm offer for a minimum of 90 days.

I, _____ certify that I am the
(Typed Name)

_____ of the corporation, partnership, organization, or other
(Typed Title)

entity named as Respondent herein and that I am authorized to sign this proposal and submit it to the Workforce Solutions Capital Area Workforce Board on behalf of said organization by authority of its governing body.

(Signature)

(Address)

(Phone)

ATTACHMENT C - CERTIFICATONS REGARDING LOBBYING, DEBARMENT, SUSPENSION AND OTHER RESPONSIBILITY MATTERS, AND DRUG-FREE WORKPLACE REQUIREMENTS

Lobbying: This certification is required by the Federal Regulations, implementing Section 1352 of the Program Fraud and Civil Remedies Act, Title 31 U.S. Code, for the Department of Education (34 CFR Part 82), Department of Health and Human Services (45 CFR Part 93).

The undersigned contractor certifies that:

- (1) No federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan or cooperative agreement.
- (2) If any funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, and officer or employee of Congress, or an employee of a Member of Congress in connection with this federal contract, grant, loan or cooperative agreement, the undersigned shall complete and submit Standard Form — LLL, "Disclosure Form to Report Lobbying", in accordance with its instructions.
- (3) The undersigned shall require that the language of this certification be included in the award documents for all sub awards at all tiers (including subcontracts, sub grants, and contracts under grants, loans, and cooperative agreements) and that all sub recipients shall certify and disclose accordingly.

Debarment, Suspension, and Other Responsibility Matters: This certification is required by the Federal Regulations, implementing, Executive Order 12549, Government-wide Debarment and Suspension, for the Department of Agriculture (7 CFR Part 3017), Department of Labor (29 CFR Part 98), Department of Education (34 CFR Parts 85, 668 and 682), Department of Health and Human Services (45 CFR Part 76).

The undersigned contractor certifies that neither it nor its principals:

- (1) Are presently debarred, suspended, proposed for debarment, and declared ineligible or voluntarily excluded from participation in this transaction by any federal department or agency.
- (2) Have not within a three-year period preceding this contract been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, State or Local) transaction or contract under a public transaction, violation of Federal or State

antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

- (3) Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity with commission of any of the offenses enumerated in Paragraph (2) of this certification; and,
- (4) Have not within a three-year period preceding this contract had one or more public transactions terminated for cause or default.

Where the prospective recipient of federal assistance funds is unable to certify to any of the statements in this certification, such prospective recipient shall attach an explanation to this certification.

Drug-Free Workplace: This certification is required by the Federal Regulations, implementing Sections 5151-5160 of the Drug-Free Workplace Act, 41 U.S.C. 701; for the Department of Agriculture (7 CFR Part 3017), Department of Labor (29 CFR Part 98), Department of Education (34 CFR Parts 85, 668 and 682), and Department of Health and Human Services (45 CFR Part 76).

The undersigned contractor certifies that it shall provide a drug-free workplace by:

- (1) Publishing a policy statement notifying employees that the unlawful manufacture, distribution, dispensing, possession or use of a controlled substance is prohibited in the workplace and specifying the consequences of any such action by an employee;
- (2) Establishing an ongoing drug-free awareness program to inform employees of the dangers of drug abuse in the workplace, the Contractor's policy of maintaining a drug-free workplace, the availability of counseling, rehabilitation and employee assistance programs, and the penalties that may be imposed on employees for drug abuse violations in the workplace;
- (3) Providing each employee with a copy of the Contractor's policy statement;
- (4) Notifying the employees in the Contractor's policy statement that as a condition of employment under this contract, employees shall abide by the terms of the policy statement and notifying the Contractor in writing within five days after any conviction for a violation by the employee of a criminal drug statute in the workplace;
- (5) Notifying Workforce Solutions within ten days of Contractor's receipt of a notice of a conviction of an employee; and,
- (6) Taking appropriate personnel action against an employee convicted of violating a criminal drug statute or requires such employee to participate in a drug abuse assistance or rehabilitation program.

These certifications are a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering this transaction.

Signature and Date

Type Name and Title

ATTACHMENT D - TEXAS CORPORATE FRANCHISE TAX CERTIFICATION

Pursuant to Article 2.45, Texas Business Corporation Act, state agencies may not contract with a for-profit corporation that is delinquent in making state franchise tax payments. The following certification that the corporation entering this contract is current in its franchise taxes must be signed by the individual on Form 203, Corporate Board of Directors Resolution, to sign the contract for the corporation.

The undersigned authorized representative of the corporation contracting herein certifies that the following indicated statement is true and correct and that the undersigned understands making a false statement is a material breach of contract and is grounds for contract cancellation.

Indicate the certification that applies to your corporation:

_____ The Corporation is a for-profit corporation and certifies that it is not delinquent in its franchise tax payments to the State of Texas.

_____ The Corporation is a non-profit corporation or is otherwise not subject to payment of franchise taxes to the State of Texas.

Signature

Date

Type Name and Title

ATTACHMENT E - STATE ASSESSMENT CERTIFICATION

The undersigned authorized representative of the firm or individual contracting herein certifies that the following indicated statement is true and correct and that the undersigned understands making a false statement is a material breach of contract and is grounds for contract cancellation.

The firm or individual certifies that:

_____Is current in Unemployment Insurance taxes, Payday and Child Labor law monetary obligations, and Proprietary School fees and assessments payable to the State of Texas.

_____Has no outstanding Unemployment Insurance overpayment balance payable to the State of Texas.

Signature and Date

Type Name and Title

ATTACHMENT F – CERTIFICATION REGARDING CONFLICT OF INTEREST

By signature of this proposal, Proposer covenants and affirms that:

- (1) no manager, employee or paid consultant of the Proposer is a member of the Board, the Executive Director, or an employee of the Board;
- (2) no manager or paid consultant of the Proposer is married to a member of the Board, the Executive Director, or an employee of the Board;
- (3) no member of THE BOARD, the Chief Executive Officer or employee of the Board owns or controls more than a 10 percent interest in the Proposer;
- (4) no spouse or member of the Board, Chief Executive Officer or employee of the Board is a manager or paid consultant of the Proposer;
- (5) no member of the Board, the Chief Executive Officer or employee of the Board receives compensation from Proposer for lobbying activities as defined in Chapter 305 of the Texas Government Code;
- (6) Proposer has disclosed within the Proposal any interest, fact or circumstance which does or may present a potential conflict of interest;
- (7) should Proposer fail to abide by the foregoing covenants and affirmations regarding conflict of interest, Proposer shall not be entitled to the recovery of any costs or expenses incurred in relation to any contract with the Board and shall immediately refund to the Board any fees or expenses that may have been paid under the contract and shall further be liable for any other costs incurred or damages sustained by the Board relating to that contract.

Disclosure of Potential Conflict of Interest (Please describe): _____

Name of Organization

Signature of Authorized Representative

Date

Typed/Printed Name and Title of Authorized Representative

ATTACHMENT G - CERTIFICATION OF LEGAL AND SIGNATORY AUTHORITY

I, _____ (typed or printed name) certify that I am the _____ (typed or printed title) of the eligible entity named as bidder and respondent herein, and I am legally authorized to sign and submit this proposal to Workforce Solutions Capital Area (WFS) on behalf of said organization by authority of its governing body.

I certify that _____ (typed or printed name) who signed the cover sheet of this proposal has the legal authority to enter and execute a contract with WFS to provide the services and activities authorized and detailed in this proposal. I agree to submit upon request by WFS such information and documentation as may be necessary to verify the certification contained herein.

I further certify that the information contained in this proposal and all attachments is true and correct. I certify that no officer, employee, board member, or authorized agent of WFS has assisted in the preparation of this proposal. I acknowledge that I have read and understand the requirement and provisions of this RFQ, and that this organization will comply with all applicable federal, state, and local laws, rules, regulations, policies and directives in the implementation of this proposal. I certify that I have read and understand the governing provisions, limitations, and administrative requirements of this RFQ and will comply with all terms and conditions.

Name of Organization (Proposer)

Signature of Authorized Representative

Date

Typed/Printed Name and Title of Authorized Representative

ATTACHMENT H - CERTIFICATION REGARDING IMPLEMENTATION OF THE NON-DISCRIMINATION & EQUAL OPPORTUNITY PROVISIONS AND THE WORKFORCE INNOVATION AND OPPORTUNITY ACT (WIOA)

As a condition to the award of financial assistance from the Department of Labor (DOL) under Title I of the Workforce Innovation and Opportunity Act (WIOA), the bidder assures that it will comply fully with the nondiscrimination and equal opportunity provisions of the following laws:

Section 188 prohibits discrimination against all individuals in the United States on the basis of race, color, religion, sex, national origin, age, disability, political affiliation or belief, and against beneficiaries on the basis of either citizenship/status as a lawfully admitted immigrant authorized to work in the United States or participation in any WIOA Title I—financially assisted program or activity;

Title VI of the Civil Rights Act of 1964, as amended, which prohibits discrimination on the bases of race, color and national origin;

Section 504 of the Rehabilitation Act of 1973, as amended, which prohibits discrimination against qualified individuals with disabilities;

The Age Discrimination Act of 1975, as amended, which prohibits discrimination on the basis of age; and

Title IX of the Education Amendments of 1972, as amended, which prohibits discrimination on the basis of sex in educational programs.

The bidder also assures that it will comply with 29 CFR part 38 and all other regulations implementing the laws listed above. This assurance applies to the bidder's operation of the WIOA Title I---financially assisted program or activity, and to all agreements the grant applicant makes to carry out the WIOA Title I---financially assisted program or activity. The bidder understands that the United States has the right to seek judicial enforcement of this assurance.

Applicant's signature below indicates organization is agreeing to comply fully with the assurance and certifications as part of its responsibilities as a successful contractor.

Signature of Authorized Representative

Date

Name and Title of Authorized Representative

ATTACHMENT I - UNDOCUMENTED WORKER CERTIFICATION

Effective September 1, 2007, HB 1196 amended Subtitle F, Title 10, of the Texas Government Code to add Subsection 2264. Chapter 2264 directs public agencies, state or local taxing jurisdictions, and economic development corporations (public entities) to require that any business applying to receive public subsidies include in the application a statement certifying that the business, or branch, division or department of the business does not and will not knowingly employ an undocumented worker.

If a business grantee is found in violation of 8U.S.C. subsection 1324a(f), consistent with the requirements of Texas Government Code subsection 2264, Boards are permitted to bring a civil action to recover any amounts owed, as well as court costs and reasonable attorney's fees.

Penalties incurred by business grantees shall be assessed damages at a rate of 20% of contract award. Said damages shall be made payable to Workforce Solutions Capital Area within 120 days of receiving the notice of violation.

DEFINITION OF TERMS

Public Subsidy – is broadly defined Texas Government Code §2264.001 (3) as a public program or public benefit or assistance of any type that is designed to stimulate the economic development of a corporation, industry, or sector of the state's economy or to create or retain jobs in Texas. The term includes, among other things, bonds, grants, loans, loan guarantees, benefits relating to an enterprise or empowerment zone, infrastructure development and improvements designed to principally benefit a single business or defined group of businesses, and matching funds. The Commission's Office of General Counsel has found that HB 1196 does not apply to the acquisition of goods and services.

Undocumented Worker – is defined as an individual who, at the time of employment, is not lawfully admitted for permanent residence in the United States or is not authorized under law to be employed in that manner in the United States.

Certification - Contractor certifies that no undocumented workers will be employed during the execution of this contract. By the signature indicated below, the contractor verifies their understanding of the terms and conditions of this requirement.

Name of Proposing Individual or Organization: _____

Name and Title of Authorized Signatory: _____

Signature of Authorized Representative: _____ Date: _____

Safeguards for TWC Information

The Board, Board staff, and subrecipients shall comply with these safeguards:

1. **Safeguards:** Maintain sufficient safeguards over all TWC Information to prevent unauthorized access to or disclosure of TWC Information. Board shall assure that Board staff, Board subrecipients, Board contractors and Board subcontractor staff comply with all safeguards and responsibilities of TWC Information Technology Security Guidelines and this Attachment A. Board shall be responsible for compliance by Board staff, Board subrecipients, Board contractors and Board subcontractor staff and shall be liable for any damages resulting from failure by Board staff, Board subrecipients, Board contractors or Board subcontractor staff to comply with these safeguards.

“TWC Information” means records maintained by the Agency, and records obtained by Board, Board staff, Board contractor, and Board subcontractor staff from the Agency under this Agreement, including (1) records and data compilations provided electronically, on paper, or via online access or e-mail, (2) records and data compilations that Board, Board staff, Board contractor, or Board subcontractor staff have converted into another format or medium (such as handwritten or electronic notes), and (3) records and data compilations incorporated in any manner into Board, Board staff, Board contractor, or Board subcontractor staff records, files, or data compilations.

2. **Monitoring:** Monitor its Users’, including Board staff, Board subrecipients, Board contractors and Board subcontractor staff, access to and use of TWC Information, and shall ensure that TWC Information is used only for the limited purpose of fulfilling Board obligations under this Agreement (limited purpose). The Board shall also ensure that TWC Information is used only for purposes authorized by law and in compliance with all other provisions of this Agreement. The Board shall require that all Board subrecipients monitor access to and use of TWC Information by Board subcontractor staff.
3. **Storage and Protection:** Board, Board staff, Board subrecipient, Board contractor and Board subcontractor staff shall store and process TWC Information in a place physically secure from access by unauthorized persons by any means.

4. Access: Board, Board staff, Board subrecipient, Board contractor and Board subcontractor staff shall undertake precautions to ensure that only authorized personnel are given access to TWC Information stored in computer systems.
5. Instruction: Board, Board staff, Board subrecipient, Board contractor and Board subcontractor staff shall instruct all personnel having access to TWC Information about all confidentiality requirements including the requirements of 20 C.F.R. Part 603, Texas Labor Code § 301.85, and 40 TAC Chapter 815, as well as the sanctions specified in this Agreement and under state and federal law for unauthorized use or disclosure of TWC Information. Board acknowledges that all personnel who will have access to TWC Information have been instructed as required.
6. Disposal: Board, Board staff, Board subrecipient, Board contractor and Board subcontractor staff shall dispose of TWC Information and any copies thereof after the limited purpose is achieved, except for TWC Information possessed by any court. Disposal means return of TWC Information to Agency or destruction of TWC Information, as directed by Agency. Disposal includes deletion of personal identifiers in lieu of destruction. In any case, Board, Board staff, Board subrecipient, Board contractor and Board subcontractor staff shall dispose of all TWC Information as required by this Agreement and the Board's written records retention requirements.
7. System: Board, Board staff, Board subrecipient, Board contractor, and Board subcontractor staff shall establish and maintain a system sufficient to allow an audit of compliance with the requirements of this Attachment A and the other provisions of this Agreement. The Board and Board contractor shall keep and maintain complete and accurate records sufficient to allow the Agency, the Texas State Auditor's Office, the United States government, and their authorized representatives to determine the compliance by Board and Board contractor with this Agreement.
8. No Disclosure or Release: Board, Board staff, Board subrecipient, Board contractor, and Board subcontractor staff shall not disclose or release any TWC Information other than as permitted in this Agreement, without prior written consent of Agency.
9. Unauthorized Disclosure: It is a breach of this Agreement to disclose TWC Information orally, electronically, in written or printed form, or in any other manner without the prior written consent of Agency:

- 9.1 to any subrecipient employee of Board or subrecipient employee of Board subrecipient or any individual not directly employed by Board or Board subrecipient;
 - 9.2 to another government entity, including a law enforcement entity; or
 - 9.3 to Board or Board subrecipient employees who do not have a need to use TWC Information for the limited purpose under this agreement.
10. Authorized Disclosure: TWC Information may only be disclosed to employees under the direct hiring-and-firing control of Board or Board subrecipient who have a need to use the TWC Information for the limited purpose under this agreement.
11. Security Violation: Board and Board subrecipient shall monitor access of Users and shall notify Agency within twenty-four (24) hours if a security violation of this Agreement is detected, or if Board or Board subrecipient suspects that the security or integrity of TWC Information has or may have been compromised in any way. The time period for notifying TWC under this section is reduced to one (1) hour for suspected security violations that involve protected health information of a covered under 45 C.F.R. Parts 160, 162, and 164, such as Medicaid Information provided from, by or accessed through the Health and Human Services Commission systems as required by the Health Information and Portability and Accountability Act (HIPAA) and the Health Information Technology Act (HITECH).
12. Breach Notice: In accordance with Texas Business and Commerce Code, Section 521.053 the Board shall provide notification to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
13. Format: TWC Information is subject to the requirements of this Agreement even if the TWC Information is converted by Board, Board staff, Board subrecipient, Board contractor, or Board subcontractor staff into another format or medium, or incorporated in any manner into Board or Board subrecipient records, files, or data compilations.
14. Access Limited: Board and Board subcontractor shall limit access to TWC Information to their employees who need access to achieve the Limited Purpose.

15. Mobile Device and Removal: Board, Board staff, Board subrecipient, Board contractor, and Board subcontractor staff shall not place TWC Information on mobile, remote, or portable storage devices, or remove storage media from Board or Board subrecipient facility, without the prior written authorization of Agency.
16. Public Information Act:
- 16.1 Unemployment Information: Under Texas Labor Code § 301.085, individually identifiable information regarding unemployment insurance benefits applicants and recipients and employer tax reported information is not “public information” for purposes of the Texas Public Information Act, Texas Government Code, Chapter 552. Board, Board staff, Board subrecipient, Board contractor, and Board subcontractor staff shall not release any TWC Information in response to a request made under the Public Information Act or under any other law, regulation, or ordinance addressing public access to government records.
- 16.2 Job Matching Services: Individually identifiable information maintained in the WorkInTexas system is not “public information” for purposes of the Public Information Act. Board, Board staff, Board subrecipient, Board contractor, and Board subcontractor staff shall not release any individually identifiable information from the WorkInTexas system in response to a request made under the Public Information Act or under any other law, regulation, or ordinance addressing public access to government records.
- 16.3 Education Records: “Student record” as defined in the Family Educational Rights and Privacy Act (FERPA) is not “public information” for purposes of the Public Information Act. Boards, Board staff, Board subrecipient, Board contractor, and Board subcontractor staff shall not release any “student records” collected, used or maintained in response to a request made under the Public Information Act or under any other law, regulation, or ordinance addressing public access to government records.
- 16.4 Protected Health Information: Protected health information as defined in Texas Health and Safety Code, Chapter 181 and 45 C.F.R. Parts 160, 162, and 164, such as Medicaid information provided from, by or accessed through the Health and Human Services Commission systems as required by the HIPAA and HITECH, is not subject to release under

the Public Information Act. Boards, Board staff, Board subrecipients, Board contractor and Board subcontractor staff shall not release any protected health information except in accordance with law as applicable to the information and shall secure the information consistent with applicable laws.

17. Subpoena: Notify the Agency within twenty-four (24) hours of the receipt of any subpoena, other judicial request, or request for appearance for testimony upon any matter concerning TWC Information. Federal regulations dictate the handling of subpoenas for TWC Information. Board or Board subrecipient shall comply with the subpoena handling requirements applicable to the information, including 20 C.F.R. § 603.7 in responding to any subpoena, other judicial request, or request for appearance for testimony upon any matter concerning TWC Information relating to unemployment compensation and employer tax information.
18. Federal Regulation: Comply with all requirements in federal and state law for safeguarding TWC Information, including 20 C.F.R. § 603.9 relating to safeguarding TWC unemployment compensation and employer tax information and insuring its confidentiality. Various federal and state laws and regulations, including but not limited to FERPA, FERPA regulations, HIPAA, HIPAA regulations, and the HITECH Act may also protect TWC.
19. Unauthorized Lookup: Shall not access TWC Information listed under the employee's Social Security number (SSN) or the SSN of a co-worker, family member, or friend.
20. Screening: Permit access to TWC Information only to employees that the Board or Board subrecipient has determined poses no threat to the security of TWC Information.
21. Internet: Board, Board staff, Board subrecipient, Board contractor, and Board subcontractor staff shall not transmit any TWC Information over the Internet unless it is encrypted using TWC approved encryption standards.
22. No Transfer: Board and Board subcontractor shall not transfer the authority or ability to access or maintain TWC Information under this Agreement to any other person or entity.
23. Resource Access Control Facility (RACF) Manager: The Board shall designate an initial RACF Manager and any subsequent RACF Managers in writing to the Agency. All designated RACF

Managers must execute a P-41 Texas Workforce Commission Information Resources Usage Agreement, and complete Security Training and Agency RACF Manager Training (“Manager Training”). The Agency will not authorize access to a designated RACF Manager until Agency RACF Administration has received copies of the designee’s Training Certificate, certificate of completion of Manager Training (“Manager Training Certificate”) and completed a P-41 Texas Workforce Commission Information Resources Usage Agreement. The RACF Manager shall create a written report within fifteen (15) calendar days after the end of each month, listing all Users authorized for online access at any time during the previous month including the unique identifier and work address of each User. The RACF Manager shall immediately terminate access of any User no longer employed by the Board or Board subrecipient or any User whose job responsibilities no longer require access to TWC Information. The RACF Manager shall provide a copy of all reports, and a list of the names, unique identifiers, and work addresses of all current Users, with P-41 Texas Workforce Commission Information Resources Usage Agreements and copies of Training Certificates attached, at any time upon Agency request. A unique identifier may be used on all reports in lieu of SSN provided that the User SSN is available upon request. The Board shall be responsible for ensuring that each RACF Manager complies with the provisions of this Agreement and shall be liable and responsible for all actions of each RACF Manager.

The RACF Manager shall provide a copy of all reports and a list of external agencies and community partners with P-48 TWC Systems Access and Data Security Report for Other Agencies and Community Partners, at any time upon Agency request.

Board Guidelines for Security

These guidelines provide the minimum acceptable standards for the Texas Cybersecurity Framework (TCF) control objectives.

Contents

Section 1. Identify	33
1.1. Privacy and Confidentiality	33
1.2. Data Classification	33
1.3. Critical Information Asset Inventory	33
1.4. Enterprise Security Policy, Standards and Guidelines	33
1.4.1 Acceptable Use	33
1.4.2 Data Security Guidelines	33
1.5. Control Oversight and Safeguard Assurance	33
1.6. Information Security Risk Management	34
1.7. Security Oversight and Governance	34
1.8. Security Compliance and Regulatory Requirements Management	34
1.9. Cloud Usage and Security	34
1.10. Security Assessment and Authorization / Technology Risk Assessments	34
1.11. External Vendors and Third-Party Providers	34
Section 2. Protect	34
2.1. Enterprise Architecture, Roadmap and Emerging Technology	35
2.2. Secure System Services, Acquisition and Development	35
2.3. Security Awareness and Training	35
2.4. Privacy Awareness and Training	35
2.5. Cryptography	35
2.6. Secure Configuration Management	35
2.7. Change Management	35
2.8. Contingency Planning	35
2.9. Media	36
2.9.1 Removable Media	36
2.10. Physical and Environmental Protection	36
2.11. Personnel Security	36
2.12. Third-Party Personnel Security	36
2.13. System Configuration Hardening and Patch Management	36

<u>2.13.1 System Configuration Hardening</u>	36
<u>2.13.2 Patch Management</u>	37
<u>2.14 Access Control</u>	37
<u>2.15 Account Management</u>	37
<u>2.15.1 User Verification</u>	37
<u>2.16 Security Systems Management</u>	38
<u>2.17 Network Access and Perimeter Controls</u>	38
<u>2.18 Internet Content Filtering</u>	38
<u>2.19 Data Loss Prevention</u>	38
<u>2.20 Identification and Authentication</u>	38
<u>2.21 Spam Filtering</u>	39
<u>2.22 Portable and Remote Computing</u>	39
<u>2.23 System Communications Protection</u>	39
<u>Section 3. Detect</u>	39
<u>3.1 Vulnerability Assessment</u>	39
<u>3.2 Malware Protection</u>	39
<u>3.3 Security Monitoring and Event Analysis</u>	39
<u>Section 4. Respond</u>	40
<u>4.1 Cybersecurity Incident Response</u>	40
<u>4.2 Privacy Incident Response</u>	40
<u>Section 5. Recover</u>	40
<u>5.1 Disaster Recovery Procedures</u>	40

Section 1. Identify

1.1. Privacy and Confidentiality

Ensuring the appropriate security of retained information and approved sharing under defined conditions with required safeguards and assurance. Includes the requirements of HIPAA, Texas Business & Commerce Code, and agency defined privacy policies that include and expand upon regulatory and legal requirements for establishing contractual/legal agreements for appropriate and exchange and protection.

1.2. Data Classification

All data within the Board must be classified and systems must be categorized by the system Owner. The default classification for all electronic data is Confidential.

Data will be classified into one of three groups of sensitivity: Confidential, Board Sensitive or Public. Data must be protected in accordance with the security controls specified for the classification level that it is assigned.

1.3. Critical Information Asset Inventory

Identification and prioritization of all the Board's information assets so that they are prioritized according to criticality to the business, so that protections can be applied commensurate with the asset's importance.

1.4. Enterprise Security Policy, Standards and Guidelines

1.4.1 Acceptable Use

Any TWC provided computer data, hardware, and software is the property of the state. All information passing through the TWC network, which has not been specifically identified as the property of other parties, will be treated as a TWC asset. Unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information is prohibited. Information entrusted to TWC will be protected in a manner consistent with its confidentiality and in accordance with all applicable standards, agreements, and laws. Every information system privilege that has not been explicitly authorized is prohibited. Such privileges will not be authorized for any TWC business purpose until approved in writing.

1.4.2 Data Security Guidelines

The Agency shall provide automated security and security procedures for Agency administered custom applications.

The Agency shall provide standards and guidelines for use of any unsecured networks, such as the public Internet, for transport of confidential data.

Logical and physical access to all information resources (hardware and software) residing in public access areas, shall be controlled by the Board, its subrecipients, contractors, subcontractors, or Agency staff as appropriate.

1.5. Control Oversight and Safeguard Assurance

Catalog the security activities that are required to provide the appropriate security of information and information resources throughout the Enterprise. Evaluate the control activities that have been implemented in terms of maturity, scope/breadth of implementation, effectiveness, or associated deficiency to assure required protection levels as specified by security policy, regulatory/legal requirements, compliance mandates, or organizational risk thresholds. Ensure that control activities are performed as required and performed in a manner that is auditable

and verifiable. Identify control activities that are not implemented or are not effective at achieving the defined control objectives. Oversee the implementation of required controls to ensure ongoing audit readiness and effective control implementations.

1.6. Information Security Risk Management

A risk assessment of the Board's information and information systems shall be performed and documented.

- (1) The inherent impact will be ranked, at a minimum, as either "High," "Moderate," or "Low".
- (2) The frequency of the future risk assessments will be documented.
- (3) Approval of the security risk acceptance, transference, or mitigation decision shall be the responsibility of:
 - a. The information owner or his or her designee(s) for systems identified with a Low or Moderate residual risk.
 - b. The Board's Chief Executive Officer for all systems identified with a residual High Risk.

1.7. Security Oversight and Governance

The Board shall have a group of fully empowered decision makers that meets at least quarterly to govern security-policy issues according to a documented charter.

1.8. Security Compliance and Regulatory Requirements Management

Monitor the legislative and industry landscape to ensure security policy is updated in consideration of changes that are pertinent or applicable to the organization. Facilitate any validation audits, assessments or reporting that is necessary to assure compliance to applicable laws, regulations, or requirements. Includes the HIPAA Privacy Office(r), IRS Safeguard Reviews, and responses to third party inquiries into the security of the organization.

1.9. Cloud Usage and Security

The assessment and evaluation of risk with the use of "cloud" technologies including Software as a Service (SAAS), Platform as a Service (PAAS), and Infrastructure as a Service (IAAS), to ensure that business operations can deliver programs and services efficiently and effectively within acceptable tolerances mitigating potential negative outcomes.

1.10. Security Assessment and Authorization / Technology Risk Assessments

Evaluate systems and applications in terms of design and architecture in conjunction with existing or available controls to ensure that current and anticipated threats are mitigated within established risk tolerances. Includes an analysis of in-place systems periodically or when significant change occurs as well as the analysis of the introduction of new technology systems.

1.11. External Vendors and Third-Party Providers

Evaluate third-party providers and external vendors to ensure security requirements are met for information and information resources that will be transmitted, processed, stored, or managed by external entities. Includes contract review as well as the development of service level agreements and requirements.

Section 2. Protect

2.1. Enterprise Architecture, Roadmap and Emerging Technology

Maintain an enterprise information security architecture that is aligned with Federal, State, Local and Board data security and privacy requirements. Use a roadmap and emerging technology evaluation process to stay abreast of the continued evolution of security solutions, processes, and technology.

2.2. Secure System Services, Acquisition and Development

Ensure that the development and implementation of new systems meets the requirements necessary to assure the security of information and resources.

2.3. Security Awareness and Training

The Board shall require all persons to whom it grants access to Agency applications to annually complete the Cybersecurity Awareness Training provided by the Agency for Agency employees. This training is available at https://twc.texas.gov/development/train/board_and_contractor_training_links.html

2.4. Privacy Awareness and Training

The Board shall require all persons to whom it grants access to Agency applications to annually complete the Sensitive Personal Information (SPI) Training provided by the Agency for Agency employees. This training is available at https://twc.texas.gov/development/train/board_and_contractor_training_links.html

2.5. Cryptography

Establish the rules and administrative guidelines governing the use of cryptography and key management in order to ensure that data is not disclosed or made inaccessible due to an inability to decrypt.

2.6. Secure Configuration Management

Ensure that baseline configurations and inventories of information systems (including hardware, software, firmware, and documentation) are established and maintained throughout the respective system development life cycles. Establish and enforce security configuration settings for information technology products employed in information systems. Ensure all systems are operating under configurations that have been agreed upon according to organizational risk management.

2.7. Change Management

Changes include, but are not limited to implementation of new functionality, interruption of services, maintenance activity and repair of existing functionality and/or removal of existing functionality.

Change management will be required based on a risk assessment of the information resources (including operating systems, computing hardware, networks, and applications).

The change management process shall include the analysis of potential security impacts to the information system as a result of the change.

Scheduled changes must be reviewed by the appropriate IT staff and data Owner(s) prior to the change. These review staff may deny or delay the change if it is determined that the change has not been adequately planned for, suffers from inadequate backup planning, will negatively impact a key business process, or adequate resources cannot be made available to support the change.

2.8. Contingency Planning

Plans for emergency response, backup operations, and post-incident occurrence recovery for information systems are established, maintained, and effectively implemented to ensure the availability of critical information resources and continuity of operations in emergency situations. Backing up data and applications is a business requirement. It enables the recovery of data and applications in the event of loss or damage (natural disasters, system disk and other systems failures, intentional or unintentional human acts, data entry errors, or systems operator errors).

2.9. Media

2.9.1 Removable Media

Removable media is defined as, but not limited to, diskettes, tapes, compact discs, DVDs & Blu-ray discs, memory cards/sticks, USB/Firewire "Flash" key/pen/thumb drives, portable mass storage devices such as external hard drives, personal audio/video players such as iPods, tablets, cellular telephones, and smart phones with or without expandable memory capabilities.

The Board shall prohibit the use of personally owned removable media unless specific exemption is granted by an authorized executive of the Board.

The Board shall require that any Agency data placed on removable media be encrypted.

In the event of loss or theft of removable media containing Agency data, the Board shall notify the TWC Chief Information Security Officer and include a complete description of the data, including an index or table of contents of those data.

The Board shall cause all removable media to be scanned for viruses, worms, Trojans, and any other malicious code prior to its use with Agency data or systems.

The Board shall assure that the reuse or disposal of removable media follows data sanitization guidelines in compliance with National Institutes of Standards and Technology Special Publication 800-88 Guidelines for Media Sanitization in order to assure removal of any electronic protected, confidential and/or sensitive Agency data.

2.10. Physical and Environmental Protection

Assure that physical access to information systems, equipment, and the respective operating environments is limited to authorized individuals. Protect the physical locations and support infrastructure for information systems to ensure that supporting utilities are provided for to limit unplanned disruptions. Protect information systems against environmental hazards and provide appropriate environmental controls in facilities containing information systems.

2.11. Personnel Security

Ensure that individuals responsible for agency information are identified and their responsibilities are clearly defined. Any individuals occupying positions of responsibility within the Board (including third-party service providers) are trustworthy and meet established security criteria for those positions, verified through a criminal history background check. Ensuring that information resources are protected during and after personnel actions such as terminations and transfers. Employ formal sanctions for personnel failing to comply with security policies and procedures.

2.12. Third-Party Personnel Security

Require all third-party providers to comply with all security policies and standards. Establish personnel security requirements including roles and responsibilities with limits on access requirements defined in accordance to least privileged and data minimization methodologies. Monitor providers for compliance.

2.13. System Configuration Hardening and Patch Management

2.13.1 System Configuration Hardening

The system hardening procedure shall include, but is not limited to:

- a. Operating systems may only be installed from Board IT approved sources.
- b. Vendor supplied patches shall be applied.
- c. Unnecessary software, system services and drivers shall be removed.

- d. Appropriate security parameters, field protections and audit-logging capabilities shall be set.
- e. Default account passwords shall be disabled or changed as appropriate.
- f. Vulnerability assessment will be run against the server before being placed into production.
- g. The information system must be configured to provide only essential capabilities and specifically prohibits and restricts the use of unnecessary functions, ports, protocols, or services.
- h. Security configurations must be set to the most restrictive mode consistent with information system operational requirements and according to the level of risk formally accepted by owners of the information systems.
- i. Password-locking screensavers shall be enabled and activated after no more than fifteen (15) minutes of inactivity.

2.13.2 Patch Management

Board IT staff must monitor information feeds for the release of new operating system and application patches and hot fixes that are pertinent to TWC information resources.

All patch releases will follow a defined process for patch deployment that includes assessing the risk, testing, scheduling, installing, and verifying, unless the need for an emergency deployment exists.

2.14 Access Control

The Board shall determine, assign, and secure the computer access codes required for a Board or subrecipient, contractor or subcontractor user or Agency staff member to perform assigned job duties, including changing/resetting user local passwords and administering RACF security adds/changes and deletes for Board, subrecipient, contractor and subcontractor users.

The Board shall require all persons to whom it grants access to Agency applications to execute a P-41 TWC Information Security Agreement, All Employees Form available at the following web address:

http://intra.twc.state.tx.us/intranet/gl/html/personnel_forms.html. The instructions for the P-41 Form are located at the same web address as P-41 INST Information Security Agreement, All Employees Instructions.

The Board shall maintain a signed copy of the most recent Agency Information Security Agreement for each user.

The Board shall determine which of its employees and subrecipients need Health and Human Services Commission (HHSC) computer access to perform assigned job duties. (NOTE: Request for HHSC computer access shall be routed to the TWIST Help Desk.)

2.15 Account Management

Account Management establishes the standards for the creation, monitoring, control, and removal of User accounts. The Account Management standard shall apply equally to all User accounts without regard to their status or category. User accounts are how access is granted to TWC information resources. Accounts are granted to Board staff determined to have a need. These accounts assist in establishing accountability for systems use and are a key component in the protection of data; its confidentiality and integrity.

- a. All accounts must be identifiable using a unique User ID.
- b. Accounts, other than service/maintenance accounts, must uniquely identify a specific User.
- c. Unsuccessful account access attempts must be monitored, and accounts locked after five (5) or less failed attempts within two (2) hours or as determined by a documented risk assessment.
- d. Written notice of removal of access authorization for any individual shall be submitted to the Agency immediately upon removal of that access.

2.15.1 User Verification

The Board shall implement and maintain a system for user verification to ensure that all user accounts are current.

- (1) The Board shall immediately revoke access to user accounts resulting from staff departures or contract, subcontract, or subgrant completions.
- (2) The Board Systems Administrators will conduct a quarterly review of Board account status to identify obsolete accounts.
 - a. For all accounts that are no longer in use, the Administrator shall notify the appropriate account management administrator to delete the account and notify the “Terminated Employees” shared distribution list to ensure that the appropriate Board accounts are deleted.
 - b. All accounts dormant for more than three (3) months will be flagged and disabled unless the Agency is notified to the contrary by the Board.
 - c. Accounts dormant for six (6) months or more will be deleted.

2.16 Security Systems Management

Design, implement, configure, administrate, maintain, monitor, and support security systems to enforce security policy and provide security services. These systems include firewalls, Intrusion Prevention Systems (IPS), Internet Proxy Servers, Security Information and Event Management (SIEM) systems, and other control enforcement or monitoring systems.

2.17 Network Access and Perimeter Controls

Network equipment such as servers, workstations, routers, switches, and printers should be installed in a manner that prevents unauthorized access while limiting services to only authorized users. A perimeter should be established to delineate internal systems and prevent unauthorized external parties from tampering, attempting access or connecting without approved remote access methods.

2.18 Internet Content Filtering

Implement a system or service to enforce controls to block access to Internet websites based upon categories of content, application types and granular application functions, time of day or amount of utilization, or the dynamically updated reputation of the destination. Web content filtering should be based on two goals:

Bandwidth Preservation – The Local Area Network (LAN) and Wide Area Network (WAN) resources within the Agency locations are limited and heavily utilized for conducting business.

Inappropriate Content – The Internet contains content that is inappropriate in nature and unacceptable for access in the workplace.

2.19 Data Loss Prevention

Implement a solution designed to detect and prevent potential data breach incidents where sensitive data may be disclosed to unauthorized personnel by malicious intent or inadvertent mistake. Detection of data at risk can be performed while in use at the endpoint, while in motion during transmission across the network, and while at rest on data storage devices.

2.20 Identification and Authentication

User chosen passwords must adhere to a minimum length and format as defined by current password guidelines:

- a. Contain at least one each upper- and lower-case letters, one non-alphanumeric and at least one number.
- b. Are at least eight characters in length.
- c. Passwords should not have consecutive duplicate characters such as 99 or BB.
- d. Passwords should not have consecutive-count numbers or letters such as 1234 or ABCD
- e. Passwords are not words in any dictionary including, slang, dialect, jargon, etc.
- f. Passwords are not based on personal information such as names, birthdates, etc.
- g. Passwords should be easily remembered.
- h. Passwords should never be the same as the User ID.

- i. All passwords must have an expiration period not to exceed 180 days or as defined by the most current password guidelines.
- j. Stored passwords must be encrypted.
- k. Passwords should not be re-used within the last 10 instances.

2.21 Spam Filtering

Implement a solution or service that filters and/or blocks any E-Mail item, inbound or outbound, which is determined to place the Board, its systems and/or networks at an unacceptable level of risk.

2.22 Portable and Remote Computing

Access to TWC systems utilizing remote portable computing devices must use a Virtual Private Network (VPN) connection.

2.23 System Communications Protection

Data Transfers Standard:

TWC utilizes and stores data that must be protected from interception and alteration. All data file transfers that involve TWC data shall be secured using an agency approved data transfer encryption method or file encryption method. Data made available for the public – including information posted on TWC publicly accessible websites or public file transfer protocol (FTP) servers is exempt from being encrypted. There are two methods of transferring electronic files. The electronic movement of data using a communication channel from one point to another, (transmission), and the physical movement of data from one point to another, (transport). There are two basic methods used to encrypt data in transmission. The data can be encrypted prior to transmission or transmission of the data over an encrypted communications channel. Data transport is accomplished by moving the media that holds the data. The data is encrypted on the media using a data at-rest method with a minimum of AES-256 algorithm.

Section 3. Detect

3.1 Vulnerability Assessment

Board must conduct periodic vulnerability assessments of their networks, applications, and other systems. Including but not limited to penetration testing to test and evaluate security controls and security defenses and to ensure that required security posture levels are met. Evaluate results of various penetration tests to provide risk-based prioritization of mitigation.

3.2 Malware Protection

The Agency shall maintain virus protection software on all systems and custom applications provided to the Board.

The Board is responsible for the use and installation of virus protection software on all systems and custom applications maintained by the Board.

Virus protection software implemented to include automatic updates that apply the most current and appropriate protection and patches for viruses or malicious code infection on all network servers that provide virus scanning services to network attached workstations. It shall also provide automatic scanning of all files stored on or attached to workstations or servers. It shall also provide automatic scanning of files accessed or copied onto a storage device from external sources, such as, but not limited to, the Internet (cloud service providers) and media such as CD-ROMs, flash drives, and floppy disks.

3.3 Security Monitoring and Event Analysis

Analyze security events and alerts generated from the Board's environment and be able to:

- a. Collect the security-related information required for assessments, metrics, and reporting.
- b. Analyze the data collected and report findings to Board management.
- c. Assess the effectiveness of security controls.
- d. Respond using technical, administrative, and operational mitigating activities.

Section 4. Respond

4.1 Cybersecurity Incident Response

The Board must develop a Cybersecurity Incident Response Plan. The plan must include adequate preparation, detection, analysis, containment, recovery, and response activities.

The Board is responsible for notifying and escalating incidents to appropriate personnel and coordinating activities to ensure timely isolation and containment, impact analysis, and any resulting remediation / resolution requirements.

4.2 Privacy Incident Response

The Board must develop a Privacy Incident Response Plan. The plan must include adequate preparation, detection, analysis, containment, recovery, and response activities.

The Board is responsible for notifying and escalating incidents to appropriate personnel and coordinating activities to ensure timely isolation and containment, impact analysis, and any resulting remediation / resolution requirements.

- a. Initial notification shall be made via email to IncidentReports.RSM@twc.state.tx.us.
- b. The Board shall comply with Agency directives in resolving any incidents.

Section 5. Recover

5.1 Disaster Recovery Procedures

Develop and maintain a Disaster Recovery Plan for all IT resources in the Board environment. The plan should cover all relevant platforms – personal computers, local area networks, workstations, and midrange systems, as appropriate. Disaster recovery activities should include data backup, local area network recovery testing, and contingency planning functions for all local data.

EXHIBIT 3 - Security Management and Texas Cybersecurity Framework

Contractor Onboarding Requirements

Finalist and Successor upon receipt of award are required to answer an online vendor onboarding questionnaire to establish an initial risk rating and score. Once the questionnaire has been completed the contractor will receive a follow-up email including a portal link to upload evidence of compliance for each control. TCF Documentation Requirements Table included in this EXHIBIT 3 provides you with a description of each control along with an example of the type of appropriate evidence required to satisfy the control.

All bidders should include a response to the following questions:

- a) How is your data protected?
- b) How is data classification is applied?
- c) What safeguards are in place to protect you data?
- d) How is data backed-up?
- e) What guidelines do you follow for back-ups?
- f) How often are back-ups tested?
- g) What is RTO and RPO for major systems i.e., financials? Along with what other systems that are critical to deliver services including third party vendors such as PEOs.
- h) What security controls do you have in place to protect from ransomware attacks?
- i) Do you conduct annual Cyber Security Training?
- j) Do you carry Cyber Security Insurance?
- k) What is your Cyber Security Insurance coverage and limits?
- l) Does your Cyber Insurance coverage include corporate and board co-located employee errors?
- m) Can you provide a Certificate of Insurance verifying your Cyber Insurance coverage and limits?
- n) What is your breach notification policy?

TCF Documentation Requirements

Item #	Associated Control(s)	Documentation Requirement
TCF #1	<u>Privacy & Confidentiality</u> Pertains to documentation for protecting privacy and confidentiality of data, such as personally identifiable information of its customer, records, PI,I etc.	1. Privacy policy on public websites 2. Privacy Notice policy on public websites 3. Privacy Internal Use policy on public websites 4. Non-Disclosure Agreements (NDAs) 5. Memorandum of Understanding Agreements (MOUs) 4. Other Privacy documents
TCF #2	<u>Data Classification</u> Pertains to documentation for classifying/labeling data, data inventory, and identifying data owners for maintaining critical data.	1. Data Categorization Documentation/Policy 2. Critical Data Inventory 3. List of data owners
TCF #3	<u>Critical Information Asset Inventory</u> Pertains to documentation for identifying critical IT Assets such as hardware, software, and data.	1. See TCF #2 Documents 2. IT Asset Inventory (Cover Page and 1st Page of IT Inventory)

Item #	Associated Control(s)	Documentation Requirement
TCF #4	<u>Enterprise Security Policy, Standards, and Guidelines</u> Pertains to documentation for organization Information Security Policies and Procedures that define acceptable use policies for the organization's information resources.	1. Information Security Policies and Procedures
TCF #5	<u>Control Oversight and Safeguard Assurance</u> Pertains to documentation for cataloging the organization's information security activities.	1. See TCF #4 Documents 2. Information Security Plan
TCF #6	<u>Information Security Risk Management</u> Pertains to documentation for the assessment and evaluation of information security risk	1. Risk Management Strategy, Policies, and Procedures 2. Risk Assessment for Critical Applications 3. Risk Registry
TCF #7	<u>Security Oversight & Governance</u> Pertains to documentation for IT Security oversight and Governance.	1. See TCF #5 & #6 Documents 2. Information Security Charter 3. Evidence that Leadership Meets on IT Security Issues: Meeting Emails/Meeting Agendas/ IT Security Annual Reports
TCF #8	<u>Security Compliance and Regulatory Requirements Management</u> Pertains to documentation for monitoring legislative and industry landscape to ensure IT Security Policy is updated based on applicability to the organization.	1. See TCF #5, #6, & #7 Documents
TCF #9	<u>Cloud Usage and Security</u> Pertains to documentation for assessing and evaluating cloud technology risk such as: Software as a Service (SAAS), Platform as a Service (PAAS), and Information as a Service (IAAS).	1. Cloud security objectives - Documentation or notation of security risks if cloud services are used 2. SOC-1 and or SOC-2 Review of Cloud Service Providers
TCF #10	<u>Security Assessment and Authorization / Technology Risk Assessment</u> Pertains to documentation for assessing security controls to ensure that security threats are mitigated within acceptable risk tolerances.	1. Security Assessment and Authorization Policy and Procedures 2. Latest Independent Security Assessment
TCF #11	<u>External Vendors & Third Party Providers</u> Pertains to documentation for evaluation of third-party and external vendor security.	1. System and Services Acquisition Policy and Procedures 2. Vendor Access Policy 3. Agreements or Memorandums, ISA, MOU (Sample Contract Template) 4. Vendor Risk assessments
TCF #12	<u>Secure Application Development</u> Pertains to documentation for coding and application development security.	1. See TCF #17, 21, & 22 Documents
TCF #13	<u>Beta Testing</u> Pertains to documentation for testing projects and systems for security prior to implementing projects and systems into production environment.	1. See TCF #17, 21, & 22 Documents

Item #	Associated Control(s)	Documentation Requirement
TCF #14	<u>Penetration Testing</u> Pertains to documentation for testing the strengths and weaknesses of the organization's information system security based on a simulated attack.	1. Penetration Testing reports
TCF #15	<u>Vulnerability Testing</u> Pertains to documentation for scanning an information system for vulnerabilities.	1. Vulnerability Scanning Policies 2. Vulnerability Scanning reports
TCF #16	<u>Enterprise Architecture, Roadmap & Emerging Technology</u> Pertains to documentation for information security architecture.	1. Current Network Diagram
TCF #17	<u>Secure System Services, Acquisition, and Development</u> Pertains to documentation for Security related to the systems development/acquisition life cycle (SDLC).	1. Evidence of security roles incorporated into the SDLC process (Contract Template/Procedure) 2. Code Development Tool Dashboard Screenshot 3. Project Management Tool Dashboard Screenshot 4. SDLC Policies and Procedures
TCF #18	<u>Security Awareness & Training</u> Pertains to documentation for Security & Privacy Awareness Training.	1. Security & Privacy Awareness Training Policies and Procedures 2. Security & Privacy Awareness Training Tool Dashboard Screenshot 3. Security & Privacy Awareness Training New Hire Curriculum 4. Security & Privacy Awareness Training Metrics
TCF #19	<u>Privacy Awareness & Training</u> See TCF #18 Documents.	1. See TCF #18 Documents
TCF #20	<u>Cryptography</u> Pertains to documentation for data encryption.	1. Evidence of Cryptographic Server Key Management (if applicable) 2. Evidence that sensitive data is encrypted 3. Evidence of Encryption of data at rest - Methods or Processes
TCF #21	<u>Secure Configuration Management</u> Pertains to documentation for ensuring that baseline configurations and inventories of information systems (including hardware, software, firmware, and documentation) are established and maintained.	1. Configuration Management Policy and Procedures 2. Windows default domain policy (Account policies, Password Policies, account lockout policy) 3. Screenshot of Configuration Management Tool
TCF #22	<u>Change Management</u> Pertains to documentation for managing changes to the organization's information system.	1. See TCF #21 Documents 2. Patch Management Policies & Procedures 3. Sample change ticket
TCF #23	<u>Contingency Planning</u> Pertains to documentation for emergency response, backup operations, and recovery for the organization's information system.	1. Contingency Plan to include approval and update pages 2. Contingency Plan testing planning and the test results from the most recent test 3. Information System Backup Policy and Procedures 4. Evidence of System Backups - configuration file/encryption used/process used for storage and management of media or files

Item #	Associated Control(s)	Documentation Requirement
TCF #24	<u>Media (handling and data sanitization)</u> Pertains to documentation for the protection of digital/electronic and non-digital/paper information system media.	1. Media Protection Policy and Procedures 2. Data Loss Prevention Tool Dashboard Screenshot 3. List of authorized personnel with access to restricted areas 4. Media Sanitization and disposal Records
TCF #25	<u>Physical and Environmental Protection</u> Pertains to documentation for the physical access to and physical protection of the organization's information system.	1. Physical and environmental Protection Policy and Procedures 2. List of personnel with authorized access to facilities containing information systems (system software, network, application and database) 3. Access monitoring tools (e.g., badge readers, security alarms, video cameras) 4. Evidence that physical access logs are reviewed 5. Evidence of Data Center Emergency Lighting and power policies, procedures and testing (If Applicable) 6. Evidence of Fire Suppression and Detection System policies, procedures and testing (If Applicable) 7. Evidence of Data Center temperature and humidity monitoring policies, procedures and testing (If Applicable) 8. Evidence of Data Center water damage and detection policies, procedures and testing (If Applicable)
TCF #26	<u>Personnel Security</u> Pertains to documentation for ensuring that security is considered for individuals (employees) who have access to the organization's information systems.	1. Personnel security policies and procedures 2. Sample of completed employee and vendor Background Check (Redact PII) 3. See TCF #11 & #29 Documents
TCF #27	<u>Third-Party Personnel Security</u> Pertains to documentation for ensuring that security is considered for third parties, contractors, and vendors who have access to the organization's information systems.	1. Personnel security policies and procedures 2. Sample of completed vendor Background Check (Redact PII) 3. See TCF #11 & #29 Documents
TCF #28	<u>System Configuration Hardening & Patch Management</u> Pertains to documentation for security patching of the organization's information systems.	1. See TCF #22 Documents
TCF #29	<u>Access Control</u> Pertains to documentation for processes used to ensure access to applications, servers, databases, and network devices in the environment is limited to authorized personnel.	1. Access Control Policy and Procedures 2. Windows GPO Setting Screenshots - Windows Security Policy or GPO for users accounts screenshot - ensure that password configurations, inactive login disabled date, and unsuccessful logins are enabled. 3. Sample Employee <u>Access provisioning</u> evidence (Ticket or Email)... Redact PII 4. Sample Employee <u>Access termination</u> evidence (Ticket or Email), Redact PII 5. Evidence of last User Access Review
TCF #30	<u>Account Management</u> Pertains to documentation for processes used to establish the standards for the creation, monitoring, control, and removal of accounts which are used to access the organization's information systems	1. See TCF #29 Documents

Item #	Associated Control(s)	Documentation Requirement
TCF #31	<u>Security Systems Management</u> Pertains to documentation for administration, maintenance, monitoring, and ongoing support of IT security systems. Systems include firewalls, Intrusion Prevention Systems (IPS), Internet Proxy Servers, Security Information and Event Management (SIEM) systems, and other control enforcement or monitoring systems.	1. TCF #7 Documents 2. SIEM Tool Dashboard Screenshot 3. Firewall Tool Dashboard Screenshot 4. Data Loss Prevention Tool Dashboard Screenshot 5. Vulnerability Scanning Tool Screenshot 6. Spam Protection Tool Dashboard Screenshot 7. Malware Protection Tool Dashboard Screenshot
TCF #32	<u>Network Access & Perimeter Controls</u> Pertains to documentation for network access and perimeter controls. Note: TWC Agency Boards are responsible for LAN.	1. See TCF #29 & #37 Documents
TCF #33	<u>Internet Content Filtering</u> Pertains to documentation for controls used to block access to Internet websites based upon specified criteria in order to protect the organization's information system from cyber threats. Note: TWC Agency Boards responsible for LAN	1. See TCF #29 & #37 Documents 2. Firewall Tool Dashboard Screenshot
TCF #34	<u>Data Loss Prevention</u> Pertains to documentation for technology designed to detect and prevent potential data breach incidents where sensitive may be disclosed to unauthorized personnel.	1. Data Loss Prevention Tool Dashboard Screenshot
TCF #35	<u>Identification and Authentication</u> Pertains to documentation for the verification of the claimed identity of users, processes, or devices as a prerequisite to permitting access.	1. Identification and Authentication Policy and Procedures 2. Evidence of multi-factor authentication 3. See TCF #29 Documents
TCF #36	<u>Spam Filtering</u> Pertains to documentation for spam protection mechanisms employed at information system entry and exit points. Also includes spam protection solutions used (e.g. McAfee Email Gateway).	1. Spam protection tool Dashboard Screenshot
TCF #37	<u>Portable & Remote Computing</u> Pertains to documentation for remote access to the organization's information systems.	1. Remote Access Policy and procedure and or VPN access procedure
TCF #38	<u>System Communications Protection</u> Pertains to documentation for controlling, monitoring, managing and protecting transmissions between information systems.	1. See TCF #20 & #31 Documents 2. System and Communications Protection Policy and Procedures 3. Example of information system security alerts, advisories, and directives received from internal and external sources

Item #	Associated Control(s)	Documentation Requirement
TCF #39	<u>Information Systems Currency</u> Pertains to documentation for the organization's planning for future information systems development and operations.	1. See TCF #17 Documents 2. Information System Modernization Strategy & Roadmap
TCF #40	<u>Vulnerability Assessment</u> Pertains to documentation for identifying and remediating security vulnerabilities in the organization's information systems.	1. See TCF #14, #15 & #22 Documents 2. Vulnerability Remediation Policy and Procedures
TCF #41	<u>Audit Logging and Accountability</u> Pertains to documentation for maintain the organization's information systems logs/records for investigatory and accountability purposes.	1. Policies and Procedures related to auditing, to include the following: <ul style="list-style-type: none"> a. Types of events audited b. Security incidents audited c. Evidence of Audit Log Review by appropriate personnel 2. List of Audit Logs captured from information systems 3. Security Monitoring Reports - Events that are monitored and managed as part of the event analysis process
TCF #42	<u>Malware Protection</u> Pertains to documentation for the prevention, detection and cleanup of Malicious Code (including virus, worm, Trojan, Spyware and other similar variants).	1. See TCF #31 Documents 2. Evidence of Malicious code protection mechanisms such as antivirus evidence automatic scanning
TCF #43	<u>Security Monitoring and Event Analysis</u> Pertains to documentation for the analysis of security events and alerts.	1. See TCF #31, #38 & #41 Documents
TCF #44	<u>Cybersecurity Incident Response</u> Pertains to documentation for Incident Response tracking, documenting, and reporting <u>Cybersecurity incidents</u> to appropriate officials and/or authorities.	1. Incident Response Policy and Procedures 2. Incident Response Plan 3. For a sample of one logical security incident that occurred during the period of review, evidence supporting the IRP process: <ul style="list-style-type: none"> a. Notifications or communication received describing the security incident b. Description of the actions taken to resolve the security incident
TCF #45	<u>Privacy Incident Response</u> Pertains to documentation for Incident Response tracking, documenting, and reporting <u>Privacy incidents</u> to appropriate officials and/or authorities.	1. See TCF #44 Documents
TCF #46	<u>Disaster Recovery Procedures</u> Pertains to documentation for managing the recovery of data and applications in the event of loss or damage.	

Security Management

WFS Capital Area adheres to the Texas Cyber Security Framework as mandated by TWC. As such all WFS contractors must adhere to the same framework and maintain a minimum level 3 cyber security maturity and agree to annual security assessments.

- The Contractor shall take appropriate actions to assure compliance with 1 TAC, Chapter 202, the Texas Cybersecurity Framework (TCF) at <https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Texas%20Cybersecurity%20Framework%20Controls%20and%20Definitions.pdf> and all other state or federal rules, regulations, and laws as applicable to Contractor programs. The Contractor shall:
 - Implement Information Security Management (ISM) compliance policies and procedures for Contractor staff and Contractor subrecipient, contractor and subcontractor staff (hereinafter referred to as “Contractor staff” for the purposes of this section); and
 - Assure and be responsible for Contractor staff compliance with such ISM requirements.
- Contractor staff shall follow all Agency security guidance when making use of Agency information resources, Agency-provided data, and/or Agency-administered systems including but not limited to Exhibit I- Safeguards for TWC Information and Exhibit J-Contractor Security Guidelines
- The Contractor shall in the event of a security violation, if a breach is detected, or if the Contractor has any reason to suspect that the security or integrity of the Agency’s data has been, or may be, compromised in any way:
 - Notify the Agency’s Chief Information Officer immediately and no later than twenty-four (24) hours via email to angelica.benavides@wfscapitalarea.com ; and
 - The time period for notifying WFS under this section is reduced to one (1) hour for suspected security violations that involve protected health information of a covered under 45 C.F.R. Parts 160, 162, and 164, such as Medicaid Information provided from, by or accessed through the Health and Human Services Commission systems as required by the Health Information and Portability and Accountability Act (HIPAA) and the Health Information Technology Act (HITECH).
- Comply with the notification requirements of Section 521.053, Business & Commerce Code, to the same extent as a person who conducts business in this state; and
- Comply with Agency directives in resolving any incidents.
- The Contractor shall designate an information security officer who:
 - reports to the Contractor’s executive-level management;
 - has authority over information security for the Contractor;
 - possesses the training and experience required to perform these duties; and
 - to the extent feasible, has information security duties as their primary duties.

Texas Cybersecurity Framework

The Texas Cybersecurity Framework (TCF) consists of forty-six(46) Control Objectives and five(5) Functional Areas as follows; Identify, Protect, Detect, Respond and Recover. TCF is also based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

- The Contractor security program will undergo a TCF assessment at least once every two years to evaluate the programs overall maturity, measured on the CMMI scale (0-5) and the maturity level of each of the TCF controls. This assessment will be conducted by a third-party assessor contracted by the Agency.
 - Control objectives below a CMMI level 3 will require submission of a management response with corrective action plan to the Agency.
 - Corrective Action Plan status reports will be made every six months, starting from the plan submission date.

Cyber Security Maturity Levels

Level 0:	Non-Existent - There is no evidence of the organization meeting the objective.
Level 1:	Initial - The organization has an ad-hoc, inconsistent, or reactive approach to meeting the objective.
Level 2:	Consistent - The organization has a consistent overall approach to meeting the objective, but the approach is mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.
*Level 3:	<u>Defined - The organization has a documented, detailed approach to meeting the objective and regularly measures its compliance.</u>
Level 4:	Risk-Based - The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.
Level 5:	Optimized - The organization has refined its standards and practices, focusing on ways to improve its capabilities in the most efficient and cost-effective manner.