

INTERAGENCY CONTRACT FOR REMOTE CHECK DEPOSIT PROGRAM SERVICES

This Interagency Cooperation Contract for Remote Check Deposit Program Services is entered into between the Texas Comptroller of Public Accounts ("Comptroller") and Texas Juvenile Justice Department, an agency of the State of Texas ("Contracting Agency"). Comptroller and Contracting Agency may alternatively be referred to as "Parties".

Part 1. Program Overview.

Comptroller operates the Remote Check Deposit Program ("Program"), which allows local offices of Texas state agencies to scan payments made by checks and electronically transmit the captured images of those checks to Comptroller, eliminating the need to physically transport the checks to Comptroller offices in Austin, Texas. The goals of the Program are to safely and efficiently reduce the costs associated with the remittances into the State treasury, and to increase interest income for the State.

Part 2. Duties and Responsibilities.

Section 2.01. Implementation Procedures.

1. Location Information. Contracting Agency will provide the name and address of each office location that collects checks for deposit under the Program.
2. Scanning Equipment. Comptroller will provide Contracting Agency with a desktop scanner for each office location collecting checks.
 - a) Each desktop scanner provided by Comptroller to Contracting Agency shall be the property of Contracting Agency, and shall include a one-year warranty to begin on the date of purchase by Comptroller. After expiration of the warranty, Contracting Agency shall be responsible for the proper maintenance, care and replacement of all desktop scanners provided under this Contract. Disposition of scanners shall be handled in accordance with state law. After expiration of the warranty, cost for all replacement scanners, repairs, and subsequent warranties shall be the sole responsibility of Contracting Agency. All replacement scanners must be pre-approved by Comptroller. Replacement scanners shall not store residual data (i.e., check images) and shall be configured to wipe the data upon scan completion.
 - b) Scanner failure or malfunction. Contracting Agency shall be responsible for resolving scanner failures or malfunctions as quickly as is reasonably practicable. During any period in which Contracting Agency does not have an operable scanner, Contracting Agency may engage in an alternate process (e.g. checks scanned at another Contracting Agency location, checks physically sent either to Contracting Agency's main office or to Comptroller for deposit) until scanner service is restored.
 - c) Contracting Agency will provide a dedicated, hardened, single-purpose computer (including any necessary peripherals) to be utilized in conjunction with each scanner. Contracting Agency will include the single-purpose computer(s) in Contracting Agency's normal desktop support. Contracting Agency will prohibit Internet browsing and email on the single-purpose computer(s), as the computer will be used solely with the Program. The recommended minimum hardware requirements for the computer are as follows:
 - i. Pentium 4 2.0 GHz or Core 2Duo 1.86 GHz Processor;

- ii. 512MB RAM;
- iii. 1024x768 video resolution;
- iv. 40GB Hard Drive;
- v. Network Card;
- vi. Broadband Internet Access; and
- vii. USB 2.0 (the final specifications for the USB will depend on the specific scanner requirements).

The recommended minimum technical controls for the single-purpose computer are as follows:

- viii. Operating System.
 - a. Actively supported by operating system vendor;
 - b. Patched with latest versions and/or security updates available from the vendor;
 - c. Hardened according to CIS Benchmarks Level 1 and Level 2;
 - d. Configured to run enterprise managed and vendor supported firewall and host intrusion prevention software (e.g., Microsoft Windows Firewall and EMET or McAfee Firewall and MalwareBytes Anti-Exploit Kit);
 - e. Limited number of users with administrative privileges (e.g. operators scanning checks do not have administrative level access).
- ix. Software Installation.
 - a. Limited to agents that provide enterprise supportability (e.g. SCCM, DLP, Anti-Malware) and components required by the scanner (e.g. drivers, .Net framework, Java);
 - b. Patched with latest versions and/or security updates available from the respective vendors.
 - c. Excludes Microsoft Office, Microsoft Silverlight, Adobe products (e.g. Flash, Reader), and Email clients.
 - d. **Please note** .NET Framework 4.8 is a prerequisite to download/install the Remote Check Deposit software and each upgrade may add the next version of .NET Framework.
- x. Web Browser.
 - a. Actively supported by web browser vendor;
 - b. Managed via enterprise support (e.g. security settings);
 - c. Configured to disable all scripts except those required for check scanning;
 - d. Patched with the latest versions and/or security updates available from the vendor.
- xi. Anti-Malware Tool.
 - a. Installed and running;
 - b. Actively supported by the tool vendor;
 - c. Patched with the latest versions and/or security updates available from the vendor;
 - d. Configured to perform scheduled full disk scans daily;
 - e. Configured to perform on-read and on-write file/disk access scan of all files;
 - f. Does not exclude any location nor file types from on-access scanning.
- xii. Internet Connectivity.
 - a. Allows access from the internal Contracting Agency network only;
 - b. Limited to Comptroller's remote check deposit software;
 - c. Restricted at the Contracting Agency's network perimeter;

- d. Restricted at single-purpose computer level (e.g. via OS configuration tools, such as computer firewall managed through GPO).
 - xiii. Operating System Firewall.
 - a. Enabled and kept up-to-date;
 - b. Restricted to traffic needed for enterprise support (e.g. apply GPO, obtain patches) and communication with the Comptroller's remote check deposit software.
 - xiv. Software Whitelisting (Native Microsoft Windows software restriction is an acceptable minimum).
 - a. Includes components required to run scanner and enterprise support tools (e.g. SCCM, Anti-Malware);
 - b. Centrally managed (e.g. GPO).
- 3. Installation. Comptroller will provide Contracting Agency staff with instructions on how to set up and install the desktop scanners and the Comptroller's remote check deposit software.
- 4. Training. Comptroller will provide training to appropriate Contracting Agency staff on how to operate the desktop scanner and other relevant aspects of the Program. The training may be onsite or in the format of a teleconference or webinar at Comptroller's discretion.
- 5. Testing. Comptroller and Contracting Agency will ensure that successful testing is accomplished before Contracting Agency begins using the Program.
- 6. Warranty. Comptroller will facilitate initial contact with Comptroller's vendor for any communications regarding the warranty. Any subsequent scanners and warranties will be the responsibility of Contracting Agency.
- 7. Connectivity. Comptroller whitelists the IP range for each state agency and/or state agency field office. In the event Contracting Agency makes network changes that alter the IP range, Contracting Agency will coordinate with Comptroller to prevent disruption of services.
- 8. Access. Comptroller will setup Contracting Agency staff on Okta to access the Comptroller's remote check deposit software. Okta is the foundation for secure connections between users and technology. Contracting Agency staff will use the Okta Verify application on personal devices, SMS (Text Messages) and Voice Call Authentication factors for Multifactor Authentication.

Section 2.02. Remote Deposit Processing Procedures.

1. Scanning of Checks. The scanner must adequately capture the front and the back images of each check. Comptroller will provide an initial scanner with endorsement capabilities, and the sequence information will be sprayed by the scanner's ink cartridge as the check passes through the scanner.
2. Receipt of Check Images from Contracting Agency. Contracting Agency will upload encrypted check images to Comptroller through a secure Internet connection as defined by Section 2.01.2.c) in accordance with security requirement of this Contract. The check images must be received by Comptroller no later than 2:00 p.m. Central Time ("CT") to be processed on the business day it is received. Check images received by Comptroller after 2:00 p.m. CT will be processed on the next business day.
3. Upload Deposit into USAS. For field offices, each day following receipt of the check images, Comptroller will upload the deposits reported into the Uniform Statewide Accounting System ("USAS"), crediting the appropriate Transaction code, Fund, Agency, PCA, and Object Code.

Comptroller will generate a deposit notice and forward it to the designated personnel at Contracting Agency via secured encrypted email transmission. For other deposits, the document number, amount, and agency number will be transmitted to USAS for validation and posting.

4. Check Retention. Contracting Agency shall be responsible for the safekeeping and destruction of the original checks that are uploaded in accordance with applicable banking industry standards for original check chain of custody, retention, and destruction.
 - a) Safekeeping. Contracting Agency will store the original checks for a reasonable amount of time in a secure and controlled manner. Contracting Agency shall ensure that checks are not re-submitted to Comptroller for processing. The suggested retention timeframe is two weeks for Comptroller's purposes; however, Contracting Agency shall be responsible for complying with any applicable records retention schedule.
 - b) Destruction. Subject to any applicable records retention requirements, the original checks may be destroyed after the retention period has expired. Contracting Agency must destroy the original checks in a secure and controlled manner.

Section 2.03. Returned Items.

1. Returned Checks. Upon receipt of returned checks, Comptroller will charge the return amount to the USAS return item default codes and forward the return item and notice to Contracting Agency in accordance with existing return check processes.
2. Non-Conforming Images. Check images may be rejected by Comptroller's bank for various reasons. In the event that a non-conforming image notice is received, Comptroller will generate a returned item transaction. Comptroller will charge the amount to the USAS return item default codes and forward the notice and a copy of the item to Contracting Agency. Upon receipt, Contracting Agency will be responsible for rescanning and depositing the item in a new deposit or obtaining the paper item to deposit at Comptroller.

Section 2.04. Exceptions.

1. Foreign Items. Contracting Agency acknowledges foreign items, which are checks not drawn on U.S. banks, will not be accepted in the Program. In the event that Comptroller receives a foreign item from Contracting Agency, Comptroller will charge the amount to the USAS return item default codes and forward the copy of the item to Contracting Agency.
2. Currency. Contracting Agency acknowledges currency is not accepted in the Program.
3. Check Rejects. Check images may be rejected during the scanning process for various reasons. Contracting Agency will be responsible for instructing the applicable Contracting Agency locations on how to handle checks that cannot be scanned and processed under the Program.

Section 2.05. Sensitive Personal Information and Security Requirements.

1. Sensitive Personal Information. Sensitive Personal Information refers to information such as individual names, account numbers, social security numbers, driver's license numbers, dates of birth, or other personal information that may be contained in the check image files provided by Contracting Agency or accessed via Comptroller systems under this Contract.
2. Transmittal, Storage, and Encryption. Comptroller and Contracting Agency will establish a secure

and encrypted method of transmission for Sensitive Personal Information exchanged under this Contract. Transmission of Sensitive Personal Information across public networks shall be protected by encryption methods such as Virtual Private Network (VPN), Secure Shell File Transfer Protocol (SFTPS), or File Transfer Protocol over SSL/TLS (FTPS). Comptroller and Contracting Agency shall mutually ensure that a secure connection is established prior to Contracting Agency making any Sensitive Personal Information available to Comptroller. The Parties shall perform a test by Contracting Agency using a secure User ID and password to send a test file to Comptroller to ensure compliance with this paragraph. The Parties shall maintain their respective systems sufficient to allow an audit of compliance with the requirements of this Contract.

3. Access to Comptroller Systems. Comptroller will provide designated Contracting Agency employees with access to Comptroller's Okta and the remote check deposit software as necessary for the Contracting Agency's participation in the Program. Contracting Agency shall ensure that (1) only Contracting Agency employees who need access for the limited purpose of participating in the Program will have access to Comptroller's Okta and the remote check deposit software; and (2) Contracting Agency employees will only use the information obtained from Comptroller's remote check deposit software for purposes authorized by law and consistent with this Contract.

Comptroller and Contracting Agency will establish procedures to add or remove Contracting Agency employees designated to have access to Comptroller's Okta and the remote check deposit software. Contracting Agency must notify Comptroller promptly upon any personnel change, such as a termination or reassignment of duties, which make Contracting Agency employee's access to Comptroller's Okta and the remote check deposit software inconsistent with the terms of the Contract.

Contracting Agency must ensure that its employees with access to Comptroller's remote check deposit software have a completed Comptroller's Confidential Treatment of Information Acknowledgement (CTIA) form prior to granting access to Comptroller's remote check deposit software. Contracting Agency must keep copies of the CTIA forms on file for five years after the user's termination date. Upon written request, Contracting Agency will provide Comptroller with copies of the completed CTIA forms demonstrating compliance with this clause.

4. Compliance with Laws. All transfers of Sensitive Personal Information between the Parties shall conform to and each Party shall maintain Sensitive Personal Information in accordance with this Contract and any applicable state and federal laws and regulations: (1) regarding data confidentiality, privacy, and security, and (2) governing negotiable instruments. Each Party shall maintain its own information systems and resources to include System Configuration Hardening, Patch Management, and System Communications Protection in accordance with Title I, Part 10, Chapter 202 of the Texas Administrative Code.

Section 2.06. Customer Service.

Comptroller will provide phone numbers for Contracting Agency to use in the event that the scanner fails to operate or Contracting Agency has issues with check image file transmission.

Section 2.07. Compliance with Comptroller's Third-Party Software License Agreement.

Contracting Agency acknowledges that Comptroller uses certain third-party software ("Software") to provide services for the Program. Contracting Agency agrees it will not:

1. reverse engineer the Software; or
2. sell rights to the Software; or
3. otherwise violate the terms of the Software license.

Comptroller will provide a copy of any applicable Software license agreement to Contracting Agency, upon written request.

Part 3. General Provisions.

Section 3.01. Costs.

Any costs and expenses incurred under the terms of this Contract will be paid by the party incurring the cost or expense. No funds appropriated to either agency shall be exchanged under this Contract.

Section 3.02. Legal Authority for the Contract.

This Contract is entered into pursuant to the authority granted in Chapters 403, 404, and 771 of the Texas Government Code.

Section 3.03. Confidentiality, Texas Public Information Act, Security Incident Notifications

The “Disclosing Party” refers to the Party disclosing information and “Receiving Party” refers to the Party receiving information.

The Receiving Party shall limit access to Sensitive Personal Information contained in the check image files provided by Contracting Agency to authorized personnel with a need to know. Comptroller’s Authorized Personnel are employees, agents, contractors, or other entities designated by Comptroller to access Sensitive Personal Information for purposes authorized by law and consistent with this Contract.

Without limitation on the foregoing, Contracting Agency acknowledges that Comptroller’s disclosure of Sensitive Personal Information contained in the check image files provided by Contracting Agency to the following entities in the course of performing its statutory or contractual duties is permitted under this Contract:

- (a) Texas Attorney General’s Office;
- (b) Texas State Auditor’s Office; and
- (c) Banks or other financial institutions.

Each Party is responsible for complying with the applicable provisions of Chapter 552, Texas Government Code (“Texas Public Information Act”) and the applicable Attorney General Opinions issued under that statute. Responses to requests for Sensitive Personal Information contained in the check image files provided by Contracting Agency shall be handled in accordance with the provisions of the Texas Public Information Act.

Each Party shall provide notice to the other as soon as possible following the discovery or reasonable belief that there has been unauthorized use, exposure, access, disclosure, compromise, modification, or loss of Sensitive Personal Information or confidential information under this Contract (“Security Incident”). Comptroller and Contracting Party will exchange confidential, detailed security and Security Incident information only between the Information Security Officers (“ISOs”) of Comptroller and Contracting Party subject to the ISO’s mutually agreed restrictions or allowances regarding further internal or external dissemination of such Security Incident information within or outside each agency. Security Incident information may include the following as agreed by the ISOs:

- Date and time incident occurred,
- Date and time incident detected,
- Date and time incident contained,

- Address where incident occurred,
- Description of how Party discovered incident,
- Type of information involved,
- Description of the nature of the incident,
- Description of the steps Party has taken or will take to investigate incident,
- Description of the steps Party has taken or will take to mitigate any negative impacts of incident,
- Information technology involved (e.g., laptop, server, mainframe).

Comptroller and Contracting Party may also disclose confidential, detailed security and Security Incident information to law enforcement authorities as required. To the extent such security and Security Incident information is confidential pursuant to Sections 2054.077, 2059.055, and 552.139, Texas Government Code, or other applicable state or federal law, each Party shall comply with all applicable statutory requirements and restrictions regarding dissemination of such information.

If any Sensitive Personal Information is released as a result of a Security Incident and such release falls within Section 2054.1125 of the Texas Government Code, the Disclosing Party will provide any statutorily-required notice and bear all associated costs.

If communications between the Parties, or between a Party and its authorized representative(s), necessitate the release of Sensitive Personal Information obtained under this Contract, Comptroller's Confidential Treatment of Information Acknowledgement (CTIA) form must be signed by each individual who will require access to or may be exposed to that information.

Section 3.04. Term of the Contract.

This Contract is effective upon the date of Comptroller's signature and will expire on August 31, 2026, unless sooner terminated as provided herein. This Contract is binding on the successors in office or function of Comptroller and Contracting Agency.

Section 3.05. Termination of the Contract.

1. Either Party may terminate this Contract immediately and without notice to the other Party (1) in the event of a Security Incident, as defined in Section 3.3; or (2) for cause if the other Party breaches a condition of the Contract. This Contract is subject to termination for convenience upon thirty (30) days written notice by either party to the other. Neither Party to this Contract shall have any liability to any other party, person, agency or entity upon termination of this Contract for any reason, whether for cause or for convenience.
2. This Contract is contingent on the availability of sufficient funds. Both Parties are state agencies whose authority and appropriations are subject to actions of the Texas Legislature. If either Party becomes subject to a legislative change, revocation of statutory authority, or lack of appropriated funds which would render either Party's delivery or performance under the Contract impossible or unnecessary, the Contract will be terminated or cancelled and be deemed null and void. In the event of a termination or cancellation under this Section, neither Party will be liable to the other for any damages, which are caused or associated with such termination or cancellation. The Party terminating or cancelling under this Section shall not be required to provide advance notice.

Section 3.06. Amendments to the Contract.

Neither Comptroller nor Contracting Agency may amend this Contract unless the amendment is in writing and signed by both parties.

Section 3.07. Certifications.

- A. Right to Audit.** The Parties acknowledge the State Auditor's authority to conduct audits of state agencies under Chapter 321, Texas Government Code. Each Party shall have the right to conduct an on-site audit of procedures and security compliance processes relevant to information shared pursuant to this Contract, using procedures to be developed by the Parties.
- B. Dispute Resolution.** The Parties agree to use good-faith efforts to resolve all questions, difficulties, or disputes of any nature that may arise under or by this Contract; provided however, nothing in this paragraph shall preclude either Party from pursuing any remedies available under Texas law.
- C. Force Majeure.** Neither Party shall be liable to the other for any delay in, or failure of performance of, any requirement included in this Contract caused by force majeure. The existence of such causes of delay or failure shall extend the period of performance until after the causes of delay or failure have been removed provided the non-performing Party exercises all reasonable due diligence to perform. Force majeure is defined as acts of God, war, fires, explosions, hurricanes, floods, failure of transportation, or other causes that are beyond the reasonable control of either Party and that by exercise of due foresight such Party could not reasonably have been expected to avoid, and which, by the exercise of all reasonable due diligence, such Party is unable to overcome.
- D. No Waiver.** This Contract shall not constitute or be construed as a waiver of any of the privileges, rights, defenses, remedies, or immunities available to either Party as an agency of the State of Texas or otherwise available to the Party. The failure to enforce or any delay in the enforcement of any privileges, rights, defenses, remedies, or immunities available to a Party under this Contract or under applicable law shall not constitute a waiver of such privileges, rights, defenses, remedies, or immunities or be considered as a basis for estoppel. Neither Party waives any privileges, rights, defenses, or immunities available to it as an agency of the State of Texas, or otherwise available to it, by entering into this Contract or by its conduct prior to or subsequent to entering into this Contract.
- E. Severability.** If one or more provisions are deemed invalid, illegal, or unenforceable for any reason, such invalidity, illegality or unenforceability shall not affect any other provision and this Contract shall be construed as if the invalid, illegal or unenforceable provision had never been contained herein.
- F. Survival.** The expiration or termination of this Contract shall not affect the rights and obligations of the Parties accrued prior to the effective date of expiration or termination and such rights and obligations shall survive and remain enforceable.
- G. Governing Law; Venue.** This Contract is governed by and construed under and in accordance with the laws of the State of Texas. Any and all obligations under this Contract are due in Travis County and venue is proper only in such county.

Section 3.08. Notices.

- A.** A written notice required or authorized by this Contract shall be sent via electronic mail (email) and will be deemed to have been delivered and received on the date of transmission. Notices to Comptroller shall be to remote.deposit@cpa.texas.gov with a copy to contracts@cpa.texas.gov. Any notices to Contracting Agency will be to tjjdinvoice@tjjd.texas.gov.
- B.** Comptroller and Contracting Agency shall maintain specifically identified liaison personnel for their mutual benefit for day-to-day communications.

Section 3.09. Signatories.

The undersigned Parties do hereby certify that: (1) the services specified above are necessary and essential and are properly within the statutory functions and programs of the affected agencies of State Government, (2) the proposed arrangements serve the interest of efficient and economical administration of those agencies, (3) the services, supplies or materials contracted for are not required by Section 21 of Article 16 of the Constitution of Texas to be supplied under contract to the lowest responsible bidder, and (4) this Contract neither requires nor permits either Party to exceed its duties and responsibilities or the limitations of its appropriated funds.

The undersigned signatories represent and warrant that they have full authority to enter into this Contract on behalf of the respective Parties. This Contract may be executed in one or more counterparts, each of which is an original, and all of which constitute only one agreement between the Parties.

Texas Comptroller of Public Accounts

Texas Juvenile Justice Department

By:  _____
DocuSigned by:
11EA6DEF0EC441E...

By: 

Lisa Craven
Deputy Comptroller

Shandra Carter
Executive Director

Date: 9/5/2023 | 4:58 PM CDT _____

Date: 8/31/23 _____