



COMPU-DATA  
*International, LLC*

## CITY OF ELGIN

DOCUMENT IMAGING AND DATA HOSTING  
STATEMENT OF WORK  
Option 2

June 27, 2019

## COMPU-DATA International, LLC

14610 Falling Creek Drive  
Houston, Texas 77068

[www.cdlac.com](http://www.cdlac.com)

Jaime Flores

[jflores@cdlac.com](mailto:jflores@cdlac.com)

(713) 443-7541





COMPU-DATA INTERNATIONAL, LLC  
Statement of Work  
Option 2



*COMPU-DATA International, LLC PROPRIETARY INFORMATION*

*The information contained in the document is confidential and is intended only for the privileged use of the City of Elgin. Any review or other use, distribution, dissemination, reproduction or taking of any action in reliance upon this information by individuals, companies or entities, other than the intended recipient, is strictly prohibited.*

*Copyright and Trademark Acknowledgement*

*All brand names and product names referenced in this document are trademarks of their respective holders.*

*Previous Proposal(s) Null and Void*

*This proposal replaces all previously submitted proposals relating to the matter this proposal addresses and therefore all such previously submitted proposals are considered Null and Void.*

*This proposal is valid for thirty (30) calendar days from the date listed on page one.*



# Table of Contents

Background ..... 4

Certifications & State Contracts ..... 4

Statement of Work ..... 5

    Project Scope ..... 5

        Prepping Requirements ..... 5

        Scanning Requirements ..... 5

        Indexing Requirements ..... 5

        Data Delivery Requirements ..... 6

        Approval Process ..... 6

        Project Start Date ..... 6

        Estimated Project Duration ..... 6

        Training and Support ..... 6

Project Personnel ..... 7

Virtual FileRoom™ ..... 8

    Repository Management & User Environment ..... 8

    Supported Text Search Modes ..... 8

    Integration with other Data Sources and Applications ..... 9

    Document and Application Security ..... 9

Pricing ..... 10

Payment Terms and Conditions ..... 11

    Accounts Payable Contact ..... 11

COMPU-DATA International, LLC Typical Service Scope ..... 12

    COMPU-DATA Imaging Quality Philosophy: ..... 12

    Box and Document Preparation: ..... 13

    Capture Process & Stage I Quality Control: ..... 13

    Stage II Quality Review: ..... 14

    Stage III Metadata Quality Review: ..... 14

    Summary of File Conversion and Compression Techniques ..... 15

    Data Approval Process ..... 15

    Document Destruction ..... 15

    Security Addendum ..... 15

        Exhibit A ..... A-1



COMPU-DATA INTERNATIONAL, LLC  
Statement of Work  
Option 2



## Background

### The Unstructured Information Management Company™

Our Mission: *Empower Users to access information instantly and without barriers  
to uncover knowledge through technology*

Founded in 1998 by the current President and CEO, Juan J. Celaya, COMPU-DATA International, LLC (CDI) specializes in the capture, index, search, and retrieval of unstructured data. Process automation and integration, as well as data security, also are key components of CDI's core services. Together, these offerings enable your organization to make your unstructured data work for you.

## Certifications & State Contracts

CDI is a DBE & MBE certified by the Texas Unified Certification Program, and a Texas HUB company whose products and services are available through the following government contracts:

- CDI Texas DIR Contract #DIR-TSO-3665
- CDI Texas DIR Contract #DIR-TSO-3902





# Statement of Work

## Project Scope

COMPU-DATA will perform for the City of Elgin the following services:

- Pick up approximately 125 banker boxes of 8.5” x 11” documents from the police department.
- Scan approximately 312,500 case files at 300dpi black & white.
- Index approximately 6,250 documents, according to project requirements.
- Upload digitized files to COMPU-DATA’s secure, cloud-hosted Virtual FileRoom™ (VFR) site for customer viewing and confirmation.
- Return requested boxes at end of project and/or destroy requested boxes

## Prepping Requirements

The City of Elgin will perform all the prepping of the Police Department files. This includes, but is not limited to, removing staples and paper clips, securing smaller pieces of paper, repairing pages as needed, and inserting document separators. In addition, the City will remove all confidential CJ I from the case files.

COMPU-DATA will provide both documentation and on-site training for the City’s prepping personnel. The documentation will describe standard prepping processes, while the on-site training will address the specific prepping requirements of the Police Department’s files.

On delivery to COMPU-DATA’s scanning facility, each box of documents will be reviewed by authorized personnel for prepping accuracy. Any issues discovered during this review will be corrected, and the box made ready for scanning.

## Scanning Requirements

All documents will be scanned in black and white at 300 dpi. If image quality requires, documents will be scanned in greyscale at 300dpi. All scanning will be performed by authorized personnel only.

## Indexing Requirements

All indexing and quality control will be performed by authorized personnel only. The index fields to be captured are as follows:

### Police Dept. Case Files

Field Name	# of Characters	Data Type	Required?	Default Value
Victim Name	15	Alpha-Numeric	Yes	
Suspect Name	15	Alpha-Numeric	Yes	
Case Number	11	Alpha-Numeric	Yes	
Report Title	15	Alpha-Numeric	Yes	



COMPU-DATA INTERNATIONAL, LLC  
Statement of Work  
Option 2



## Data Delivery Requirements

Listed below are the requirements for the delivery of the data from COMPU-DATA to the City of Elgin:

1. Searchable PDF format
2. Upload all files to respective libraries within the city's Virtual FileRoom™.

## Approval Process

COMPU-DATA International, LLC will upload the processed images/documents into its exclusive Virtual FileRoom™ (VFR), hosted on our secure Cloud environment. As part of the deliverable process, city staff will log into the VFR system to review the work that is ready for your review and approval. You will receive an email each time data is loaded and ready for review; approximately daily. At that time, you are allotted five (5) business working days to either approve or identify any corrections that need to be addressed. At the end of the five (5) working days, the data will be considered approved.

## Project Start Date

TBD

## Estimated Project Duration

Project is completion is TBD

## Training and Support

COMPU-DATA will schedule a remote training session for your VFR end-users, in which the following topics will be covered:

- Accessing and logging into VFR
- Accessing a library
- Searching for documents
  - Search templates
  - Searching using metadata
  - Using wildcards
  - Content search
  - Members versus Sets
- Viewing documents
  - Hit headers
  - Hint boxes
  - Modifying an asset
  - Viewing a file
  - Downloading a document
- Review and approval of scanned documents
- Process for submitting service requests with COMPU-DATA support
- Additional topics as identified during training



## Project Personnel

The COMPU-DATA International project team will include the following members and respective functions:

1. **Project Manager**

Responsible for overall project success and customer liaison

2. **Supervisors**

Day to day supervision of staff activities and problems resolution

3. **Document Preparation Staff**

Responsible for preparing documents in batches that are going to be scanned. Sample tasks: remove all clips, bands, staples, and other fasteners from folders and from multi-page documents. Use an appropriate tool to prevent tearing or otherwise damaging the documents.

4. **Document Scanning Staff**

Responsible for pre-scanning decisions, document scanning, indexing, etc.

5. **Quality Control Staff**

Quality checks will be performed at periodic intervals throughout the document prepping, capture and indexing process. During these checks, random samples of the documents are collected, both manually and electronically, and checked against project metrics to ensure both the quality of the image and the accuracy of the metadata.



## Virtual FileRoom™

In 1997, CDI commenced development of its core product, Virtual FileRoom™ (VFR). VFR handles all media sources encountered every day in the business world, such as paper, email, electronic documents, audio, video and images. Out of the box, VFR delivers administration, search and retrieval, collaboration functionality, reporting, and audit trails of digital assets, and is easily integrated into any business process and other application through its Web Services APIs.

CDI's product offerings are flexible and can be integrated with existing applications or products, including Microsoft Office and Adobe Acrobat. As VFR is accessed through the user's web browser, it is compatible with any operating system and any browser.

## Repository Management & User Environment

VFR supports any file format including image, audio and video files. With automatic, content-based indexing, VFR will index the text content of any file saved in the system as a "Content File", in addition to all the index fields associated with the file. For file formats of video or images whose content does not contain text, VFR will index the associated index fields. Users' access to libraries, sub-libraries and documents are managed through an integrated access control system. This system allows the system administrators to have exact control over access rights. VFR also is compatible with Microsoft Active Directory, enabling those who use it to manage VFR access rights using already established groups, users and permissions. Users are empowered to manage, store, search, retrieve and share content discovered through their search and discovery process. When used by another application to store and retrieve documents, the integrated application can be responsible for the access controls of the data stored in VFR.

The VFR Search Interfaces allows users on multiple systems to use the sophisticated underlying search engine to access online repositories. With VFR, you can perform a Content or Boolean search over multiple defined information repositories simultaneously.

## Supported Text Search Modes

**Boolean mode** – A query mode in which exact query terms are matched against the documents in the library (or against incoming documents, in the case of real time profiles); documents are not ranked for relevance; Boolean operators (AND, OR, NOT, WITHIN, ADJ, BETWEEN) can be used to control matching; special operators used with individual query terms enable concept (!), pattern (~), or wildcard (\*, [search expression], \_, @, #, ^) expansion.

### VFR Highlights Include:

- User-Functionality Access.
- Statistics and Monitoring Tools.
- Web-based application with industry standard, XML architecture.
- Highly scalable architecture built on high-end search engine versus database technology.
- Automatic indexing and retrieval of nested attachments in Outlook® email files.
- Automatic indexing and retrieval of nested attachments in archive files including zip and war formats.
- Built on common business process requirements through customer collaboration.
- Support for companion files – a file linked to an indexed content file.





# COMPU-DATA INTERNATIONAL, LLC

## Statement of Work Option 2



- Dynamic update and search field templates with options to be administered by the end user, subject matter expert and the application administrators.
- Administrator or user defined field definitions for content classification.
- User defined Personal and Public Collections. End users may define Collections to associated digital assets with project needs and share information with other users.
- Document level security based on existing or developed Access Control Lists.
- Reporting and audit trail options assuring data integrity.
- Searchable document content contribution capabilities.
- Version Control and much more!

## Integration with other Data Sources and Applications

The VFR product provides ease of integration with other applications using web services and other robust sets of APIs that will allow any vendor to interface to the CDI VFR product. These APIs allow a vendor/user to perform the following:

- Allows access to the documents stored in the CM libraries.
- Allows access to the Index fields stored with the documents.
- Allows access to the user of the CM.
- Allows login to the CM.
- Allows query data in the CM.

These are just some of the examples that are available.

## Document and Application Security

VFR satisfies the following Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the FBI's Criminal Justice Information Services (CJIS) security requirements:

- Access Control
- Unique User Identification
- Emergency Access Procedure
- Automatic Logoff
- Encryption and Decryption
- Audit Controls
- Data Integrity
- Person or Entity Authentication



**COMPU-DATA INTERNATIONAL, LLC**  
Statement of Work  
Option 2



## Pricing

Document Capture Pricing						
Description	Qty (Est.)	Price	Unit	OCR	Notes	Line Total
8.5" x 11" B&W Capture	312,500	\$ 0.06	Per Image	incl.	125 boxes @ 2500 pages per box	\$ 18,750.00
8.5" x 11" Indexing	350,000	\$ 0.015	Per Document		56 characters per document x 50 documents per box x 125 boxes	\$ 5,250.00
Document Prep Review	125	\$ 18.00	Per Hour		125 Boxes x 1 hr per box	\$ 2,250.00
Document Prep Training	1	\$ 500.00	Per Project		On-Site Training of Prepping Personnel	\$ 500.00
Setup	1	\$ 500.00	Per Project		One Time Cost	\$ 500.00
Pickup/Delivery	1	\$ 500.00	Per Trip		One Initial Trip	\$ 500.00
Document Destruction	125	\$ 10.00	Per Box		Certificate of Destruction Included	\$ 1,250.00
<b>Total *</b>						<b>\$ 29,000.00</b>

\* Note: All quantities are estimated. Invoices will reflect actual quantities of scanned images, characters indexed, and prepping review hours.

Virtual FileRoom™ (Annual Charge)					
Item Description	Quantity *	MSRP	DIR Monthly Rate	# Months	DIR Item Total
<b>Data On-Demand:</b> SaaS multi-tenant VFR Edition. 5 users, up to 50 GB of usable storage, 50 GB metered bandwidth, 1 desktop scanner (35+ ppm), and 14-day backup retention period. Includes advanced security features. Requires a 3-year agreement.	1	\$ 356.25	\$ 323.30	12	\$ 3,879.60
<b>Data On-Demand:</b> Additional 50 GB of usable storage, including 14-day backup retention period. Data usage is calculated on a monthly basis, and additional storage is automatically added, in blocks of 50 GB, as required.	4	\$ 27.00	\$ 25.85	12	\$ 1,240.80
<b>Data On-Demand:</b> Application Setup. One-time charge.	1	\$ 2,550.00	\$ -	0	\$ 2,441.63
<b>Data On-Demand:</b> Application Training. One-time charge.	1	\$ 1,100.00	\$ -	0	\$ 1,053.25
<b>First-Year SaaS Fee</b>					<b>\$ 8,615.28</b>
<b>Yearly Recurring SaaS Fee After First Year</b>					<b>\$ 5,120.40</b>

\* Note: In total, these rates include 5 user accounts and 250 GB of usable storage.



COMPU-DATA INTERNATIONAL, LLC  
Statement of Work  
Option 2



## Payment Terms and Conditions

Payment is due upon receipt of invoice. COMPU-DATA International, LLC will invoice weekly for all scanning work accepted at time of invoices and all deliverables completed at time of invoicing.

## Accounts Payable Contact

- **Name:** Phillip Taylor
- **Title:** Assistant Chief of Police
- **Office Phone:** (512) 285-5757
- **Email Address:** [ptaylor@pd.ci.elgin.tx.us](mailto:ptaylor@pd.ci.elgin.tx.us)
- **Billing Address:** 202 Depot St.
- **Billing City:** Elgin
- **Billing State:** Texas
- **Billing Zip:** 78621

Describe the process COMPU-DATA must follow, if any, to submit its invoices, such as the need for a Purchase Order: TBD

IN WITNESS THEREOF, and per the Service Agreement Terms and Conditions, the parties hereto have executed this Agreement on the day and year first above written.

**CLIENT: CITY OF ELGIN**

**COMPU-DATA International, LLC**

By: \_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Date: \_\_\_\_\_



## COMPU-DATA International, LLC Typical Service Scope

(provided as a reference only)

COMPU-DATA International will implement a Quality Assurance and Control Plan tailored to reach our customer's goals and validate the implementation of the plan for the duration of the contract. Quality Assurance and Control is a cradle-to-grave process integrated from contract award through the capture process, quality review of images and data, evolving through the initial stages of the project and culminating in the delivery of digital documents and data. Throughout the project life cycle, quality assurance feeds back into the capture process, adjusting the process toward continual improvement based on the operational changes and conditions of the collection being processed.

The latest available technology in imaging hardware and software will be utilized to expedite the capture process, while operators and analysts will provide human oversight and quality control of image definition and metadata accuracy. Images and data will be checked at multiple stages within the conversion process to identify any deficiencies in image quality, data validation or other issues.

COMPU-DATA's project manager will provide oversight on imaging personnel and processes and will be responsible for the resulting quality of images and data. The on-site operations manager or supervisor will manage the day-to-day activities and quality of the deliverables.

### COMPU-DATA Imaging Quality Philosophy:

All members of the project team will consistently focus their efforts to provide the highest quality digital product, defined as:

1. Optimal image quality subject to the client-specified resolution – factors considered include image brightness, contrast, despeckling, deskewing, deshading, folded corners covering readable data and black border removal.
2. To enhance the OCR recognition rates to the extent practical given source document quality and image resolution.
3. To maximize the success of the image conversion rate to PDF.
4. To minimize the number of page orientation errors.
5. To minimize the number of blank pages included in the final output of digital documents.

While the COMPU-DATA team strives for perfection in the final electronic documents and respective data, each project has its own intrinsic limiting factors. Some examples relevant to this project include the collection volume, the quality and state of the paper being processed, conversion production rate changes or other time constraints, available resources as well as existing and available technological capabilities. The challenge is to mitigate these factors to the extent possible and practical.



## Box and Document Preparation:

The primary purpose of this step is to properly separate the individual documents and expedite the scanning process by ensuring that the documents are arranged properly and can be physically transported through the selected scanning equipment with minimal intervention on the part of the operator. Production scanning rates at the level required under this project make this factor critical to its success.

For this project, COMPU-DATA personnel will be responsible for box and document preparation. This includes, as needed: The removal of all bindings, paper clips, staples, etc., correct orientation of the individual pages in each document, inserting a patch code document separator at the front of each document, and any other preparation required to ensure that each individual document will pass through the scanner with no damage. When the scanning work is completed, depending on the project specifications, the materials either will be destroyed, or they will be re-boxed, quality checked and then transported by CDI personnel to the UNTHSC storage location.

## Capture Process & Stage I Quality Control:

The paramount concern relative to the conversion of the several document types is the image quality of the digital rendition. Without legibility, the content cannot be read visually on a display, full-text search rates are adversely impacted, and the content becomes of little value to the end user. In a high production environment, it is critical to leverage the proper imaging hardware and software technology and processes available against the various types of documents to facilitate feeding the scanners at their rated speed while optimizing image quality.

Each scanning workstation will be configured through software with the following settings:

1. Output Resolution – minimum of 300 DPI
2. Output File format(s) – Searchable PDF
3. Automatic page rotation – off\*
4. Deskew at or less than 12°
5. Despeckle-on
6. Blank page automatic deletion – less than 1,000 bytes\*\*

\* Initial setting. Page orientation errors during document preparation require operators to have this feature engaged.

\*\*Effectiveness of setting will be analyzed and adjusted as needed.

Each document will be preconfigured during document preparation for separation and with metadata fields as specified by UNTHSC. This will be accomplished in an automated fashion, populating data through the utilization of 2D bar and patch codes inserted.

Scan operators will remove paper documents from boxes and position them in the scanner's automatic document feeder (ADF) in the orientation established during document preparation. As scanning begins, the scan operator will monitor the images and the data extracted from the bar codes as they display on the screen to identify issues with image quality and legibility, orientation, and to identify blank pages that have not been deleted by the software. Any images caught at this stage of the quality process will be corrected via the software in the case of orientation and blank pages or through modification of camera settings and rescan to improve sub-standard image brightness, contrast, etc. Additionally, the software is configured to flag documents missing data from the primary barcode.



COMPU-DATA INTERNATIONAL, LLC  
Statement of Work  
Option 2



## Stage II Quality Review:

After a batch of documents is scanned, the images will be routed to a Quality Assurance (QA) Operator who begins the second quality control process. It is the responsibility of the QA Operator to ensure that each document is imaged and meets or exceeds COMPU-DATA and/or UNTHSC quality requirements and those errors are identified and corrected. Steps in the quality control process include the following:

- The QA operator will check the visual legibility at screen resolutions of an image on the display. The purpose of this step is to make sure that an image can also produce viable text. If the display image is not legible, the source image will be reviewed to determine if a rescan of that image will be required.
- The QA operator will validate that images are upright and right-reading to the extent practical. The QA operator will rotate the image as necessary to emulate the original page format. Exceptions requested by UNTHSC will be added to the exception list.
- The QA operator will search for blank pages and all pages identified as blank images will be deleted prior to release. The QA operator will validate that truly blank images are removed by verifying questionable images with an electronic magnifying glass to ensure valid pages are not deleted. Since the software analysis is fallible, bias will be toward retention of pages to ensure that actual data is not deleted from the electronic files.

## Stage III Metadata Quality Review:

Two final processes take place in verifying that data was extracted from the barcodes. Daily, there is an automated process that reviews every document scanned and ensures that data has been extracted from the barcodes associated with each document. Finally, one last random check on the metadata extracted is performed by the operations manager after all boxes have been selected for inclusion into the weekly Transmittal.

Any errors found during these two processes are immediately addressed by reprocessing the specific document and readying it for inclusion into the weekly Transmittal.



COMPU-DATA INTERNATIONAL, LLC  
Statement of Work  
Option 2



## Summary of File Conversion and Compression Techniques

COMPU-DATA uses industry standard file conversion and compression techniques such as PDF, Searchable PDF, TIFF, JPEG, PNG, etc. The customer should select the format(s) that are most appropriate for its project.

## Data Approval Process

COMPU-DATA International, LLC will upload the processed images/documents into its exclusive Virtual FileRoom™ (VFR), hosted on our secure Cloud environment. As part of the deliverable process, your staff must log into the VFR system to review the work ready for your review and approval. You will receive an email each time data is loaded and ready for your approval; approximately daily. At that time, you are allotted 5 working days to approve or identify any corrections that need to be addressed. At the end of the 5 working days, the data will be considered approved.

## Document Destruction

COMPU-DATA can provide complete document destruction services for an additional fee. This service can be provided both for documents we first scan and digitize, and for documents that your organization wishes only to be destroyed.

COMPU-DATA uses a third-party service for document destruction. However, all document destruction occurs under the supervision of COMPU-DATA representatives. Once destroyed, proof of destruction will be provided to you in the form of a Certificate of Destruction.

## Security Addendum

Exhibit A, beginning on the following page constitutes an addendum to the terms and conditions of this Statement of Work and is incorporated herein for all purposes.

# **EXHIBIT A**

## **FEDERAL BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM**

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

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

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

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

### 1.00 Definitions

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

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

### 2.00 Responsibilities of the Contracting Government Agency.

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

### 3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed),



as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

#### 4.00 Security Violations.

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

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

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

#### 5.00 Audit

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

#### 6.00 Scope and Authority

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

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

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

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

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

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

**FEDERAL BUREAU OF INVESTIGATION  
CRIMINAL JUSTICE INFORMATION SERVICES  
SECURITY ADDENDUM  
CERTIFICATION**

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

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

\_\_\_\_\_  
Signature of Contractor Employee

\_\_\_\_\_  
Date

\_\_\_\_\_  
Printed or Typed Contractor Employee Name

Sex: \_\_\_\_\_ Race: \_\_\_\_\_ DOB: \_\_\_\_\_ State/ID or DL: \_\_\_\_\_

\_\_\_\_\_  
Signature of Contractor Representative

\_\_\_\_\_  
Date

\_\_\_\_\_  
Printed or Typed Name of Contractor  
Representative

\_\_\_\_\_  
Organization Name and Representative's Title

## Texas Signatory Page

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

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

(To be signed and dated by the vendor(s) and law enforcement agency representative(s) who signed the original contract, or at least who have authority to bind each entity – to include subcontractor services; third party service provider if applicable)

---

Printed Name of Agency Representative

---

Signature of Agency Representative

---

Title

---

Agency Name and ORI

---

Date

---

Printed Name of Vendor (Contractor) Representative

---

Signature of Vendor (Contractor) Representative

---

Title

---

Vendor Organization Name

---

Date

---

Printed Name of Vendor (Sub-Contractor)  
Representative

---

Signature of Vendor (Sub-Contractor) Representative

---

Title

---

Vendor Organization Name

---

Date