



REQUEST FOR PROPOSALS (RFP #2526-06)

IP Video Surveillance System Upgrade

Gregory-Portland Independent School District

Attention: Chris Casarez
1200 Broadway Blvd.
Portland, TX 78374

Proposal Deadline:
Thursday, April 16, 2026 | 2:00 PM (CT)

Equal Opportunity Statement

Gregory-Portland Independent School District (GPISD) is an Equal Opportunity employer. Historically Underutilized Businesses (HUBs) are strongly encouraged to submit proposals.

1. STATEMENT OF WORK

1.1 Purpose

The purpose of this Request for Proposals (RFP) is to solicit sealed proposals from qualified Installers, Systems Integrators, or Partners (“Respondents”) to **design, furnish, install, configure, and support** a comprehensive IP Video Surveillance System across GPISD facilities.

1.2 Project Objectives

GPISD seeks a **turnkey, scalable, and secure** surveillance solution that will:

- Enhance campus safety and situational awareness
- Provide centralized video management
- Integrate with existing systems (including access control)
- Support future expansion and technology upgrades
- Ensure reliable video retention and retrieval

1.3 Coverage

This RFP applies solely to GPISD. The District reserves the right to:

- Reject any or all proposals
 - Modify project scope
 - Award in whole or in part
 - Cancel this RFP at any time without liability
-

2. GENERAL INFORMATION

2.1 District Overview

Gregory-Portland ISD is a public, tax-exempt school district located in Portland, Texas, serving approximately **5,000 students** across:

- Five (5) elementary schools
- One (1) junior high school
- One (1) high school

Additional information: <https://www.g-pisd.org/>

2.2 Existing Environment

The District currently operates approximately **1,182 cameras** across multiple campuses.

The upgraded system must:

- Provide coverage of **interior and exterior areas**, including:
 - Entrances/exits
 - Parking lots and roadways
 - Athletic and auxiliary facilities
 - Support **minimum 30-day retention at 15 FPS and full resolution**
 - Integrate with existing **Keyscan Aurora Access Control System (~162 doors)**
 - Utilize and optimize existing network infrastructure where feasible
-

2.3 Schedule of Events

Milestone	Date
RFP Release	March 26, 2026
Questions Due	April 13, 2026 (5:00 PM CT)
Proposal Submission Deadline	April 16, 2026 (2:00 PM CT)
Evaluation Period	April 17–20, 2026
Board Recommendation	April 20, 2026

GPISD reserves the right to modify this schedule.

3. COMMUNICATION & SUBMISSION

3.1 Point of Contact

All communications must be directed to:

Chris Casarez
Email: ccasarez@g-pisd.org
Phone: (361) 777-1091

⚠ Unauthorized communication with other District personnel may result in disqualification.

3.2 Questions & Addenda

- All questions must be submitted **in writing** by April 13, 2026
 - Responses will be issued via formal addenda
 - Verbal communication is **non-binding**
-

3.3 Proposal Submission Requirements

Respondents must submit:

- **1 Original (signed) hard copy**
- **2 Copies**
- **1 Electronic copy (USB drive)**

📍 Submit to:
Gregory-Portland ISD
Attn: Chris Casarez
1200 Broadway Blvd.
Portland, TX 78374

Late submissions will not be accepted.

Faxed or emailed proposals will not be considered.

4. SCOPE OF WORK & TECHNICAL REQUIREMENTS

4.1 General Scope

The selected Respondent shall provide a **complete turnkey solution**, including:

- System design and engineering
 - Equipment procurement
 - Installation and configuration
 - Integration with existing systems
 - Testing and commissioning
 - Documentation and training
 - Ongoing support and maintenance
-

4.2 System Requirements

4.2.1 Video Management System (VMS)

The proposed VMS must:

- Be enterprise-grade and scalable
 - Support centralized and remote management
 - Provide role-based access control
 - Include audit logging and cybersecurity protections
 - Be compatible with ONVIF or equivalent standards
-

4.2.2 Cameras & Hardware

- High-definition IP cameras (interior/exterior rated as required)
 - Support for low-light and high dynamic range environments
 - Vandal-resistant housings where appropriate
 - PoE-compatible devices preferred
-

4.2.3 Storage & Retention

- Minimum **30 days retention** at full resolution
 - Redundant and fault-tolerant storage architecture
-

4.2.4 Integration

- Integration with **Keyscan Aurora access control system**
 - Compatibility with future systems (analytics, emergency response tools, etc.)
-

4.3 Installation Requirements

- Coordinate with GPISD IT Department
 - Minimize disruption to school operations
 - Clearly label and document all equipment and cabling
 - Provide as-built drawings upon completion
-

4.4 Training

Respondent must provide:

- On-site administrator and operator training
 - Recorded training sessions
 - User manuals and documentation (digital + hard copy)
-

4.5 Support & Maintenance

Minimum requirements:

- **3-year support agreement (required)**
 - Optional annual renewals
 - **24-hour response (critical issues)**
 - **48-hour response (non-critical issues)**
 - Software updates and patch management
 - Annual preventive maintenance
-

5. PROPOSAL FORMAT

Proposals must include:

1. Cover Page
2. Executive Summary
3. Company Profile & Qualifications
4. Relevant Experience & References (minimum 3)
5. Technical Solution Description
6. Implementation Plan & Timeline
7. Support & Maintenance Plan
8. Pricing Proposal (5-year total cost)
9. Required Certifications & Licensing

6. PRICING REQUIREMENTS

Provide a **5-year Total Cost of Ownership (TCO)** including:

Category	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Hardware						
Software Licensing						
Installation						
Maintenance						
Training						
Project Management						
Other						

Pricing must remain valid for **60 days**.

7. EVALUATION CRITERIA

Proposals will be evaluated based on:

- Technical compliance and solution quality
- Vendor experience and qualifications
- Implementation approach and timeline
- Support and service capabilities
- Cost effectiveness (Total Cost of Ownership)
- System usability and scalability

GPISD reserves the right to request presentations or clarifications.

8. TERMS & CONDITIONS (SUMMARY)

- GPISD is **not liable for proposal preparation costs**
 - All submissions become District property
 - Texas law governs this RFP
 - Required **100% performance and payment bonds**
 - Insurance requirements per Exhibit D
 - Vendors must comply with all applicable laws and regulations
-

SCOPE OF WORK, SPECIFICATIONS AND REQUIREMENTS

Gregory-Portland ISD is requesting proposals from qualified Bidders interested in providing an IP Video Surveillance System solution. This system will expand the existing video surveillance system and integrate with the existing access control system [where applicable].

4.1 IP Video Surveillance System Specifications

The IP Video Surveillance System solution should be capable of handling 1,182 cameras, (150 new and 1,032 existing). The solution should be scalable and have the capability of adding cameras as required by Gregory-Portland ISD.

Approved IP Video Surveillance System manufacturer: Avigilon Unity

The qualified Bidder will provide an Avigilon Unity IP Video Surveillance System consisting of the following components: [retain only those items defined in the scope of work for this project]

- Avigilon Unity Video management software, formerly Avigilon Control Center (ACC) software, and also known as the Network Video Management System (NVMS) or Video Management Software (VMS).
- Avigilon Unity Video Surveillance Recording Servers
- Avigilon Unity Video Surveillance Storage Appliances
- Avigilon Unity Video Surveillance Cameras and Hardware
- Avigilon Unity Video Surveillance System Analytics
- Avigilon Unity Video Surveillance Positioning Equipment
- Avigilon Unity Video Surveillance Sensors
- Avigilon Unity Video Management System Interfaces
 - Avigilon Unity Video Surveillance Remote Monitoring Workstations
- Power Supplies
- System Design including structured cabling, installation, maintenance, service and support, warranty and training.

Note:

- Prior to installation, the qualified Bidder will provide Gregory-Portland ISD with a camera schedule document or matrix with corresponding camera locations. The final revision will become 'EXHIBIT "B": PROPOSED VIDEO SURVEILLANCE CAMERA SCHEDULE AND NETWORK ROOM SCHEDULE'. This is not required for RFP submittal.
- Prior to installation, the selected Bidder will provide Gregory-Portland ISD with device layout drawings (including conduit/cable routing), point-to-point diagrams, installation details, installation manuals, and product data sheets for all systems and devices provided by the Bidder. The final revision will become 'EXHIBIT "C": BUILDING FLOORPLANS, DRAWINGS AND DEVICE LOCATIONS'. This is not required for RFP submittal.

4.1.1 Network Video Management Software (NVMS)

Basis of Design: Avigilon Unity Video 8 video management software, formerly known as Avigilon Control Center (ACC) video management software.

Description: Provide workstations with a simplified screen layout, intuitive controls, and customizable features that improve multi-person interactions.

The user interface shall include the following Avigilon video analytics and artificial intelligence (AI) features and capabilities:

Generative AI Analytics: the Avigilon GenAI feature is a 100% on-premise analytic that enhances operational awareness by allowing the user to create custom visual alerts for site-specific incidents using natural language.

- Avigilon Appearance Search™ Technology: video analytics technology and sophisticated deep learning AI-powered video search engine that quickly sorts through hours of video to locate specific persons or vehicles of interest by entering physical descriptions, uploading photos, or by finding examples within recorded video. Search video footage for additional vehicle subclasses including van, pickup truck and commercial and box truck. Improves incident response times and enhances forensic investigations by helping operators compile robust video evidence to reveal specific routes or last-known locations.
- Facial Recognition Technology: AI-powered facial recognition technology helps

security operators accelerate response times by quickly identifying people of interest to enable users to respond to events proactively. People of interest are based on secure watch lists managed by the user. The system can generate alarms from uploaded images or faces from recorded video and watch list matches.

- Focus of Attention interface: uses artificial intelligence to detect and flag live video events that may require the attention of the security operator. Events can be highlighted visually in color-coded nodes to indicate different types of events and levels of importance:
 - Blue = motion detected
 - Teal = Unusual Motion Detection or analytic event
 - Yellow = Unusual Activity Detection, Face Watch List Match Event, License Plate Watch List Match Event, or No Face Mask Detected
 - Red = Alarm.Focus of Attention interface provides a clean and simple display to verify security event notifications with a simple mouse hover over the illuminated node. Security operators can preview live video or click the node to expand it for a closer review and video playback of the event.
- License Plate Recognition (LPR) Analytics: automatically reads license plate information from vehicles, linking it to multiple watch lists and live and recorded video. Enables security operators to quickly search and find specific captured license plate video for verification and investigation. Create and import multiple vehicle license plate watch lists for instant alarm notification when a license plate match is detected.

Avigilon AdaptAI 6 Analytics: Additionally, Avigilon AdaptAI 6 Analytics shall be provided as the next era of edge-based, AI-powered analytics supported by Avigilon Unity Video. AdaptAI offers several robust features and enhancements such as Unusual Activity Detection, Unusual Motion Detection, Dynamic Privacy Masking, crowd detection, audio analytics and additional vehicle sub-classifications with analytics event support. Includes technology for improved speed detection and accuracy, expanded object classification, and improved analytic event generation and Appearance Search results.

- Unusual Activity Detection (UAD): provides new edge-based intelligence using advanced AI technology. UAD is designed to enable the detection of atypical activities such as people and vehicles traveling at faster speeds or that are found in unusual locations, which will alert operators and system users.
 - Unusual Motion Detection (UMD): learns through advanced AI technology what typical activity in a scene looks like and then detects and flags unusual motion as an alarm to allow operators to filter through large amounts of recorded video more quickly. It flags atypical events that may require further investigation.
- Dynamic Privacy Masking: easily meet privacy requirements with the ability to track and blur people and vehicles appearing in video and have the flexibility for authorized personnel to lift it during investigations.
- Crowd Detection: the Avigilon cameras allow security operators to flag unusual crowds.
- Audio Analytics: allows for expanded situational awareness with audio alerts from several different sources. Provides the ability to review video from the triggering camera to investigate the sound, with the option to record audio when needed. Separate license required.
 - o Screaming (up to 15 meters)
 - o Glass Break (up to 15 meters)
 - o Car Alarm (up to 30 meters)
 - o Smoke Alarm (up to 15 meters)
 - o Dog Barking (up to 15 meters)
 - o Metal Crash (up to 15 meters)
 - o Tire Screeching (up to 15 meters)
 - o Loud Noise (up to 40 meters)
 - o Ultrasonic Panic Alarm (up to 40 meters)

Other Key System Features and Capabilities:

- HDSM SmartCodec™ Technology: automatically adjusts compression levels for regions in a scene to optimize bandwidth while still maintaining image quality.
- FIPS 140-2 Certified Encryption: for government agencies and enterprises that require FIPS-compliant cryptography, Unity Video offers an option to use Microsoft Windows FIPS 140-2 certified cryptographic libraries to comply with IT policies.
- Avigilon Self-Learning Video Analytics: provide effective monitoring and enable proactive, real-time responses. These include Advanced Pattern-Based Analytics that recognize movements of people and vehicles while ignoring motion not relevant to a scene, and Teach-By-Example technology with Object Classification that provides more accurate alarm events and decreases false-positive alarm rates.
- Visible Firearm Detection (VFD): technology detects people with drawn firearms using cloud-enhanced AI analytics and provides real-time alerts and alarms to security operators for additional verification and action.
- Unity Cloud Services: enables a 100% cloud-based Decision Management System (DMS) to allow streamlining of investigations with an intuitive interface. Easily unify video, access control and intrusion management into a single screen. Streamline software upgrades with the ability to automatically download all Unity Video software components with a new single installer
- Unity Video Services: easily access camera feeds, receive real-time mobile notifications and manage system settings using a cloud-managed mobile device.
- Unity Video Mobile app: gain a holistic view of site alerts from the home screen with alarm notifications. Easily switch between organizations and sites with Org and Site selectors. Easily toggle between recorded and live video streams with the newly designed video player using live and recorded views.
- Access Control Unification: allows for seamless unification of Avigilon Unity Video with Avigilon Unity Access.
- Simple Camera and Server Installation: Plug-and-play capabilities for NVRs and cameras that automatically identify themselves on the network, without manual configuration or searching.
- Video Archive: Retain and manage large amounts of video for on demand retrieval and review. Extend storage beyond NVRs using the Avigilon Video Archive for reliable and scalable storage.
- Scalable Integration with External Systems: Distributed architecture features .NET-based and REST-based APIs that can easily be integrated with other systems, such as access control and building management systems.
 - ONVIF Compliance: Profiles S, T, M and G compliant VMS. Allows video and audio recovery from SD cards installed in Profile G cameras in case of network failure. Ensures interoperability between ONVIF conformant security devices.

System: Provide a scalable NVMS solution with the following minimum capabilities:

- >300 cameras per server.
- >10,000 cameras per site.
- >100 servers per site.
- Unlimited client licenses.

4.1.2 Network Video Management Software (NVMS) Functionality

General: Provide an NVMS software application that can be installed on any open platform hardware and does not require hardware multiplexer or time-division technology for video or audio.

- Recording Storage Capacity: Expandable without additional licenses.
- Video Decompression: Decompresses H.264 video through Owner supplied graphics

processing unit (GPU).

- The NVMS server and client software applications can be installed and run on same computer or on separate computers.
- Languages: Provide software with versions for the following languages:
 - o Arabic.
 - o English.
 - o French.
 - o German.
 - o Italian.
 - o Japanese.
 - o Korean.
 - o Spanish.
 - o Dutch.
- Secure Transmission: Securely sends video and audio data by transmitting commands and control data via TCP/IP using cryptographic keys based on SSL/TLS to prevent eavesdropping or tampering.
- Device Connections: Support the recording and management of video and audio sources through use of industry standard protocols, including the following:
 - o ONVIF Profile S, T, M and G.
 - o Select 3rd party proprietary device APIs.
- De-warping: Supports de-warping of live and recorded video from the following devices:
 - o Supported cameras fitted with an Immervision Panomorph lens.
 - o From cameras with a fixed fisheye lens, including but not limited to the Oncam Grandeye Evolution line of cameras.

Alarms and Events: Provide the ability to configure and manage alarms and events with the following capabilities:

- Defines event triggers that are configured to result in an alarm.
- Generates alarms based on the following event types:
 - o Detect events that occur within a camera's field of view.
 - o Detect presence of persons within a sensor's range.
 - o Detect if video or audio signal is lost and alert system administrator.
 - o Door activity detected by an access control application.
 - o Notify users of system errors.
 - o Receive alarms from third party systems (access control, etc.) and configured to be monitored.
 - o Support receiving digital input triggers and triggering digital outputs from:
 - An input/output board.
 - Supported IP camera, encoder or sensor.
 - Integrated systems, including POS.
- Receives events from devices through ONVIF driver.
- Configure an unlimited number of rules to trigger specific video operations.
- Supports receiving Simple Network Management Protocol (SNMP) messages from servers and alert users.
- Customizes and forwards alarm and event notifications to the following:
 - o Users logged into client application.
 - o Users logged into mobile application.
 - o Configured email addresses.
 - o External entities and third-party software, such as central monitoring stations and call centers.
- Escalates alarms from one user or group to another if alarm is unacknowledged for a preset duration.
- Configures email notifications to the following:
 - o Notify users and system administrators when an event or system health error occurs.
 - o Schedule when email notifications are sent.
 - o Include camera images in email notifications.
- Configures Central Station Notifications to the following:

- o Notify a central station monitoring service when an event or system health error occurs.
 - o Include video clips and/or camera images with camera motion, analytic or digital input events.
 - o Optionally use ANSI/SIA DC-09-2013 standard event notification format. ▪
- Provides ability to send central monitoring stations periodic heartbeat messages, or regular notification to confirm system connection and that there are no events of note.
- Arms or Disarms events and alarms based on a user configurable schedule or specific digital input state.

Event Triggers: Assign actions in response to specific event triggers. Response actions include the following:

- User Notification Actions:
 - o Display on-screen message.
 - o Send an email.
 - o Send notification to central monitoring station.
 - o Play a sound.
- Monitoring Actions:
 - o Start live streaming video.
 - o Create bookmark.
 - o Open a saved view.
 - o Start live streaming on a virtual matrix monitor.
 - o Open a map on a virtual matrix monitor.
 - o Open a web page on a virtual matrix monitor.
- Device Actions:
 - o Reboot camera.
 - o Activate digital output.
 - o Deactivate digital output.
- PTZ Actions:
 - o Go to Preset.
 - o Go to Home Preset.
 - o Run a Pattern.
 - o Set Auxiliary.
 - o Clear Auxiliary.
- Alarm actions:
 - o Trigger an alarm.
 - o Acknowledge an alarm.
- Supports conditional event triggers based on selected digital input status. ▪

Manually triggers digital output through the following:

- o A pre-configured software control.
- o A physical trigger that is connected to a supported input/output device.

Video Analytics: Provide configurable classified object detection for each device with self-learning video analytics capabilities.

- Allows users to connect individual video sources to analytics appliance channels. ▪
- Allows users to configure events based on classified object motion detection. ▪
- Allows configured video analytics events to be used as alarm and rule triggers. ▪
- Allows users to mark classified objects as a true or false detection.
 - o Transmits collected data to video source to improve accuracy of video analytics device.
- Support the following video analytic event types when captured by supported cameras:
 - o Object in area.
 - o Object loitering.
 - o Object crossing beam or defined line.
 - o Object appears or enters area.
 - o Object not present in area.
 - o Object enters area.
 - o Object leaves area.
 - o Object stops in area.
 - o Object too close.
 - o Direction (of travel) violated.

- o Smart Motion Rule.
 - o Tamper detection.
 - o Crowd size.
 - o Unusual crowd growth.
 - o Unusual crowd size.
 - o Scene dramatically changes in an unexpected fashion.
- Avigilon Appearance Search™ Technology: video analytics technology and sophisticated deep learning AI-powered video search engine that quickly sorts through hours of video to locate specific persons or vehicles of interest by entering physical descriptions, uploading photos, or by finding examples within recorded video. Search video footage for additional vehicle subclasses including van, pickup truck and commercial and box truck. Improves incident response times and enhances forensic investigations by helping operators compile robust video evidence to reveal specific routes or last-known locations.
 - Facial Recognition Technology: AI-powered facial recognition technology helps security operators accelerate response times by quickly identifying people of interest to enable users to respond to events proactively. People of interest are based on secure watch lists managed by the user. The system can generate alarms from uploaded images or faces from recorded video and watch list matches.
 - Focus of Attention interface: uses artificial intelligence to detect and flag live video events that may require the attention of the security operator. Events can be highlighted visually in color-coded nodes to indicate different types of events and levels of importance:
 - Blue = motion detected
 - Teal = Unusual Motion Detection or analytic event
 - Yellow = Unusual Activity Detection, Face Watch List Match Event, License Plate Watch List Match Event, or No Face Mask Detected
 - Red = Alarm.
 Focus of Attention interface provides a clean and simple display to verify security event notifications with a simple mouse hover over the illuminated node. Security operators can preview live video or click the node to expand it for a closer review and video playback of the event. Provides functionality which automatically focuses the operator's attention during critical events.
 - o Event Handling:
 - Classified object motion detection.
 - Unusual motion.
 - Rule based video analytic events.
 - Alarm events.
 - o Filtering:
 - Event types: Provide a user interface which allows for inclusion or exclusion of unnecessary event types.
 - Frequent event handling: Support the identification and exclusion of frequently recurring events on a per-camera and per event basis.
 - License Plate Recognition (LPR) Analytics: automatically reads license plate information from vehicles, linking it to multiple watch lists and live and recorded video. Enables security operators to quickly search and find specific captured license plate video for verification and investigation. Create and import multiple vehicle license plate watch lists for instant alarm notification when a license late match is detected. Supports operation of a license plate recognition system that includes:
 - o Defines region of an image where license plate detection is performed. o Stores detected license plates with video data.
 - o Support multiple watch lists that are used to create events or alarms when specific license plates are detected.
 - o Defines the longest retention period for license plate detections for privacy compliance.

Signal Processing and Compression: Supports storage and processing of video and audio as follows:

- Natively records camera signals with no transcoding.

- Supports industry standard video compression formats, including, but not limited to, the following:
 - o JPEG2000.
 - o MJPEG.
 - o MPEG-4.
 - o H.264.
 - o H.265.
- Synchronizes audio and video regardless of frame-rate, resolution or bitrate.

Dynamic Video Stream Management: Performs dynamic video stream management as follows:

- Provide High-Definition Stream Management (HDSM)[™].
- Reduces system bandwidth and storage usage by only transmitting video to client as determined by the Owner.
- The client communicates the maximum monitor resolution to the server and the server acts as a video proxy and streams the required video resolution. ▪ Tile multi-megapixel videos streams and only transmit requested portion of video stream to the client.
- Extend recorded video storage by dynamically reducing quality of recorded video over time so video is still viable but uses less storage.
 - o Reduces JPEG and JPEG2000 video image rate to one half or one quarter of original image rate.
 - o Record both a high-quality stream and a low-quality stream, discarding high quality streams after a set amount of time determined by the Owner. ▪ Allow availability of dynamic video stream management to local users, remote users, and mobile devices.

Event Logging: Maintain an event log and allows users to use log events as triggers for specific event actions. Logged events include the following:

- Server events:
 - o Server application starting up.
 - o Server application shutting down.
 - o Server application terminated unexpectedly.
 - o Server application low on resources.
 - o Server application installation error.
 - o License expires soon.
 - o License expired.
 - o Database error.
 - o Data initialization error.
 - o Data volume failed.
 - o Data volume recovered.
 - o Data volume size reduced.
 - o Data write error.
 - o Data upgrade started.
 - o Data upgrade completed.
 - o Data upgrade failed.
 - o Data recovery started.
 - o Data recovery completed.
 - o Data recovery failed.
 - o Bookmark save failed.
 - o Network connection found.
 - o Network connection lost.
 - o Email send error.
 - o Server hardware event.
 - o Archiving started.
 - o Archiving completed.
 - o Archiving interrupted.
 - o Server connection lost.
 - o Analytics server queue full.
 - o Analytics server connection lost.
 - o LPR service restarted.
 - o LPR service terminated unexpectedly. ▪

Device Events:

- o Connection created.
- o Connection removed.
- o Connection created to standby server. o
- Connection removed from standby server. o
- Connection failure.
- o Device failed.
- o Connection restored.
- o Network packet loss unacceptable. o
- Network packet loss acceptable.
- o Motion detection started.
- o Motion detection ended.
- o Video analytics event started.
- o Video analytics event ended.
- o Tampering detected.
- o Recording started.
- o Recording ended.
- o Recording interrupted.
- o Recording resumed.
- o Digital input activated.
- o Digital input deactivated.
- o Firmware upgrade started.
- o Firmware upgrade completed.
- o Firmware upgrade failed.
- o Obsolete firmware detected.
- o User-defined event started.
- o User-defined event ended.
- o Presence detected.
- o Presence ended.
- o Presence dwell time exceeded. o
- Presence dwell time ended.

▪ User Events:

- o User login.
- o User logout.
- o Server setting changed.
- o Site setting changed.
- o Device setting changed.
- o Device connected.
- o Device disconnected.
- o Digital output triggered.
- o Bookmark added.
- o Bookmark updated.
- o Bookmark deleted.
- o PTZ moved.
- o PTZ idle.
- o Export performed.
- o Speaker activated.
- o Speaker deactivated.
- o Virtual matrix monitor opened.
- o Map added.
- o Map updated.
- o Map deleted.
- o View added.
- o View updated.
- o View deleted.
- o Web Page added.
- o Web Page updated.
- o Web page deleted.
- o Site View updated.
- o Custom keyboard command triggered. ▪

Alarm Events:

- o Alarm acknowledged.

- o Alarm auto acknowledged.
- o Alarm triggered.
- o Alarm assigned.
- o Alarm unassigned.
- o Alarm purged.
- POS Transaction Events:
 - o POS transaction started.
 - o POS transaction ended.
 - o POS transaction exception.
- License Plate Recognition Events:
 - o License plate detection started.
 - o License plate detection ended.
 - o License plate watchlist match.
- Access Control Events:
 - o Door access denied.
 - o Door access granted.
 - o Door closed.
 - o Door forced.
 - o Forced door closed.
 - o Door held open.
 - o Held door closed.
 - o Door opened.
 - o Door duress.
 - o Door request to exit.
 - o Certificate validation failed.
 - o Input activated.
 - o Input deactivated.
 - o Input fault detected.
 - o Input fault cleared.

Storage Management: Allow management of recorded content with the following capabilities:

- Multiple levels of video storage management:
 - o Tier 1: Video recorded directly on local server.
 - o Tier 2: Recorded video continuously archived to long term storage.
 - o Ad Hoc: Recorded video on local server can be archived on-demand to administrator-defined storage location.
- Support for the following video and audio recording options:
 - o Manually triggered recording.
 - o Pre-event and post-event recording options.
 - o Reference frame recording option in absence of events.
 - o Recording schedules that can be defined individually for each video source, including, but not limited to continuous recording.
 - o Event based recording that is triggered by the following:
 - Pixel or classified object motion.
 - Digital inputs.
 - POS transactions.
 - Alarms.
 - License plates recognition.
 - o Customized daily and weekly schedule.

Backup and Archiving:

- Schedules archive of recorded video with associated events to a local folder or mapped network drive.
- Backs-up settings and configuration for each server, including the following:
 - o Site settings, such as users/groups, maps and web pages.
 - o Server settings, including device connections.
 - o Encrypts backup to maintain security of information.
- Restores backed-up settings and configurations to a new or replacement server in a site.

4.1.3 Network Video Management Software (NVMS) Credentials and Security

Single Login Credential: Provides simple management of all aspects of the video management system with a single, unified login.

Authentication: System must require users to be authenticated prior to granting access to the NVMS.

Unity Privilege Management: Allows the user to configure roles, user groups and policies across the organization to harmonize privileges on all system sites.

Customization: Provide access rights that can be tailored to each user or group of users. Access rights include the following:

- View live images:
 - Use PTZ controls.
 - Lock PTZ controls.
 - Trigger manual recording.
 - Trigger digital outputs.
 - Broadcast to speakers.
- View recorded images:
 - Export images.
 - Archive images.
 - Create teach markers.
- Manage saved views.
- Manage maps.
- Manage web pages.
- Manage virtual matrix monitors.
- Initiate collaboration sessions.
- Manage user sessions.
- Listen to microphones.
- Setup cameras:
 - Setup general settings.
 - Setup network settings.
 - Setup image and display settings.
 - Setup compression and image rate settings.
 - Setup image dimension settings.
 - Setup motion detection settings.
 - Setup privacy zone settings.
 - Setup manual recording settings.
 - Setup digital input & output settings.
 - Setup microphone settings.
 - Setup speaker settings.
 - Setup analytics settings.
 - Setup teach by example.
- Setup sites:
 - Setup name.
 - Manage site.
 - Setup site view.
 - Setup user and group settings.
 - Setup Active Directory Synchronization.
 - Setup Corporate Hierarchy.
 - Setup alarm management settings.
 - Setup POS transaction settings.
 - Setup LPR settings.
 - Setup email settings.
 - Setup rule engine settings.
 - View site logs.
 - Connect and disconnect devices.
 - View Site health.
- Setup servers:
 - Manage server.
 - Setup schedule settings.
 - Setup recording and bandwidth settings.
 - Setup Storage Management.
 - Backup settings.

- o Setup server analytics.

Access Ranking: Provide the ability to rank access rights based on a user's position within a configured hierarchy.

- Ranked users may only administer changes to users and groups that are subordinate in rank.
- Corporate hierarchy can be used to enforce authority of a parent site over user and group settings of one or more child sites.

Hierarchical Site families: Allow for the creation and management of parent-child relationships among sites.

- Child sites may be connected to an appropriately licensed parent site.
- Parent site will have control over user permission and information of a child site.
- If a user has access to parent site, child sites are automatically discovered.

Credentials: Allow multiple credentials for system access, including but not limited to:

- Validation of user credentials and password entered into NVMS user database where user passwords meet a configurable strength requirement.
- Two-factor authentication of users in the NVMS using time-based One-Time Password (TOTP) and a supported mobile authenticator application used to generate a code on Apple and Android mobile devices.
 - Importing members of Active Directory groups as users in NVMS.
 - o Automatically synchronizes changes made to members in Active Directory with NVMS.
 - o Directly adds users imported from Active Directory to existing permission groups.
 - Importing roles from Access Control Manager application.
 - o Automatically synchronizes changes made to roles in the access control application with NVMS.
 - o Directly adds users imported from the access control application to existing permission groups.
 - o Imported users with appropriate privileges will be able to control doors within NVMS.
- Windows credentials.

Security: Manage and personalize user access as follows:

- Allow administrators to override user access to an NVR if there are insufficient licenses.
- Allow administrators to restrict user access to any video recorded earlier than the current login session
- Allow administrators to restrict user access to high resolution recorded video for privacy compliance.
 - Allow administrators to restrict specific user's access to search features that use what is considered personally identifiable information (PII) for privacy compliance, such as license plates and physical appearance.
- Allow administrators to define rules that disable video or audio streams from specific devices for privacy compliance.
 - Set client software to automatically log in to multiple sites.
- Set client software to automatically log out of all sites when application is left idle.
- Set client software to automatically save and restore last window layout.
- Set maximum bandwidth of streamed video data from server to client application.
- Record and permit reporting on user activity including log-in, log-out events, video export requests, live video viewing by camera, access to recorded video by camera.

4.1.4 Network Video Management Software (NVMS) Compatibility

Mobile Client Software Compatibility: Provide software compatible with the following mobile device applications:

- Android version 5.x or later.
 - iPad, iPhone and iPod touch with iOS 10 or later.

Monitoring Sources: Monitors video and audio sources from the following sources:

- Avigilon cameras/encoders

- ACTi cameras/encoders
- ALESYS SRL – Integro
- AMAG Technology
- Arecont cameras
- Axis cameras/encoders
- Bosch cameras/encoders
- Commend International GMBH
- Everbridge
- IQInvision cameras
- IVMS GMBH
- Lenel/S2
- Magos Systems
- Mobotix cameras
- Motorola Solutions Orchestrate support
- Netwatch
- ONVIF Profile S, T, M and G conformant cameras and encoders ▪
- Panasonic cameras/encoders
- Paxton Access
- Pelco cameras
- Quanergy
- Rialto Video Analytics Appliances
- Samsung/Hanwha cameras/encoders
- Samsung/Hanwha Techwin cameras
- Senstar Network manager
- Shooter Detection Systems
- Sony cameras
- Spotter Global
- Teldio
- TSS Group – C4 Integration System
- VeoVision Solutions
- VideoIQ cameras/encoders

Device Discovery and Identification: Detects and systems on network by the following methods:

- Automatic: Servers, video and audio sources that are connected to same network as client are automatically discovered.
- Search: Servers, video and audio sources running on a different network segment than client can be discovered by searching for device's IP address or hostname.
- Parent to Child: By logging into a parent site automatically discovers configured child sites.
- Manual Detection: Allows manually discovered server instances, video and audio sources, and access control appliances to be visible to users of a single client workstation.
- Network Settings: Identical for all users of a single client workstation.

Integration with Third-Party Systems and Products:

- Access Control applications:
 - o Supports configurable network connection to access control appliances. o Creates link between cameras and doors.
 - o Creates rules triggered by door actions that result in actions performed by NVMS.
 - o Synchronizes users and user privileges from access control system to provide access to doors.
 - o Supports identity verification using access control credentials to compare access token images against live video.
 - o Supports identity search using access control credentials to review door access activity in recorded video.
 - o Support using identity search results to initiate an Appearance Search across cameras in the current or alternative sites.
 - o Provides door grant access while monitoring video.

- Point of Sale (POS) Integration:
 - Supports the operation of a point of sale (POS) system that includes:
 - Receiving of transaction information from POS sources.
 - Supports multiple encoding formats from POS sources.
 - Monitors live and recorded transactions from POS sources with linked video.
 - Generates events based on POS transaction exceptions.

- Third Party Integration Requirements: Support software level integration with third-party applications using NVMS software development kit (SDK) or Application Programming Interface (API) and provide the following features to the third-party software:
 - Connection: Auto-discover servers, login and authentication.
 - Video Streaming: Auto-discover connected cameras, live and recorded video (RAW or MJPEG format; H.264 only to Windows applications).
 - Video Overlays: Display overlays over streaming video (classified object bounding boxes, motion detection, camera name/location, timestamp).
 - PTZ Control: Control PTZ cameras (pan/tilt, zoom, presets, patterns, iris and lock PTZ).
 - Audio Streaming: Stream audio from third-party system to an NVMS camera (camera to third-party system only to Windows application).
 - Alarm Management: List, query, trigger, assign, acknowledge & purge alarms.
 - Event Management: List, query, subscribe for notification on events (camera, server, administrative, digital I/O, video analytics, license plate recognition, point of sale).
 - Bookmark Management: List, query, create, delete.
 - Digital Output: Trigger digital outputs.
 - Archive/Export: Trigger archive or export in NVMS native export video format or generic video/image formats including AVI, PNG, TIFF, JPEG.

- Support integration with the following systems:
 - Avigilon Unity Access, formerly known as Avigilon Access Control Manager (ACM).
 - Motorola Solutions Orchestrate support.
 - DSX Access Systems WinDSX.
 - RS2 AccessIT! Universal.NET.
 - Avigilon Control Center License Plate Recognition (V2 LPR plug-in).
 - ACRE
 - AMAG Symmetry.
 - Gallagher Command Centre.
 - Identiv
 - Jacques IP Intercom.
 - Lenel OnGuard.
 - Paxton Net2.
 - S2 Netbox.
 - Software House CCure 9000.
 - Vingtor-Stentofon AlphaCom.

Pan-Tilt-Zoom Configuration and Control: Enables and configures PTZ control on RS-485 interface of a video source.

- Supports the following PTZ protocols:
 - American Dynamics Sensormatic.
 - Avigilon.
 - AXSYS.
 - AXSYS DCU.
 - Ernitec ERNA.
 - Honeywell Diamond.
 - JVC JCBP.
 - Kalatel ASCII.
 - Pelco D.
 - Pelco P.

- o TEB Ligne.
- o Vicon extended.
- o Vicon normal.
- o Videotec Legacy.
- o Videotec MACRO.
- Supports pan-tilt-zoom (PTZ) cameras and provides the following:
 - o Supports controlling mechanical PTZ, iris and focus as well as setting presets and patterns.
 - o Provides ability to name PTZ presets.
 - o Supports ability to create PTZ guard tours by combining a set number of presets that are run in order or random sequence.
 - o Supports ability to center a PTZ camera's field of view by clicking anywhere on video image.
 - o Supports ability to click and drag to define an area for PTZ camera to mechanically zoom and center on.
 - o Supports controlling mechanical PTZ camera on-screen display and auxiliary controls.
 - o Support selecting digital image defog levels where supported.
 - o Support selecting camera day/night operation mode where supported.
 - o Supports locking PTZ controls.
 - o Permits a user with a higher rank to override a PTZ control lock.
 - o Supports using a USB joystick to control PTZ functions.

4.1.5 Network Video Management Software (NVMS) User Interface

General: Provide a graphic user interface with the following functionality:

- A system tree of video sources in video monitoring tab.
 - o The system tree display can be configured.
 - o The system tree can be organized into virtual folders that are represented as branches within site.
 - o Users can be granted access to individual items or entire folders within system tree.
 - o Maps, saved views and web pages may be viewed.
- Client adjustable light and dark theming with settings specific to each application and workstation.
- Support for collaborative application window sharing within in a joint session among multiple users.
- Support for an unlimited number of monitors used for monitoring video and audio streams connected to a single workstation.
 - o Displays all video sources connected to system.
 - o Support ability to drag and drop items from system tree into video monitoring area.
 - o Support monitoring live and recorded video and audio streams simultaneously on same monitor.
 - o Support viewing same live or recorded video stream at different zoom levels and areas of interest.
 - o Support ability to switch from live to recorded video on demand for an instant replay of recently recorded video.
 - o Support creation of unlimited views with unique layouts of video streams.
 - o Support ability to toggle between tiled and full-screen view.
 - o Support ability to save configured display setting.
 - o Support ability to cycle through views (guard tour) based on a specified interval.
 - o Supports live or recorded video monitoring of 1 to 64 video streams simultaneously on a single monitor.
 - o Supports displaying videos streams in the following standard layouts:
 - Full Screen
 - 2 x 2
 - 3 x 3
 - 4 x 4
 - 5 x 5
 - 6 x 6

- 8 x 8
 - 1 + 5
 - 1 + 7
 - 1 + 12
 - 2 + 8
- o Provides tools to build custom video monitoring layouts.

Video Parameter Controls: Support modifications to the following image quality and image rate parameters for each individual video source:

- Video streaming format.
 - System optimized recording profile or manual configuration.
 - Keyframe interval.
 - Secondary stream for live viewing.
 - Configure video streaming at a lower image rate when scene is idle. ▪
- Customize primary and secondary stream on supported cameras.

Camera Controls: Provide the ability to change the following supported video options at the client or video source:

- Encrypt camera configuration data if supported by camera.
- Camera passwords from client application.
 - Exposure, iris, IR filter, backlight compensation, gain, priority, sharpening, saturation, focus, and white balance settings for a video source.
- Image dimensions for a video source.
 - Rotate image 90, 180 or 270 degrees within a video source.
- Addition of multiple privacy zones within a video source to block areas from being viewed or recorded in image field of view.
 - Set a maximum duration for manually triggered recording within a video source.

Audio Controls:

- Provides ability to change input, output, gain and volume for an audio source. ▪
- Supports use of uni-directional and bi-directional audio.
- Provides ability to link any audio source to any video source. o
 - Able to link multiple audio sources to a single video source.
 - o Able to link an audio source to many video sources.
- Provides ability to synchronize audio and video on playback. ▪ Supports ability to bias displayed video to a lower frame rate or lower image resolution if there is insufficient network bandwidth or processing power. o Bias shall not affect video recording.
 - o Bias shall not affect video exports.
- Supports ability to independently control if audio source is enabled for the user to monitor and if audio source is recorded with the video source
- Provides a Virtual Matrix application module supporting remote control of multiple monitor displays, including video walls. Displays simultaneous video streams on connected monitor displays from multiple sites.
- Displays overlays on top of video images.
 - o Auto-hiding functional overlays that changes depending on video streaming mode and device support. Functional overlays include, but are not limited to, the following:
 - Button to manually trigger video recording / video recording indicator.
 - Button to trigger digital output.
 - Button to capture video snapshot.
 - Button to close video stream.
 - Button to reserve a portion of screen for alarm video.
 - Button to enable audio.
 - Button to display POS transactions.
 - Button to maximize video display.
 - Button to trigger single-camera search.
 - Button to grant door access.
 - Click classified object bounding box to initiate Appearance Search. •
 - o PTZ controls.
 - o Information overlays that include, but are not limited to, the following: •
 - Camera name.

- Camera location.
 - Playback timestamp with option of displaying device time or local time. •
 - Live timestamp with option of displaying device time or local time. •
 - Recording indicator.
 - Motion activity.
 - Video analytics object detection activity with colored bounding boxes around moving objects classified as humans or vehicles.
 - Video analytics unusual motion anomaly detection with colored bounding boxes indicating area of motion.
 - Detected license plate.
- Supports alarm management operations through video monitoring interface. Including but not limited to:
 - o Designated tab for reviewing alarms.
 - o Interface supports sequential viewing of alarms.
 - o Interface supports sorting of alarms by:
 - Priority.
 - Activation time.
 - Status.
 - o Interface supports filtering alarms by status in the following priority: •
 - Assigned to me.
 - Active alarms (unassigned).
 - Alarms assigned to others.
 - Acknowledged alarms.
 - o Supports ability to assign alarms to user.
 - o Supports ability to acknowledge alarms.
 - o Supports ability to bookmark alarms.
 - o Designate one or more regions in video display area for displaying video directly linked to triggered alarms or rules.
 - Supports ability to acknowledge alarms from designated video display area.

Site Mapping: Support mapping of the physical locations of cameras and other devices throughout surveillance system.

- Provide maps with the ability to do the following:
 - o Create a hierarchy of interlinked maps.
 - o Drag and drop objects in system tree onto map.
 - o Click and display objects from map.
 - o Drag and drop a video source from map into video viewing area. o
 - o Display a preset area of selected video source.
 - o Provide customizable map icons.
 - o Highlight specific cameras when an alarm linked to camera is triggered. ▪
- Image Size: 3000px by 3000px or 9 MP, maximum.
- File Formats: Maps may be created from the following file formats: o
 - o JPEG/JPG.
 - o BMP.
 - o PNG.
 - o GIF.

Playback of Recorded Video and Audio: Support playback of recorded video and audio with the following features:

- Forward and reverse playback of recorded content at variable speeds. ▪
- Recorded content plays back synchronously when signal sources are linked. ▪
- Playback of recorded video from archived long-term storage. ▪ The ability to require dual authorization to access features and require specific user groups to request a second user authentication before recorded video may be displayed.
- Provide the following methods for navigating recorded video: o
 - o Selectable calendar.
 - o Horizontal, scrollable timeline:
 - Timeline lists all displayed video sources.
 - Timeline highlights motion and events in recorded video.
 - Video archived to long term storage shall be identified on timeline. •

- Supports a timeline that can display down to quarter second increments.
- Supports a timeline that can synchronize video displayed on multiple tabs to same point in time.
- Interface supports filtering unusual motion anomaly events on the timeline by rarity, duration and type.

Search of Recorded Video and Audio: Allow for searching of recorded content with the following functionality:

- Support recorded video search with the following selectable parameters:
 - o Time.
 - o Date.
 - o Event type.
 - o Visual search based on a pre-defined image area, or image thumbnail:
 - Thumbnails can be based on entire image region or a pre-selected area.
 - Thumbnails can be stacked to support an automatic secondary search when looking at a large timespan of video.
 - o Pixel motion in user defined areas.
 - o Classified object motion detection in user defined areas on supported video analytics sources.
 - o Bookmarks.
 - o Video source.
 - o Point of sale transactions.
 - o Alarm.
 - o License plate detection events.
- Support object Appearance Search across multiple cameras:
 - o Ability to search for a person or vehicle of interest in recorded video from multiple cameras in the current or alternative site to return possible matches.
 - Automatically enhance person search by utilizing face characteristics to match similar people from supported cameras.
 - Supported cameras with self-learning video analytics capabilities that are connected to an NVR with a supported GPU accessory should be able to return possible matches for search.
 - o Ability to initiate an Appearance Search of recorded video for similar persons or similar vehicles based on a specific user selected object in a video scene
 - o Ability to initiate an Appearance Search of recorded video by description:
 - Using one or more personal characteristics: gender, age category (child vs adult), hair color, upper body color, lower body color
 - o Ability to initiate search from recorded video in Client application or dedicated player.
 - o Supports reviewing search results and confirmation of correct matches.
 - o Supports editing search parameters including:
 - Cameras included in search.
 - Time range for search.
 - o Supports playback of search results, including:
 - Recorded video associated with individual results.
 - Sequential playback of recorded video associated with confirmed to be correct matches.
 - o Supports exporting video associated with results, including:
 - Recorded video associated with one of more selected results.
 - Recorded video associated with confirmed to be correct matches.
 - Redacting video for privacy to blur the resulting video except for the objects selected in the results.
 - o Supports creation of bookmarks for results, including:
 - One or more selected results.
 - Confirmed to be correct matches.

Bookmarking:

- Supports creating bookmarks for recorded video and audio. Bookmarks can be:
 - o Viewed from multiple sources.
 - o Displayed on timeline during playback.
 - o Used as a search criteria for recorded video and audio. Search criteria can include but are not limited to:

- Name.
- Description.
- Bookmark creator.
- o Supports protecting a bookmark so associated video and audio data is never overwritten.
- o Supports private bookmarks that are only visible to user who designated bookmark as private, and system administrator.

Media Exporting: Support the ability to export media and provide the following options:

- Clip Link Sharing: allows the user to easily export and share short video clips via a link enabled by Unity Video Services. No additional licenses, fees or subscriptions required.
- Exports recorded video in the following formats:
 - o Native (AVE)
 - o JPEG
 - o PNG
 - o TIFF
 - o AVI
 - o Print
- Exports recorded audio in the following formats:
 - o WAV
 - o Native (AVE)
 - o AVI
- Exports a still frame of video as displayed in video preview area:
 - o Native (AVE)
 - o JPEG
 - o PNG
 - o TIFF
- Native (AVE) format exported as follows:
 - o Digitally sign recorded video and audio using 256-bit encryption so video can be authenticated for evidentiary purposes.
 - o Protect exported video with a password meeting configurable strength requirement.
 - o Able to export video from one or multiple camera streams simultaneously.
 - o Supports exporting multiple video segments from different spans of time.
 - o Supports reviewing of exported or backed-up video and audio in a dedicated player.
 - o Supports playback of exported clips in synchronized, sequential time.
 - o Supports playback of multiple clips in continuous, sequential order.
 - o Supports exporting of video in lower frame-rates than originally recorded.
 - o Supports exporting of a designated area from camera's recorded field of view.
 - o Supports re-export into Native or other supported formats.
 - o Provides a record of video source with the following metadata:
 - Camera model
 - Firmware version
 - Location
 - MAC address
 - Serial number
 - Resolution

Version Upgrade: Provide a process for upgrading versions:

- Upgrading server software shall not require physical access to servers.
 - o Launch upgrades from client interface.
 - o All connected servers and clients shall receive a distribution of new version upgrade.
 - The administrator can manually trigger upgrade of each server.
 - o The user shall be able to monitor upgrade progress from client interface.
- Upgrading number of connected devices or upgrading to enterprise version only requires a change in license key.
- Upgrade from one version to another occurs without having to uninstall

- application and previous version.
- Automatically upgrade connected video or audio source device firmware if applicable.
- Automatically prompt user to upgrade client application if it is out of date with respect to server software.

4.1.6 Hardware

Owner Furnished, Contractor Installed (OFCI) Hardware:

- Configure NVMS to run as a service to automatically start when server or workstation is powered on.
 - The NVMS allows users to monitor and administer system from:
 - o A single client application for monitoring live and recorded video and audio.
 - o A single window for administering all system connections.
 - o A single tab for monitoring overall system health including:
 - All sites connected in parent-child relationships.
 - Any connected analytic appliances in the site.
 - Any connected Access Control systems.
 - Server-side License Plate Recognition processes.
 - Server-side Analytic Service processes with peak load information.
 - o Ability to export health report to Portable Document Format (PDF).
 - o Each client with access to a local or distributed network.
 - The NVMS provides a maintenance log and audit trail of all system errors and events.
 - The NVMS provides multiple levels of system redundancy:
 - o Cluster and synchronize at least 100 servers into a unified site.
 - In the event of a server failure, system can continue running and allow other servers to take over failed server's tasks.
 - o Centralized system administration:
 - Site and server configuration details are replicated to each server in the site.
 - Sites can be organized in a hierarchical parent-child relationship where parent can always control child site settings.
 - o Connect a video or audio source to multiple servers to achieve redundant recording.
 - o Create a failover connection for a video or audio source between servers in a site.
 - The NVMS provides the capability to replace malfunctioning video or audio sources with a new device and associate old recorded video with the new device. ▪ The NVMS provides capability to rename all sites, servers, and video and audio sources.

Peripherals:

- The NVMS provides ability to control client application using the following types of peripherals:
 - o A USB keyboard and/or mouse
 - o A USB joystick.
 - o A PTZ controller keyboard.

4.1.7 Cameras

Approved Outdoor Bullet Camera: Avigilon H6A Bullet Camera.

Description: The Bullet Camera shall be the Avigilon H6A (short) Bullet Camera. No substitutions will be accepted. The camera will be an indoor/outdoor IP bullet camera with up to 8 MP (4K) image resolution, equipped with Artificial Intelligence (AI) and audio analytics, and with the option for wide angle or telephoto lenses.

Primary Characteristics: The 8 MP (4K) (short) Bullet Camera shall meet or exceed the following primary characteristics:

1. H.264 HDSM SmartCodec, H.265 HDSM SmartCodec and MJPEG compression.
2. Resolution up to 3840 x 2160 pixels.
3. Maximum frame rate up to 60 fps (in High Frame Rate Mode with analytics disabled).

4. Built-in microphone for audio analytics with physical disable switch.
5. Day/night operation with 850 nm IR LED.
6. Power: POE+ IEEE 802.3at Class 4 and POE IEEE 802.3af Class 3.
7. Onboard storage and cloud management.
8. Optional per-camera license available for license plate recognition (LPR) analytic functionality.
9. Remote zoom and focus; auto focus.

Additional Camera Specifications (Short Bullet):

1. Image Performance:
 - Image Sensor: 1/1.8" progressive scan CMOS
 - Resolution: 8 MP (4K) up to 3840 x 2160 pixels.
 - Dynamic range:
 - WDR Off: up to 83 dB
 - WDR On (IEC 62676): up to 130 dB (dual exposure, 30 fps)
 - WDR On: up to 144 dB (dual exposure, 20 fps or less)
 - Max Image Rate:
 - 50 Hz / 60Hz: 25 fps / 30 fps
 - Signal-to-Noise Ratio: >50 dB
2. Lens and Illumination:
 - Focal Length: 4.4 – 9.3 mm
 - Max IR range:
 - Full Tele: 229' (70 m)
 - Full Wide: 131' (40 m)
 - Minimum illumination:
 - With IR: 0 lux in monochrome mode
 - Without IR: 0.006 lux in monochrome mode; 0.02 lux in color mode ●
 - Horizontal Angle of View:
 - 47° - 109° (16:9)
 - 39° - 78° (4:3)
 - Vertical Angle of View:
 - 26° - 57° (16:9)
 - 26° - 57° (4:3)
 - Max Aperture: f/1.3
 - Control:
 - Remote Zoom and Focus
 - Autofocus
 - Automatic Night Mode
 - IR cut filter
 - 850 nm IR LED
3. Image Control:
 - Image Compression Method:
 - H.264 HDSM SmartCodec
 - H.265 HDSM SmartCodec
 - Motion JPEG
 - Streaming:
 - Multi-stream H.264
 - Multi-stream H.265
 - Motion JPEG
 - Motion Detection:
 - Pixel Motion with selectable sensitivity and threshold
 - Classified Object Detection
 - Camera Tamper Detection
 - Electronic Shutter Control
 - Automatic
 - Manual (1/7.5 to 1/15000 sec)
 - Iris Control
 - Automatic
 - Open
 - Closed
 - P-iris
 - Day/Night Control:

- o Automatic
- o Manual
- o External
- Flicker Control:
 - o 60 Hz, 50 Hz
- White Balance:
 - o Automatic
 - o Manual
- Backlight Compensation: adjustable
- Image Rotation:
 - o 0°
 - o 90°
 - o 180°
 - o 270° including corridor mode
- Privacy Zones: up to 64
- Electronic Image Stabilization
- Digital Defog: adjustable/off

4. Network:

- Connectivity: 100BASE-TX
- Cabling: CAT-5e
- Connector: RJ-45
- ONVIF: Profile S, T, M and G
- Security:
 - o Password protection
 - o HTTPS encryption
 - o Digest Authentication
 - o WS Authentication
 - o User Access Log
 - o 802.1x port-based authentication
 - o FIPS 140-2 L1 (with optional camera license)
 - o Onboard FIPS 140-2 L3 certified TPM
 - o Secure Boot
 - o Signed and encrypted firmware
- Network Protocols Supported:
 - o IPv6 - Internet Protocol Version 6
 - o IPv4 - Internet Protocol Version 4
 - o HTTP - Hypertext Transfer Protocol
 - o HTTPS - Secure Hypertext Transfer Protocol
 - o SOAP - Simple Object Access Protocol
 - o DNS - Domain Name System
 - o NTP - Network Time Protocol
 - o RTSP - Real-Time Streaming Protocol
 - o RTCP - Real-Time Control Protocol
 - o RTP - Real-Time Transport Protocol
 - o TCP – Transmission Control Protocol
 - o UDP – User Datagram Protocol
 - o IGMPv3 - Internet Group Management Protocol v3
 - o ICMP - Internet Control Message Protocol
 - o DHCP - Dynamic Host Configuration Protocol
 - o Zeroconf
 - o HSTS – HTTP Strict Transport Security
 - o QoS – Quality of Service
 - o DSCP – Differentiated Services Code Point
 - o FTP – File Transfer Protocol
- Streaming Protocols Supported:
 - o RTP/UDP
 - o RTP/UDP multicast
 - o RTP/RTSP/TCP
 - o RTP/RTSP/HTTP/TCP
 - o RTP/RTSP/HTTPS/TCP
 - o HTTP

- o S RTP
 - Device Management Protocols:
 - o SNMP v2c
 - o SNMP v3
- 5. Peripherals:
 - USB Port 2.0
 - Onboard Storage:
 - o Two microSD / microSDHC / microSDXC slots
 - o Video speed class card required; Class V10 or better recommended.
- 6. Auxiliary I/O:
 - Audio Compression Method:
 - o G.711 PCM 8 kHz
 - o Opus
 - Audio Input/Output: line level input and output
 - External I/O Terminals:
 - o 1 x relay in
 - o 1 x relay out
 - o 1 x 12 VDC out at 50 mA
 - Microphone: built-in for audio analytics with physical disable switch
- 7. Mechanical (Short Bullet):
 - Dimensions (L x W x H): 12.23" x 5.23" x 5.23" (311 mm x 133 mm x 133 mm)
 - Weight: 4.65 lbs (2.11 kg)
 - Body: Polycarbonate and aluminum
 - Housing: Backbox mount
 - Finish:
 - o High polished plastic injection mold
 - o Powdercoat grey
 - o Pantone 427C
 - Adjustment Range:
 - o Hinge: +/- 90°
 - o Rotation: +/- 175°
- 8. Electrical (Short Bullet):
 - Power Consumption: 25W max
 - Power Source:
 - o PoE: IEEE 802.3af Class 3
 - o PoE+: IEEE 802.at Class 4
 - IR Illuminator Behavior:
 - o PoE:
 - Above 140 °F (60 °C) IR will be disabled.
 - Between 23 °F (- 5 °C) and 131 °F (55 °C) IR operates at 30% power.
 - Below -4 °F (-20 °C) IR operates at 10% power.
 - Hysteresis at 9 °F (5 °C).
 - o PoE+ or Aux Power:
 - Above 140 °F (60 °C) IR will be disabled.
 - Between 122 °F (50 °C) and 140 °F (60 °C) IR operates at 50% power.
 - Below -4 °F (-20 °C) IR operates at 50% power.
 - Hysteresis at 9 °F (5 °C).
 - External Power: 12-24 VDC +/- 10%
 - RTC Backup Battery: 3V manganese lithium
 - Memory:
 - o 4GB RAM
 - o 4GB flash
 - Redundant Power: Seamless failover between PoE and Aux and back without interrupt in camera operation (for H6X only)
- 9. Environmental:
 - Operating Temperature: -58°F to 149°F (-50°C to 65°C)
 - Startup Temperature: -40°F to 149°F (-40°C to 65°C)
 - Absolute Maximum Temperature: 165°F (74°C) per NEMA TS2 (Temp.) para 2.2.7.2 - 2.2.7.7

- Storage Temperature: 14°F to 158°F (-10°C to 70°C)
 - Humidity: 0-100% non-condensing
10. Certifications:
- Certifications/Approvals:
 - UL, cUL, CE, ROHS, RCM, UKCA, NOM, KC, BIS
 - Safety Standards:
 - UL 62368-1
 - CSA 62368-1
 - IEC/EN 62368-1
 - IEC 62471
 - Environmental Standards/Ratings:
 - IEC 60529
 - IP66
 - IP67,
 - IP68 (1.8m depth for 2 hours)
 - IPX9K
 - NEMA 4X
 - IEC 60068-2 Shock & Vibration
 - NEMA TS2 Sec 2.2.7-2.2.9,
 - IK10
 - Electromagnetic Emissions Standards:
 - FCC Part 15 Subpart B (Class B)
 - ICES-003 (Class B)
 - EN 55032 (Class B)
 - EN 61000-6-3
 - EN 61000-3-2
 - EN 61000-3-3
 - EN 50121-4
 - EN 50130-4
 - Electromagnetic Immunity Standards:
 - EN 55035
 - EN 61000-6-1
 - EN 50121-4
 - EN 50130-4
 - Warranty: Limited 5 year
11. Supported Analytic Events:
- Object in Area
 - Object Loitering
 - Object Crossing Beam
 - Object Appears in Area
 - Object Not Present in Area
 - Object Enters Area
 - Object Leaves Area
 - Object Stops in Area
 - Object too Close
 - Direction Violated
 - Smart Motion Rule
 - Tamper Detection
 - Crowd Size
 - Unusual Crowd Growth
 - Unusual Crowd Size
12. Supported Classified Object Types:
- Outdoor Mode:
 - Vehicle Sub-types:
 - Car
 - Pickup Truck
 - Large Truck
 - Van
 - Motorcycle
 - Bus
 - Person
 - Indoor Mode: person

Approved Recording Server: Avigilon AI NVR 2

Description: The recording server shall be the Avigilon AI NVR 2 cloud-ready enterprise hardened recorder with AI. No substitutions will be accepted.

4.1.9 System Integration

- The IP Video Surveillance System shall have the ability to integrate with the District's existing] Access Control System consisting of approximately 162 doors [if applicable].
- The IP Video Surveillance System shall have the ability to integrate with the District's existing Motorola Solutions handheld two-way Land Mobile Radio system.

7 BIDDER ACKNOWLEDGEMENT

This Acknowledgement attests to the Bidder's awareness and agreement to the content of this RFP and all accompanying calendar schedules and provisions contained herein.

The Bidder must ensure that the following acknowledgement is duly completed and correctly executed by an authorized officer of the company.

This proposal is submitted in response to RFP #2526-06 IP Video Surveillance System Upgrade issued by Gregory-Portland ISD. The undersigned is a duly authorized officer, hereby certifies that:

(Bidder/Installer/Systems Integrator/Partner Name)

Agrees to be bound by the content of this proposal and agrees to comply with the terms, conditions, and provisions of the referenced RFP and any addenda thereto in the event of an award. Exceptions are to be noted as stated in the RFP. The proposal shall remain in effect for a period of [60] calendar days as of 04/20/2026.

The undersigned further certify that their firm (check one):

IS

IS NOT

currently debarred, suspended, or proposed for debarment by any federal entity. The undersigned agree to notify Gregory-Portland ISD of any change in this status, should one occur, until such time as an award has been made under this procurement action.

Person(s) authorized to negotiate on behalf of this firm for purposes of this RFP are:

Name: _____ Title: _____

Signature: _____ Date: _____

Name: _____ Title: _____

Signature: _____ Date: _____

Signature of Authorized Officer:

Name: _____ Title: _____

Signature: _____ Date: _____

EXHIBIT “A”: NOTICE OF INTENTION

RFP #2526-06 IP Video Surveillance System Upgrade

Gregory-Portland Independent School District

Bidder’s Company Name: _____

Authorized Representative: _____

Address: _____

Telephone Number: _____

E-Mail: _____

Please state your intention regarding the Request for Proposal “**RFP #2526-06 IP Video Surveillance System Upgrade**” issued by **Gregory-Portland ISD** by selecting one of the following:

Bidder ‘Intends to Respond’ to the **Gregory-Portland ISD** Request for Proposal.

Bidder ‘Does Not Intend to Respond’ to the **Gregory-Portland ISD** Request for Proposal.

EXHIBIT “B”: PROPOSED VIDEO SURVEILLANCE CAMERA SCHEDULE AND NETWORK ROOM SCHEDULE

RFP #2526-06 IP Video Surveillance System Upgrade

Gregory-Portland Independent School District

[Insert Complete Camera Schedule/BOM and Network Room Schedule here]

EXHIBIT “C”: BUILDING FLOORPLANS, DRAWINGS AND DEVICE LOCATIONS

RFP #2526-06 IP Video Surveillance System Upgrade

Gregory-Portland Independent School District

[Insert Individual Building Floorplan Graphics or Drawings with Camera Locations here]

EXHIBIT “D”: SAMPLE INSURANCE REQUIREMENTS FOR INSTALLER/SYSTEMS INTEGRATOR/PARTNER

RFP #2526-06 IP Video Surveillance System Upgrade

Gregory-Portland Independent School District

I. Notwithstanding any terms, conditions or provisions, in any other writing between the parties, the Installer/Systems Integrator/Partner hereby agrees to effectuate the naming of the customer's business as an additional insured on the Installer/Systems Integrator/Partner's insurance policies.

- II. The policy naming **Gregory-Portland ISD** as an additional insured entity shall:
- Be an insurance policy from an A.M. Best rated A- XII or better.
 - List **Gregory-Portland ISD** as an additional insured via an Installer/Systems Integrator/Partner's additional insured endorsement or its equivalent.
 - Have that organization's coverage as primary and non-contributory coverage for **Gregory-Portland ISD**, its Board, employees and volunteers.

III. The Installer/Systems Integrator/Partner agrees to indemnify the customer for any applicable deductibles and self-insured retentions.

IV. Required Insurance:

- Commercial General Liability Insurance
\$1,000,000 per occurrence/ \$2,000,000 aggregate.
- Auto Liability Insurance
\$1,000,000 combined single limit.
- Excess Insurance
\$1,000,000 each occurrence and aggregate on a “follow-form” basis.
- Workers' Compensation Insurance
\$500,000/500,000/500,000 Employers Liability Limits.
- Property Insurance
Coverage for Installer/Systems Integrator/Partner's property, tools and equipment is the responsibility of the Installer/Systems Integrator/Partner.

V. The Installer/Systems Integrator/Partner must provide **Gregory-Portland ISD** with a certificate of insurance and additional insured endorsement, with evidence that the above requirements have been met. Installer/Systems Integrator/Partner acknowledges that failure to obtain such insurance on behalf of **Gregory-Portland ISD** constitutes a material breach of contract and subjects it to liability for damages, indemnification, and all other legal remedies available to the customer.

VI. At **Gregory-Portland ISD's** request, the Installer/Systems Integrator/Partner shall provide a copy of the declaration page of the liability policy with a list of endorsements. If so requested, the Installer/Systems Integrator/Partner will provide a copy of the policy endorsements.

ATTACHMENTS (REQUIRED)

The following must be completed and returned:

Exhibit A, B, C, D

- Attachment A – Certification by Proposer

- Attachment B – Statement of Work
- Attachment C – Lobbying/Debarment Certification
- Attachment D – (If applicable)
- Attachment E – References
- Attachment F – Insurance Certificate
- Attachment G – W-9
- Attachment H – Conflict of Interest (Form 1295)
- Attachment I – CIQ Form
- Attachment J – Felony Conviction Notice
- Attachment K – Non-Collusion Statement
- Attachment L – State Assessment Certification

SUBMISSION ADDRESS

- Gregory-Portland Independent School District
Attn: Chris Casarez
1200 Broadway Ave.
Portland, TX 78374
- Phone: (361) 777-1091 ext. 1039

ATTACHMENT A
CERTIFICATION BY PROPOSER

II. DESCRIPTION OF SERVICES PROVIDED

Gregory-Portland ISD is seeking qualified vendors to deliver Occupational Services.

Provide scope of work or proposal which your firm would make available to the District.

Within _____ days of notice to proceed you will be able to begin the delivery of services.

What capacity or expertise does your organization have in the delivery of these services? (Attach any documentation deemed necessary).

III. SIGNATURE

Signature of Respondent: _____

Date Proposal Form Submitted: _____

Incomplete responses received after the deadline will not be considered.

Responses should be mailed or delivered to:

Gregory-Portland Independent School
District Attention: Chris Casarez
1200 Broadway Ave.
Portland, TX, 78374

Phone# (361) 777-1091 x-1039

ATTACHMENT B

Services Proposal Form

We propose to enter into contract with Gregory-Portland ISD for the delivery of requested Occupational Services at designated District facilities in accordance with the specifications in this proposal, for the prices set forth below.

We have carefully reviewed, and understand, the terms, conditions, and specifications, of the requested services. We understand that Gregory-Portland ISD reserves the right to reject any or all proposals and to waive any informalities in the proposal, and to award the contract in the best interests of Gregory-Portland ISD.

Indicate any additional services your organization is able to provide to the District. _____

PRINT NAME: _____

Company: _____

By: _____
(signature) (Title) (date)

Attach any other documents required detailing the proposed Scope of Work or your service offerings. Please feel free to attach any brochures or literature which you feel best represents the capacities and capabilities of your organization to the deliver the requested services.

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 sub-contracts, 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 30 17), 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, 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 30 17), 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:

- (a) 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;
 - (b) 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 inlposed on employees for drug abuse violations in the workplace;
 - (c) Providing each employee with a copy of the Contractor 's policy statement;
 - (d) 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;
 - (e) Notifying the District within ten days of Contractor's receipt of a notice of a conviction of an employee; and,
 - (f) Taking appropriate personnel action against an employee convicted of violating a criminal drug statute or require such employee to participate in a drug abuse assistance or rehabilitation program.
-

Further Certifications:

The undersigned contractor further certifies that contractor will abide by all State and federal laws applicable to the provision of its services, activities or programs to the District, including but not limited to, the Americans with Disabilities Act, 42 USC §12111, *et seq.*, 29 CFR §1630, *et seq.*; Section 504 of the 1973 Rehabilitation Act, 34 CFR §104.1, *et seq.*; the Family Educational Rights and Privacy Act, 20 USC §1232g, *et. seq.*, 34 CFR §99.1, *et seq.*; Title IX of the Education Amendments of 1972, 20 USC §1681 *et seq.*, 34 CFR §106.1 *et seq.*; Copeland Anti-Kickback Act, 18 USC §874 as supplemented in 29 CFR Part 3; 34 CFR Part 76 (State-Administered Grant Programs); 34 CFR Part 75 (Direct Grant Programs); and any applicable federal, State, local and private grant requirements.

All of the above certifications in this Attachment C 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 into this transaction.

Name and Title of Authorized Representative

Signature

ATTACHMENT E

REFERENCES

Please indicate all required Point of Contact information requested

Name of Company: _____

Address of Reference: _____

Point of Contact: _____

Phone: _____

Email: _____

Name of Company: _____

Address of Reference: _____

Point of Contact: _____

Phone: _____

Email: _____

Name of Company: _____

Address of Reference: _____

Point of Contact: _____

Phone: _____

Email: _____

CONFLICT OF INTEREST QUESTIONNAIRE

For vendor doing business with local governmental entity

A complete copy of Chapter 176 of the Local Government Code may be found at <http://www.statutes.legis.state.tx.us/Docs/LG/htm/LG.176.htm>. For easy reference, below are some of the sections cited on this form.

Local Government Code § 176.001(1-a): "Business relationship" means a connection between two or more parties based on commercial activity of one of the parties. The term does not include a connection based on:

- (A) a transaction that is subject to rate or fee regulation by a federal, state, or local governmental entity or an agency of a federal, state, or local governmental entity;
- (B) a transaction conducted at a price and subject to terms available to the public; or
- (C) a purchase or lease of goods or services from a person that is chartered by a state or federal agency and that is subject to regular examination by, and reporting to, that agency.

Local Government Code § 176.003(a)(2)(A) and (B):

(a) A local government officer shall file a conflict-of-interest disclosure statement with respect to a vendor if:

(2) the vendor:

(A) has an employment or other business relationship with the local government officer or a family member of the officer that results in the officer or family member receiving taxable income, other than investment income, that exceeds \$2,500 during the 12-month period preceding the date that the officer becomes aware that

- (i) a contract between the local governmental entity and the vendor has been executed; or
- (ii) the local governmental entity is considering entering into a contract with the vendor;

(B) has given to the local government officer or a family member of the officer one or more gifts that have an aggregate value of more than \$100 in the 12-month period preceding the date the officer becomes aware that:

- (i) a contract between the local governmental entity and the vendor has been executed; or
- (ii) the local governmental entity is considering entering into a contract with the vendor.

Local Government Code § 176.00G(a) and (a-1)

(a) A vendor shall file a completed conflict of interest questionnaire if the vendor has a business relationship with a local governmental entity and:

- (1) has an employment or other business relationship with a local government officer of that local governmental entity, or a family member of the officer, described by Section 176.003(a)(2)(A);
- (2) has given a local government officer of that local governmental entity, or a family member of the officer, one or more gifts with the aggregate value specified by Section 176.003(a)(2)(B), excluding any gift described by Section 176.003(a-1); or
- (3) has a family relationship with a local government officer of that local governmental entity.

(a-1) The completed conflict of interest questionnaire must be filed with the appropriate records administrator not later than the seventh business day after the later of:

(1) the date that the vendor:

- (A) begins discussions or negotiations to enter into a contract with the local governmental entity; or
- (B) submits to the local governmental entity an application, response to a request for proposals or bids, correspondence, or another writing related to a potential contract with the local governmental entity; or

(2) the date the vendor becomes aware:

- (A) of an employment or other business relationship with a local government officer, or a family member of the officer, described by Subsection (a);
- (B) that the vendor has given one or more gifts described by Subsection (a); or
- (C) of a family relationship with a local government officer.

FELONY CONVICTION NOTICE

Texas Education Code, Section 44.034, Notification of Criminal History, Subsection (a) states, "a person or business entity that enters into a contract with a School District must give **advance notice** to the District if the person or owner or operator of the business entity has been convicted of a felony." The notice must include a general description of the conduct resulting in the conviction of a felony.

Subsection (b) states, "a school District may terminate a contract with a person or business entity if the District determines that the person or business entity failed to give notice as required by Subsection (a) or misrepresented the conduct resulting in the conviction." The District must compensate the person or business entity for services performed before the termination of the contract.

I, the undersigned agent for the firm named below, certify that the information concerning notification of felony conviction has been reviewed by me and the following information furnished is true to the best of my knowledge.

Vendor's Name _____

Authorized Company
Official's Name (please print) _____

A. My firm is not owned or operated by anyone who has been convicted of a felony.

Signature of Company Official _____ Date: _____

B. My firm is owned or operated by the following individual(s) who has /have been convicted of a felony.

Name of Felon(s) _____

Details of Conviction(s) _____

Signature of Company Official _____ Date: _____

C. My firm is a publicly owned, Stock-exchange Corporation; therefore, this reporting requirement is not required.

Signature of Company Official _____ Date: _____

Suspension or Debarment Certificate

Non-Federal entities are prohibited from contracting with or making subawards under covered transactions to parties that are suspended or debarred or whose principals are suspended or debarred. Covered transactions include procurement for goods or services equal to or in excess of \$100,000.00. Contractors receiving individual awards for \$100,000.00 or more and all subrecipients must certify that the organization and its principals are not suspended or debarred.

By submitting this offer and signing this certificate, the bidder:

Certifies that the owner/operator has not been convicted of a felony except as indicated on a separate attachment to this offer, in accordance with Section 44.034, Texas Education Code, and

Certifies that no suspension or disbarment is in place, which would preclude receiving a federally funded contract under the Federal 0 MB, A-102, Common Rule (_ .36)

Vendor Name _____

Authorized Company Official's Name _____

Signature of Company Official _____ Date _____

Vendor E-mail Address

Vendor Telephone Number _____

ATTACHMENT L

STATE ASSESSMENT CERTIFICATION

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

The corporation certifies that:

It 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.

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

Name and Title of Authorized Representative

Signature

