

DIVISION 28 – ELECTRONIC SAFETY AND SECURITY

28 20 00 Electronic Surveillance

28 23 00 Video Surveillance

28 23 13 Video Surveillance Control and Management Systems

28 23 16 Video Surveillance Monitoring and Supervisory Interfaces

28 23 19 Digital Video Recorders and Analog Recording Devices

28 23 23 Video Surveillance Systems Infrastructure

28 23 26 Video Surveillance Remote Positioning Equipment

28 23 29 Video Surveillance Remote Devices and Sensors

PART 1 GENERAL

1.01 SUMMARY

1. This section includes the minimum requirements for a Managed Video Software as a Service platform comprised of, but not limited to, the following components:
 - A. Network Video Management Server(S)
 - B. Remote Workstation(S)
 - C. Remote Client Software Applications
 - D. Network Video Management Software
 - E. Online Web Services
2. References
 - A. 28 23 13 Video Surveillance Control and Management Systems
 - B. 28 23 19 Digital Video Recorders and Analog Recording Devices
 - C. 28 23 23 Video Surveillance Systems Infrastructure
 - D. 28 23 29 Video Surveillance Remote Devices and Sensors

1.02 SUBMITTALS

1. Manufacturers data sheets in digital or printed form
2. Manufacturers installation and operations manuals in digital or printed form

1.03 QUALIFICATIONS

1. Manufacturer
 - A. Manufacturer shall have been in business for more than 10 years
2. Installer
 - A. All installation, configuration, setup and related work shall be performed by an authorized technician designated as “Certified” or “Premier Certified” by the manufacturer

- B. All installation shall be performed by a technician licensed to install and service video surveillance and security equipment as mandated by the authority having jurisdiction

1.04 WARRANTY AND SUPPORT

1. A manufacturer warranty shall be available for a period of no less than 2 years against all defects in materials and workmanship
2. The manufacturer shall offer 1-year advanced replacement on all hardware products and make available an optional second year advance replacement for purchase
3. Software updates and patches shall be available free of charge during any active software subscription or Web Services subscription period

- END OF SECTION -

PART 2 PRODUCTS

2.01 ARCHITECTURE

1. The installed hardware and software solution shall collectively function as a Managed Video Surveillance Platform (MVSP)
2. The MVSP shall allow seamless management of all Network Video Management Servers, Client Applications, Network Video Management Software and Network Video Devices across multiple locations through a central Web Services Portal.
3. The MVSP shall be capable of being sourced from a single manufacturer with components to include but not be limited to:
 - A. Network Video Management Server(s)
 - B. Remote Workstation(s)
 - C. External Storage Array(s)
 - D. Client Applications
 - E. Network Video Management Software (NVMS)
 - F. Online Web Services Management Portal (Web Service)
 - G. Network Video Devices
4. The MVSP shall support an API for 3rd party integration leveraging the platforms relay technologies including but not limited to:
 - A. Transmission of live video
 - B. Transmission of recorded video
 - C. Transmission of system events for real time notification
 - D. Export of recorded video
 - E. Export of recorded video snapshot images

2.02 NETWORK VIDEO MANAGEMENT SERVER(S)

1. The MVSP shall support multiple network video management server options from the same manufacturer as the NVMS.
 - A. Server options shall include but not be limited to models with:
 - i. Integrated PoE switch enabling Plug and Play operation
 - ii. Integrated AHD, TVI & CVI encoder video encoding
 - iii. Front removable drive bays
 - iv. Dual redundant SSD boot drives and RAID 5 storage arrays

2.03 CLIENT APPLICATION(S)

1. General
 - A. The MVSP shall include, but not be limited to, a Web Client, Desktop Client application, and Mobile Client application
 - B. The Web Client, Desktop Client application, and Mobile Client application shall all:
 - i. Authentic users based upon real-time credentials stored and managed in the Web Service
 - ii. Support two-step (multi-factor) authentication. The second authentication code shall be delivered to the user's mobile device via SMS text

- iii. Encrypt metadata transmitted to the Web Service using the Transport Layer Security (TLS) protocol
- iv. Support relay communication using the WebSockets protocol
- v. Support single sign on technology by automatically providing access to all NVMS instances based upon the user's real-time access rights stored and managed in the Web Service
- vi. Support 3rd party single sign on authentication through Azure AD, OKTA, SAML 2.0 and ADFS
- vii. Automatically receive NVMS site and connection information updates pushed in real time from the Web Service (NVMS connection information shall not be manually programmed within the client application)
- viii. Automatically display or hide menu options for live, search, export, and setup capabilities based upon the user permissions stored and managed in the Web Service and client feature set
- ix. Support WAN connectivity to the NVMS established via a secure session relayed through the Web Service
- x. Support WAN or LAN connectivity directly to the NVMS server's IP address providing the user with the option to bypass the Web Service when required
- xi. Enable the user to preview an image from each network video device displayed in the client's NVMS site list
- xii. Provide the following general video playback capabilities
 - a. The ability to playback video based upon a time and date selection
 - b. The ability to playback video based upon an event and duration of the event
 - c. The ability to playback video based upon a user configurable alert
 - d. The ability to playback video in multiple recorded stream resolutions
 - e. The ability to playback video in a digitally zoomed state
 - f. The ability to playback video forward and backwards
 - g. The ability to control video playback speed
 - h. The ability to step playback video forward and backward on a frame by frame basis
 - i. The ability to export a JPEG image
- xiii. Provide the following general live video viewing capabilities
 - a. The ability to view live video in multiple stream resolutions
 - b. The ability to view live video in a digitally zoomed state
 - c. The ability to view live video in a full screen state
 - d. The ability to view live video simultaneously from multiple network video devices

2. Web (Thin) Client

- A. The Web Client shall support the most current version of Google Chrome, Microsoft Edge (Chromium based), Opera and Mozilla Firefox for Windows

- B. The Web Client shall support the most current version of Apple Safari, Google Chrome and Microsoft Edge (Chromium based) for macOS
- C. The Web Client shall not require ActiveX, Flash, or other 3rd party plugin download in order to function
- D. The Web Client shall support localization in English, Spanish, French, Chinese and Korean
- E. The Web Client's live view interface shall provide the user with the following capabilities:
 - i. The ability to drag and drop streams from the network video device tree view to a video pane and from one video pane to another
 - ii. The ability to view up to three different video stream resolutions on a per network video device basis
 - iii. The ability to view video from up to 16 network video device streams in each browser window depending on the browser type
 - iv. The ability to select from a 4:3, 16:9, original, and stretch video viewing aspect ratio
 - v. The ability to select from multiple video grid viewing options
 - vi. The ability to view the following information in real time on a per network video device basis:
 - a. Stream resolution
 - b. Transmission codec
 - c. Bandwidth consumption
 - d. Viewing frame rate
 - vii. The ability to maintain viewing state (including digital zoom) when switching between the search or setup interface and when logging out and into the Web client
 - viii. The ability to control PTZ and presets from the live interface
 - ix. The ability to full screen the live interface
 - x. The ability to dewarp and view video streams from 360 network video devices
- F. The Web Client's video playback interface shall provide the user with the following capabilities:
 - i. Timeline information bar
 - a. The ability to view video data including motion events on a timeline information bar
 - b. The ability to zoom out to multiple days of video data and the ability to zoom in to view as little as 5 seconds of video data on the timeline information bar
 - c. The ability to preview a recorded video image when hovering over the timeline information bar

- ii. Thumbnail search
 - a. The ability to preview thumbnail images based on a timeline in increments of 25, 16, or 9
 - b. The ability to view thumbnail images at a specified time from a date range of up to 25 days
 - c. The ability to drill down to an actual video event by selecting a thumbnail image to reduce the time range interval
- iii. General search
 - a. The ability to playback video from up to 16 network video devices in a synchronized state depending on browser type
- iv. Event search
 - a. The ability to select start, end and duration of an event filter
 - b. The ability to select event type to filter
 - c. The ability to select all or individual event type options
 - d. The ability to display events type, source, date, time and duration
 - e. The ability to preview start, middle and end of an event
- G. The Web Client's video export interface shall provide the user with the following capabilities:
 - i. The ability to upload a digitally signed video clip to the Web Service in a format that does not require a proprietary video player
 - ii. The ability to download a digitally signed video clip to the user's local workstation in a format that does not require a proprietary video player
 - iii. The ability to specify a video quality level for video exports
 - iv. The ability to specify video resolution in either mobile compatible or original
 - v. The ability to export multiple channels of digitally signed video clips to Web Services and a user's local workstation in a format that does not require a proprietary player
 - vi. The ability to manage video exports in a single interface
 - vii. The ability to specify include audio if available on export
 - viii. The ability to export a JPEG to the user's local workstation
 - ix. The ability to export a proprietary multi-camera file as an archive with a standalone viewer available for download
- H. The Web Client's setup interface shall present the user with all NVMS configuration options
- I. The Web Client shall include quick link access to the Web Service for the purpose of quick connect, user management, and recorder management
- J. The Web Client shall include the following NVMS software update capabilities:
 - i. The ability to automatically notify users of any NVMS updates available
 - ii. The ability to view software release notes which shall be automatically displayed based upon the delta between the version installed and the current version available

- iii. One button execution of a NVMS update via the Web Service without the need to manually download or install the software
 - K. The Web Client shall provide a mechanism for the user to submit usability feedback, software bug reports, and feature requests including the ability to upload a reference file
 - L. The Web Client shall provide a mechanism for the user to view license agreements of third-party software used by the Web Client
- 3. Desktop (Thick) Client Application
 - A. The Desktop Client shall support the following connectivity capabilities when user authentication is initiated through the Web Service:
 - i. The ability to determine when a LAN connection is available and to automatically establish such connection
 - ii. The ability to determine when a peer to peer WAN connection is available and to automatically establish such connection
 - iii. The ability to determine when LAN and peer to peer WAN connection is not available and establish a relay connection with Web Services
 - B. The Desktop Client shall support a multi-monitor environment and shall include the following viewing capabilities:
 - i. The ability to open and configure independent application windows and tabs within the application windows across multiple monitors
 - a. The users viewing configuration shall be automatically reloaded when a user logs out and back into the Desktop Client application
 - ii. The ability to create screen layouts spanning multiple NVMS servers and to save them to the Web Service
 - iii. The ability to view shared screen layouts created by other users that have been saved to the Web Service
 - C. The Desktop Client's live view interface shall provide the user with the following capabilities:
 - i. The ability to simultaneously view video streams from multiple NVMS servers
 - ii. The ability to view NVMS server and network video device connection state
 - iii. The ability to drag and drop streams from the network video device tree view to a video pane and from one video pane to another
 - iv. The ability to view up to three different video stream resolutions per network video device
 - v. The ability to dewarp and view video streams from supported 360 network video devices
 - vi. The ability to view video streams from up to 81 network video devices in each independent application window
 - vii. The ability to select from an original, stretch, 4:3 and 16:9 video viewing aspect ratio
 - viii. The ability to select from multiple video grid viewing options

- ix. The ability to see the following information in real time on a per video stream basis
 - a. Stream resolution
 - b. Transmission codec
 - c. Bandwidth consumption
 - d. Viewing frame rate
 - x. The ability to maintain viewing state (including digital zoom) when switching between the search or setup interface and when logging out and into the Desktop Client
 - xi. The ability to control PTZ and presets from the live interface
 - xii. The ability to full screen the live interface
 - xiii. The ability to listen to live IP audio and control its volume
 - xiv. The ability to sequence live video in grid views
 - xv. The ability to search video in live view
 - xvi. The ability to utilize the systems GPU to decode live video
- D. The Desktop Client's video playback interface shall provide the user with the following capabilities:
- i. Timeline information bar
 - a. The ability to view video recording data including motion events on a timeline information bar
 - b. The ability to zoom out to multiple days of video data and the ability to zoom in to view as little as 5 seconds of video data
 - c. The ability to preview a recorded video image when hovering over the timeline information bar
 - d. The ability to select a visually identifiable range on the timeline information bar while previewing an image for the purpose of exporting a video clip
 - e. The ability to full screen the timeline search interface
 - f. The ability to utilize the systems GPU to decode search video
 - ii. Thumbnail search
 - a. The ability to preview thumbnail images based on a timeline in increments of 25, 16, or 9
 - b. The ability to view thumbnail images at a specified time from a date range of up to 25 days
 - c. The ability to drill down to an actual video event by selecting a thumbnail image to reduce the time range interval
 - d. The ability to full screen the thumbnail search interface
 - iii. General search
 - a. The ability to playback video streams from up to 81 network video devices from NVMS servers in a synchronized state
 - b. The ability to dewarp and view video streams from supported data from recorded 360 network video devices

- c. The ability to full screen the general search interface
 - d. The ability to playback recorded audio associated with an IP camera
 - iv. Event search
 - a. The ability to select start, end and duration of an event filter
 - b. The ability to select event type to filter
 - c. The ability to select all or individual event type options from multiple recorders
 - d. The ability to display events type, recorder, source, date, time and duration
 - e. The ability to preview start, middle and end of an event
 - f. The ability to display event results in thumbnails or a detailed view
 - v. Object search
 - a. The ability to select start, end and sensitivity of an event filter
 - b. The ability to select an individual camera
 - c. The ability to display a camera preview image in a video pane
 - d. The ability to click and drag in a video pane to create a motion region
 - e. The ability to display recorder, source, date, time and duration
 - f. The ability to preview start, middle and end of an event
 - g. The ability to display event results in thumbnails or a detailed view
 - vi. Archive Viewer
 - a. The ability to load proprietary archive files
 - b. The ability to playback multiple cameras from an archive simultaneously in a synchronized state
 - c. The ability to playback archives using timeline and thumbnail search
 - d. The ability to export MP4 or JPG files from an archive locally
- E. The Desktop Client's video export interface shall provide the user with the following capabilities:
 - i. The ability to upload a digitally signed video clip to the Web Service in a format that does not require a proprietary video player
 - ii. The ability to download a digitally signed video clip to the user's local workstation in a format that does not require a proprietary video player
 - iii. The ability to specify a video quality level for video exports
 - iv. The ability to specify video resolution in either mobile compatible or original
 - v. The ability to export multiple channels of digitally signed video clips to Web Services and a user's local workstation in a format that does not require a proprietary player
 - vi. The ability to manage video exports in a single interface
 - vii. The ability to specify include audio if available on export
 - viii. The ability to export a JPEG to the user's local workstation
 - ix. The ability to export a proprietary multi-camera file as an archive with a standalone viewer

- F. The Desktop Client's setup interface shall present the user with all NVMS configuration options
 - M. The Desktop Client shall include quick link access to the Web Service for the purpose of quick connect, user management, and recorder management
 - G. The Desktop Client shall include the following software update capabilities:
 - i. The ability to automatically notify users of any Desktop Client software updates available
 - ii. The ability to view software release notes which shall be automatically displayed based upon the delta between the version installed and the current version available
 - iii. One button execution of a Desktop Client software update via the Web Service without the need to manually download or install the software
 - H. The Desktop Client shall provide a mechanism for the user to submit usability feedback, software bug reports, and feature requests including the ability to upload a reference file
 - I. The Desktop Client shall provide a mechanism for the user to view license agreements of third-party software used by the Desktop Client
 - J. The Desktop Client shall provide a mechanism for the user to change localization to English, Spanish, French, Chinese or Korean
 - K. The Desktop Client shall provide a mechanism by which the user may grant system access to the NVMS technical support team
 - L. The Desktop Client shall include the capability to configure and operate PTZ presets
 - M. The Desktop Client shall be configurable as the local user interface on the NVMS Windows server
 - N. The Desktop Client shall provide the following map functionality
 - i. The ability to create a map using JPG, BMP, or PNG image formats
 - ii. The ability to create map groups
 - iii. The ability to add a camera icon or map link icon on a map
 - iv. The ability to display and interact with a map in a live grid view
 - v. The ability to save a map in a layout
 - vi. The ability to import or export a map configuration
 - O. The Desktop Client shall provide the following keyboard/joystick functionality
 - i. The ability to change video displayed in the live grid
 - ii. The ability to control and change position of PTZ cameras
 - iii. The ability to set and initiate PTZ presets
4. Mobile Client Applications
- A. The Mobile Client shall support the following connectivity capabilities when user authentication is initiated through the Web Service:
 - i. The ability to determine when a LAN connection is available and to automatically establish such connection
 - ii. The ability to determine when a peer to peer WAN connection is available and to automatically establish such connection

- iii. The ability to determine when LAN and peer to peer WAN connection is not available and establish a relay connection with Web Services
- B. The Mobile Client's live view video interface shall provide the user with the following capabilities:
- i. The ability to view video streams from a single NVMS server
 - ii. The ability to manually select the video stream resolution that will work best for the network connection
 - iii. The ability to view video from up to 6 (phone) or 16 (tablet) network video devices per viewing pane
 - iv. The ability to digital zoom when viewing a single network video device
 - v. The ability to maintain viewing state (including digital zoom) when switching between live view and search when viewing a single network video device
 - vi. The ability to control PTZ from the live interface
 - vii. The ability to switch to full screen view when mobile device is rotated
 - viii. The ability to select from multiple video grid viewing options
 - ix. The ability to listen to live IP audio
 - x. The ability to talk to live IP audio receiver
- C. The Mobile Client's video playback interface shall provide the user with the following capabilities:
- i. General search
 - a. The ability to playback video from up to 4 network video devices per pane in a synchronized state
 - b. The ability to playback recorded audio associated with a video stream
 - ii. Event search
 - a. The ability to select start, end and duration of an event filter
 - b. The ability to select event type to filter
 - c. The ability to select all or individual cameras and sensors
 - d. The ability to display events type, source, date, time and duration
 - e. The ability to preview start, middle and end of an event with a thumbnail image
- D. The Mobile Client's video export interface shall provide the user with the following video export capabilities:
- i. The ability to initiate the upload of one or more digitally signed video clips to the Web Service in a format that does not require a proprietary video player
 - ii. The ability to specify a video quality level for video exports
 - iii. The ability to specify video resolution in either mobile compatible or original
 - iv. The ability to specify including audio if available on export
- E. The Mobile Client shall include indicator when connection to Web Services is using relay connection
- F. The Mobile Client shall include snapshot ability to save a JPEG image of the current view to the mobile device

- G. The Mobile Client shall have the ability to notify users of Web Services alerts using Push Notifications
- H. The Mobile Client shall support localization in English, Spanish, French, Chinese and Korean

2.04 NETWORK VIDEO MANAGEMENT SOFTWARE (NVMS)

1. General
 - A. The NVMS shall be an enterprise class network video management solution
 - B. The NVMS shall be compatible to run on both a Linux and Windows operating system
 - C. The NVMS shall support operating in virtualized environments
 - D. The NVMS shall have the ability to pull licenses for registration through the cloud
 - E. The NVMS shall support onboard and IP sensor and relay
 - F. The NVMS shall support integration with 3rd party camera analytics
 - G. The NVMS shall support integration with 3rd party intrusion
2. The NVMS shall include following connectivity capabilities:
 - A. NAT technology for establishing connectivity with the Web Service
 - B. Support for WAN client relay connectivity established by the Web Service
 - C. Support for WAN client peer to peer connectivity established by the Web Service
 - D. Support for direct WAN client connectivity
 - E. Support for direct LAN client connectivity
 - F. The NVMS shall not require a DDNS or external IP address for client accessibility over a WAN
 - G. The NVMS shall not require inbound ports to be opened on the network firewall for client accessibility over a WAN without establishing a VPN connection
 - H. Support for network Proxy servers with null authentication
 - I. Support for UDP or TCP traffic and configuration of network video devices globally
3. The NVMS shall include the following video recording capabilities:
 - A. The ability to natively configure and process an algorithm for video motion detection on a per video stream basis and to record video based upon such motion detection
 - B. The ability to continuously record video using a primary stream and the ability to record a secondary stream when motion is detected
 - C. The ability to configure different recording durations on a per network video device and per stream basis
 - D. The ability to record video on pre-event and post-event basis
 - E. The ability to record video based on sensor, analytic and intrusion alarm events
 - F. The ability to set data retention duration per network video device
 - G. The ability to set a global maximum data retention
4. The NVMS shall include the following Network Video Device Management capabilities:
 - A. The ability to interface with any ONVIF Profile S or later network video device
 - B. The ability to interface with Arecont network video devices using native Arecont protocol with H.264
 - C. The ability to interface with Hanwha networking devices using native Hanwha analytics protocol
 - D. The ability to interface with Axis networking devices using native Axis protocol
 - E. The ability to interface with supported 360 network video devices
 - F. The ability to interface with supported video network encoders

- G. The ability to manually add a network video device via RTSP, ONVIF Profile S, Arecont, Vivotek, Hanwha and Axis
 - H. The ability to merge a video stream when a network video device is replaced
 - I. The ability to change stream resolution, frame rate, bitrate and GOP from within the NVMS interface
 - J. The ability to configure the following network video device image settings from within the NVMS when communicating via the ONVIF & AXIS protocol
 - i. Brightness
 - ii. Saturation
 - iii. Sharpness
 - iv. Contrast
 - v. White balance
 - vi. WDR
 - vii. IR
 - viii. Shutter speed
 - ix. Rotate
 - K. The ability to rename network video devices
 - L. The ability to search and discover network video devices located on the same network as the NVMS
 - M. When interfacing with network video devices of like brand to the NVMS manufacturer, the NVMS shall be capable of:
 - i. Accessing the network video device's native setup graphical user interface through the NVMS GUI over a WAN with Camera Link function
 - ii. Automatically search and discover network video devices across subnets independent from the NVMS
 - iii. Updating the network video device's firmware
 - iv. Auto authenticate to the devices default username and password
 - v. Support HTTP IP camera communication
 - N. The NVMS shall be compatible with a server that includes a built-in encoder for video device connectivity. When installed on compatible internal encoder enabled hardware, the NVMS shall be capable of:
 - i. Automatically detecting, displaying and recording video streams from network video devices of like brand on a plug and play basis
 - O. The NVMS shall be compatible with a server that includes a built in POE switch for network video device connectivity. When installed on compatible POE enabled hardware, the NVMS shall be capable of:
 - i. Automatically detecting, displaying, and recording video streams from network video devices of like brand on a plug and play basis
 - ii. Viewing network video device power consumption on a per port basis
 - iii. Cycling power to network video devices connected to the internal POE switch
5. The NVMS shall include the following Permissions & User Management capabilities:

- A. The NVMS shall interface with a Web Service for the purpose of managing user access and NVMS permissions on a centralized basis
 - B. The NVMS shall maintain a persistent connection with the Web Service for the purpose of updating its permissions and user access settings in real time
 - C. The NVMS shall locally cache its permissions and user access settings to support direct LAN or WAN client connections in the event connectivity with the Web Service is lost
 - D. The NVMS shall authenticate users before enabling system access and shall support two-step (multi-factor) authentication
 - E. The NVMS shall support role-based user groups with custom definable permissions and NVMS server access
 - F. The NVMS shall support hidden camera permissions
 - G. The NVMS shall include the following local NVMS level permissions:
 - i. Video
 - a. View Live Video
 - b. View Searchable Video
 - c. Export Video
 - d. View Hidden Cameras
 - e. Control PTZ
 - ii. Setup
 - a. Setup Configuration
 - H. When a permission is disabled it shall automatically be hidden from the associated user's client interface(s)
6. The NVMS shall be capable of uploading digitally signed video to the Web Service
7. The NVMS shall include a local graphical user interface (GUI) with the following capabilities:
- A. The local GUI shall support live video viewing
 - B. The local GUI shall support auto boot to live display
 - C. The GUI shall support auto sequence of live video
 - D. The local GUI shall support video playback
 - E. The local GUI shall support all NVMS configuration options
 - F. The local GUI shall support video, snapshot and archive export
 - G. The local GUI provide a mechanism by which the user may grant system access to the NVMS technical support team
 - H. The local GUI shall support localization for English, Spanish, French, Chinese and Korean
 - I. The local GUI shall support the ability to dewarp and view video streams from 360 "fisheye" network video devices
 - J. The local GUI shall support the ability to digital zoom when viewing a single network video device
8. The NVMS shall support public view monitors and shall include the following capabilities:
- A. When installed on a compatible server with dual monitor capability, the NVMS shall enable a secondary programmable and functionally independent live view display

- B. The NVMS shall support dedicated network decoding and display devices with LAN or WAN connectivity to the NVMS server
9. The NVMS shall include a cloud-based health monitoring and reporting solution with the following capabilities:
- A. The NVMS servers shall broadcast a heartbeat to the Web Service every 5 minutes for the purpose of health monitoring
 - B. The NVMS shall monitor the following system health metrics and shall broadcast any health alerts to the Web Service in real time:
 - i. Network video device connection status
 - ii. Video loss alerts
 - iii. No recording warnings
 - iv. Hard drive errors including RAID, SMART, and drive failure
 - v. Missing hard drive warnings
 - vi. Unexpected NVMS server restart
 - C. The NVMS shall broadcast the following information to the Web Service daily:
 - i. A daytime image from all network video devices
 - ii. A nighttime image from all network video devices
 - iii. The NVMS server's current video retention in days
 - iv. The NVMS server's projected video retention in days
 - v. The NVMS server's CPU, Memory, Disk read, Disk write
 - vi. Other health and performance metrics
10. The NVMS shall provide a mechanism for the user to submit usability feedback, software bug reports, and feature requests including the ability to upload a reference file
11. The NVMS shall include an Application Programming Interface (API) for the purpose of integrating third party applications
12. The NVMS shall integrate with an enterprise class point of sale and exception-based reporting software solution
13. The NVMS shall support localization in English, Spanish, French, Chinese and Korean
14. The NVMS shall include additional functionality and features as a result of integration with an online Web Service as outlined in the "Web Service" section

2.05 WEB SERVICE

1. The Web Service shall include the following connectivity capabilities:
 - A. Support for relaying connectivity between the NVMS and the clients
 - B. Automatically instruct the client applications to establish a LAN connection with the applicable NVMS server whenever available
 - C. Single click access to all NVMS servers based upon site information and user permissions that are updated in real time
2. The Web Service shall be the primary method of administering all NVMS permissions, user management capabilities, and NVMS server connection information. The Web Service shall include the following related capabilities:
 - A. The ability to create role-based user groups with customizable permissions and NVMS server access
 - B. The ability to create recorder groups with NVMS server access and user group level permissions
 - C. The ability to update all user access and permissions to NVMS servers in real time
 - D. The ability to update all user access and permissions to the Web Service in real time
 - i. When a Web Service permission is disabled it shall automatically be hidden from the associated user
 - E. The ability to push and update all NVMS server connection information to the client applications in real time
 - F. The ability to push shared layouts to the Desktop Client application in real time
 - G. The ability to grant network video device access
 - H. The ability to restrict network video device access. Restricting access will apply to all sensors and alerts associated with the restricted device.
3. The Web Service shall include a Videos page with the following capabilities:
 - A. The ability to receive and store video files transmitted from the NVMS
 - B. The ability for users to share video files to other users within their Web Services company
 - C. The ability for users to share video files to contacts outside of Web Services and create guest accounts
 - D. The ability to send a custom message when sharing a clip
 - E. The ability to set an expiration date for shared clips
 - F. The ability for viewing shared clips in any browser type by generating a custom URL that requires a username and password
 - G. The ability for users to write notes regarding video clip files in a private location that will be visible to Web Service users and in a public location that will be visible to non-system users
 - H. The ability for users to download video clip files
 - I. The ability for an administrator to view who a clip has been shared to, how many times it has been viewed, and how many times it has been downloaded
4. The Web Service shall include the following software update capabilities:

- A. The ability to automatically notify NVMS administrators of any NVMS updates available
 - B. The ability to view software release notes which shall be automatically displayed based upon the delta between the version installed and the current version available
 - C. One button execution of a NVMS software update via the Web Service without the need to manually download or install the software
 - D. The ability to manage software updates for all recorders added to Web Services without needing to connect to each recorder
5. The Web Service shall include the following health monitoring and reporting capabilities:
- A. The ability to notify individual users or user groups in real time with a Web Service generated email or push notification when:
 - i. Abnormal restart event is received from a NVMS server
 - ii. Motion event with a user definable duration and schedule is received from a NVMS server
 - iii. Sensor event with a user definable duration and schedule is received from a NVMS server
 - iv. Loss of connection to associated network video device event is received from a NVMS server
 - v. Return of connection to associated network video device event is received from a NVMS server
 - vi. Hard drive error event is received from a NVMS server
 - vii. Hard drive missing event is received from a NVMS server
 - viii. RAID drive removed event is received from a NVMS server
 - ix. RAID volume degraded or failed event is received from a NVMS server
 - x. Video recording has not met the user definable storage retention threshold configured per network video device
 - xi. Web Services detects a network video device has not reported back for a period that exceeds a user definable duration
 - xii. Web Services detects a network video device has not been recording for a period that exceeds a user definable duration
 - xiii. Area Armed/Disarmed event detected from an intrusion panel
 - xiv. Door Access event detected from an intrusion panel
 - xv. Panel Disconnected event detected from an intrusion panel
 - xvi. Intrusion Sensor Alarm event detected from an intrusion panel
 - xvii. Video analytics event detected from supported cameras
 - xviii. Audio analytics event detected from supported cameras
 - xix. Motion, Sensor, or Analytics events detected when an intrusion panel is armed
 - B. The ability to suppress sending notification emails by waiting a configured amount of time before sending additional notification emails
 - C. The ability to suppress sending notification emails by only sending a configured amount of notification emails per hour

- D. The ability to automatically generate the following online reports:
- i. NVMS Server Inventory report which contains:
 - a. NVMS server Web Services online status
 - b. NVMS server serial number
 - c. NVMS server name
 - d. Web Services end user account associated to NVMS server
 - e. NVMS server location
 - f. NVMS server MAC address
 - g. Web Services license start and end dates
 - h. NVMS server last connection date and time to Web Services
 - i. NVMS server software version
 - j. NVMS server operating system and image version
 - k. NVMS server model number
 - l. NVMS server license type
 - m. NVMS server channel count unlocked by license
 - ii. Camera Inventory report which contains:
 - a. Camera names
 - b. Camera manufacturer name
 - c. Camera model name
 - d. Camera firmware version
 - e. Camera event and continuous resolution
 - f. Camera event and continuous framerate
 - g. Camera event and continuous bitrate
 - h. Camera event and continuous GOP
 - i. Camera recording mode
 - j. Camera motion detection type
 - k. Camera auxiliary options (PTZ, Audio, 360, Analytics)
 - l. Camera IP Address
 - m. Camera MAC Address
 - n. Camera Integration ID
 - o. Camera recording retention in days per stream
 - p. Camera recording storage used on hard drive per stream
 - iii. Day/Night report which contains:
 - a. Installation reference images from day and from night for each associated network video device
 - b. Current image from day and from night for each associated network video device
 - iv. System Summary report which contains:
 - a. Account usage details
 - b. Current operational and health status
 - c. Current video retention in days
 - d. Video clip uploads, views and downloads status

- e. Geographical location of NVMS devices represented by a map
 - v. Thumbnail report which contains a thumbnail image from one or more user defined cameras from one or more user defined times.
 - vi. Trend report which contains a graphical view of one or more Alert Rules to effectively identify patterns and anomalies.
 - E. The ability to send users reminder emails that links to the Web Services online reports on a daily, weekly or monthly basis
 - F. The ability to designate elevated severity for configured notification types. When set to elevated, users can acknowledge the notification and Web Services will keep track of the user activity
 - G. The ability to display elevated notifications on a dashboard
 - H. The ability to provide users with web browser access to the following information in real time
 - i. A list of all associated NVMS servers and network video devices
 - ii. NVMS server model or serial number, and software revision
 - iii. NVMS health and alert history
 - iv. NVMS warranty and licensing status
 - v. NVMS server MAC address
- 6. The Web Service shall receive a grade of "A-" or better in a real-time security analysis performed by SSL Labs (<https://www.ssllabs.com/ssltest>)
- 7. The Web Service shall include the following cyber security and data protection capabilities:
 - A. Two-Step (multi-factor) authentication
 - B. All metadata transferred between the Web Service and the NVMS shall be encrypted using the transport layer security (TLS) protocol
 - C. Login credentials shall be stored by the Web Service in an encrypted format compliant with NIST standards
 - D. Backup data stored in the Web Service shall be encrypted using AES-256
 - E. Data stored on the Web Service shall be protected with 60 days of rolling online backups and a 30-day offline backup that is isolated from all public networks
 - F. Customer data shall be logically separated through a tenant isolation layer
 - G. Decommissioned servers shall be degaussed and physically destroyed using processes recommended by the Department of Defense and the NIST
 - H. Personnel with access to Web Service servers shall receive a thorough background check and all Web Service administrative actions shall be tracked
- 8. The Web Service shall be hosted in redundant data centers with the following certifications:
 - A. PCI DSS Level 1
 - B. SOC 1/ ISAE 3402, SOC 2, and SOC 3
 - C. MTCS Tier 3
- 9. The Web Service shall provide a mechanism for the user to submit usability feedback, software bug reports, and feature requests including the ability to upload a reference file
- 10. The Web Service shall offer user authentication and management through Azure AD, OKTA, SAML 2.0 and ADFS

11. The Web Service shall support localization in English, French, Spanish, Chinese and Korean
12. The Web Service shall have the ability to restrict connection to the NVMS server by connection method (Direct Connect, LAN Smart Forwarding, Peer to Peer, or Relay)
13. The Web Service shall have the ability to restrict connection to the NVMS server by client type
14. The Web Service shall have the ability to restrict connection to the NVMS server by IP Address range
15. The Web Service shall have the ability to force encrypted connections using Relay only connection type
16. The Web Service shall support the ability to enable remote support session with Bomgar service
17. The Web Service shall have the ability to receive and store configuration files from NVMS
18. The Web Service shall have the ability to enforce a password policy for all users of the company account

- END OF SECTION -

PART 3 EXECUTION

3.01 INSTALLATION

1. Installer shall comply with all instructions and best practices specified by the hardware and software manufacturer
2. Installer shall comply with all applicable state and local regulatory requirements

3.02 STORAGE

1. Equipment shall be stored in environmental conditions within the stated temperature and humidity ranges specified by the hardware manufacturer

3.03 COMMISSIONING

1. The manufacturer shall offer the option for factory pre-configuration of all hardware and software purchased from the manufacturer as an additional paid service
2. The manufacturer shall offer the option for remote or in person system commissioning as an additional paid service

- END OF SECTION -