Date: 24-04-2019

Network Video Recorder (NVR) A&E Specification
Construction Specifications Institute (CSI) edition

A&E Specification for Shield | Key™ NVRs

Prepared by:

Arxys

Headquarters:

Bridgette, Inc. DBA Arxys
435 W Bradley Ave, Suite C
El Cajon, CA 92020
U.S.A.
Phone: (619) 258-7800
Web: www.arxys.com

Specifications

This Architectural and Engineering Specifications document utilizes MasterFormat™ Titles and Numbers April 2018 Edition and SectionFormat™/PageFormat™ December 2009 Edition standards by the Construction Specifications Institute (CSI).

This document specifies the architectural/engineering and bid criteria for a premises-based networked Network Video Recorder including Video Management Software application.

Notes to Specifier

1. Where several alternative parameters or specifications exist, or where the Specifier has the option of inserting text, such choices are presented in **bold red text**.
2. Explanatory notes and comments are presented in red hidden text. To display the hidden text, see the Instructions at the end of this document.
3. Delete any item or paragraph that is not applicable to this project, renumber the paragraphs. Insert additional provisions as required for this project.

Document Disclaimer and Restrictions

Information in this document was current as of the time of publication, and subject to change without notice. For the most up-to-date information, visit www.Arxys.com

SECTION 28 05 19.15
NETWORK VIDEO RECORDER

[**Specifier Note:** Delete Specifier Notes and unused optional items in red.]

PART 1 GENERAL

1.1. SUMMARY

A. *Section includes:* Description, architectural and functional requirements, design criteria, data security requirements, operational capabilities, and computer equipment requirements for a Network Video Recorder.

B. *Compliance:* System equipment and installation shall comply with all provisions and requirements of this specification as well as all applicable national, state and local codes and standards.

C. Products Furnished **[OR]** Supplied But Not Installed Under This Section.

D. Products Installed But Not Furnished **[OR]** Supplied Under This Section.

E. Related Requirements:

1. Section 27 00 00 Communications (Division 27).

a. Section 27 05 00 Common Work Results for Communications.
[**SPECIFIER NOTE:** For general requirements that are common to more than one section in Division 27.]

1) Section 27 05 28 – Pathways for Communication Systems.

b. Section 27 10 00 – Structured Cabling.

1) Section 27 13 00 – Communications Backbone Cabling.

2) Section 27 15 00 – Communications Horizontal Cabling.

2. Section 28 00 00 Electronic Safety and Security (Division 28).

a. Section 28 05 00 – Common Work Results for Electronic Safety and Security.

b. Section 28 08 00 Commissioning of Electronic Safety and Security.
[**SPECIFIER NOTE:** For expanded requirements for commissioning, systems readiness checklists, and training.]

1) 28 08 11 Testing for Baseline Performance Criteria.

1.2. REFERENCES

A. Trademarks Used in This Document:

1. *Intel:* Intel®, Core™, Iris™, Xeon®.

2. *Microsoft:* Microsoft®, Active Directory®, SQL Server®.

3. *Milestone:* XProtect®, Milestone Husky™, Milestone Federated Architecture™, Milestone Interconnect™.

4. *PassMark Software:* PassMark®.

B. *Brand Names Used in This Document:*

1. Arxys®
2. Arxys® Shield | Key T4
3. Arxys® Shield | Key T8
4. Arxys® Shield | Key R12
5. Arxys® Shield | Key R12E
6. Arxys® Shield | Key R36E
7. XProtect® Corporate
8. XProtect® Expert
9. XProtect® Express+
10. XProtect® Professional+

C. *Abbreviations and Acronyms:*

1. AES: Advanced Encryption Standard.
2. AVC: Advanced Video Coding.
3. CNA: Converged Network Adaptor.
4. DES: Data Encryption Standard.
5. DVI: Digital Visual Interface.
6. DVR: Digital Video Recorder.
7. FCoE: Fibre Channel Over Ethernet.
8. FPS: Frames per Second.
9. GB: Gigabyte.
10. Gbit: Gigabit Ethernet (1000Mbps).
11. H.264/H.265: Video Compression Formats.
12. HD: High Definition video resolution of 1280 x 720 pixels.
13. HDMI: High-Definition Multimedia Interface.
14. HEVC: High Efficiency Video Coding.
15. HTTPS: Hyper Text Transfer Protocol Secure.
16. I/O: Input/Output.
17. iSCSI: Internet Small Computer System Interface.
18. IoT: Internet of Things.
19. IP: Internet Protocol.
20. ISO/IEC: International Organization for Standardization/International Electrotechnical Commission
21. JPEG: Joint Photographic Experts Group (image format).
22. LAN: Local Area Network.

23. MIP SDK: Milestone Integration Platform Software Development Kit.
24. MPEG: Moving Picture Experts Group (video format).
25. NAS: Network Attached Storage.
26. NAT: Network address translation.
27. NVR: Network Video Recorder.
28. ONVIF: Open Network Video Interface Forum.
29. PoE: Power over Ethernet.
30. PTZ: Pan-tilt-zoom.
31. RAID: Redundant Array of Independent Disks.
32. RTSP: Real Time Streaming Protocol.
33. SAN: Storage Area Network.
34. SATA: Serial Advanced Technology Attachment.
35. SSD: Solid-State Drive.
36. UHD: Ultra High Definition video resolution of 3,480 x 2,160 pixels.
37. UPnP: Universal Plug and Play.
38. UPS: Uninterruptible Power Supply.
39. VMS: Video Management Software.
40. WAN: Wide Area Network.

D. *Definitions:*

1. *Authentication:* Process that establishes the origin of information or determines an entity’s identity.
2. *Authorization:* Process that associates permission to access a resource or asset with a person and the person’s identifier(s) for the purpose of granting or denying access.
3. *Bit Rate:* Number of bits per time unit sent over a network.
4. *Contractor:* Firm selected by Owner and any of Contractor’s subcontractors, vendors, suppliers or fabricators, to perform work specified in these contract documents and supporting documentation. Contractor shall supply all equipment, labor, material and services necessary to complete the project construction in accordance with Contract Documents.
5. *Central Processing Unit (CPU):* General purpose electronic circuitry within a computer that carries out the instructions of a computer program, typically contained in a single integrated circuit chip.
6. *Graphics Processing Unit (GPU):* Specialized electronic circuit designed to rapidly manipulate images and accelerate the creation of video images in a video frame buffer intended for output to a display device, much more efficiently than can be done by general purpose computer CPUs. GPUs are used in mobile phones, personal computers, workstations and game consoles.
7. *Hardware Acceleration:* Use of computer hardware (such as a GPU) to perform some functions more efficiently than is possible in software running on a more general-purpose CPU.
8. *High Efficiency Video Coding (HEVC):* Video compression standard also known as H.265 and MPEG-H Part 2, one of several potential successors to the widely used AVC (H.264 or MPEG-4 Part 10). In comparison to AVC, HEVC offers about double the data compression ratio at the

same level of video quality, or substantially improved video quality at the same bit rate. It supports resolutions up to 8192×4320, including 8K UHD.

9. *Internet Small Computer System Interface (iSCSI):* SCSI protocol mapped to TCP/IP and run over standard Ethernet technologies.

10. *Kerberos:* Ticket-based network authentication protocol designed to provide strong authentication for client/server or server/server applications.

11. *Multicast:* Communication between a single sender and multiple receivers on a network.

12. *Multi-site:* Reference to a VMS system that spans multiple physical site locations.

13. *Open Network Video Interface Forum (ONVIF):* Global and open industry forum for the creation of standards for how IP-networked products within video surveillance and other physical security areas can communicate with each other.

14. *Passmark:* PassMark Software Pty Ltd is a privately-owned software development group headquartered in Sydney, Australia with a branch office in California, United States. PassMark provided CPU benchmarking software that provides a CPU Mark rating based upon a series of eight different tests. PassMark maintains the world’s largest CPU benchmarking website, cpubenchmark.net.

15. *Reseller:* Contractor authorized by manufacturer to furnish, install and maintain manufacturer’s NVR, who may be the primary contractor or a subcontractor for the provision of this project’s NVR system.

16. *Universal Plug and Play (UPnP):* Set of networking protocols that permits networked devices, such as personal computers, printers, Internet gateways, Wi-Fi access points, IP video cameras and mobile devices to seamlessly discover each other's presence on the network and establish functional network services for data sharing and communications.

1.3. SUBMITTALS

A. *Submission:* Submit under provisions of Section 01 30 00 - Administrative Requirements.

B. *Product Data:* Provide manufacturer's data sheets and installation manuals on each product to be used, including:

1. Preparation instructions and recommendations.
2. Storage and handling requirements and recommendations.
3. Installation methods.

C. *Shop Drawings:* Provide the following drawings.

1. Schematic of system components with physical space requirements.
2. System network topology diagram.
3. Connecting riser diagrams for all interfacing equipment.
   a. List of all equipment with part numbers.
   b. Locations for all components to be installed under this scope of work.

1.4. CLOSEOUT SUBMITTALS

A. *As-Built Drawings:* Provide original shop drawings modified to reflect changes made to comply with installation/configuration requirements and actual field conditions.

B. *Maintenance Contracts:* Submit a maintenance service agreement, including cost and services for a two-year period for Owner's review.

C. *Warranty Documentation:* Submit manufacturer's standard NVR warranty.

1.5. QUALITY ASSURANCE

A. Qualifications:

1. Manufacturer shall regularly and presently produce, as one of the manufacturer's principal products, the material, equipment and services specified for this project for commercial, military or industrial use.

2. *Contractors / Installers:*

   a. *Licensure:* Contractor or security sub-contractors shall be licensed to perform security installations in the state/region the work is to be performed if so required.

   b. *Experience:* Contractor or security sub-contractor shall have a minimum of three years of experience installing and servicing systems of similar scope and complexity**.**

   c. *Technician Certification:* Utilize only manufacturer-trained technicians to install, program, and service NVR equipment**.**

      1) Provide copies of system manufacturer certification for all technicians**.**

      2) Ensure technicians have a minimum of three continuous years of technical experience in electronic security systems, including IP networking and NVR solutions**.**

   d. *Dealer Certification:* Provide evidence that installing service company is an authorized dealer in good standing for the product's manufacturer, and that it meets the manufacturer's technical certification requirements.

1.6. DELIVERY, STORAGE AND HANDLING

A. Deliver materials in manufacturer's labeled packages. Store and handle in accordance with manufacturer's instructions and requirements.

1.7. SITE CONDITIONS

A. Ambient Conditions:

B. Existing Conditions:

1.8. WARRANTY

A. Manufacturer Warranty and Support:

1. *Hardware Warranty:*

   a. Warrant that hardware products are free from defect in materials and/or workmanship for a period of three years from the date of shipment.

   b. Warranty must include advanced parts replacement (APR) next business day (NBD) warranty support for a minimum of three years

   c. Warranty must be extendable to a full five years of advanced parts replacement (APR) next business day (NBD) warranty support

   d. Case Management online tool for submitting and tracking technical cases.

e.

2. *Software Warranty:*

    a. Manufacturer’s software warranty must be described in the manufacturer’s EULA for the product.

3. *Software Support:*

    a. Provide free access to any software service updates or hot fixes released due to a material defect or error in the product.

    b. Provide new device driver packs, multiple times per year, to extend support for additional devices without the need for a new version of the product.

    c. Provide free access to self-paced interactive e-training.

B. Contractor Warranty:

1. Fully warrant parts, materials and labor for a minimum of one year from date of the final acceptance of the NVR, including wiring, software, hardware and third-party products, including:

    a. Provision of all new software service releases during the warranty period.

    b. Provision of all new device driver packs.

2. Additional years of software upgrades shall be available for purchase separately. Coverage options shall include:

    a. Case Management online tool for filing and tracking technical cases.

    b. Direct Access to technical support via e-mail and phone.

    c. Prioritized handling of phone response times.

    d. Access to self-paced interactive user e-training.

C. Maintenance and Service:

1. *General Requirements:*

    a. Provide all services required and equipment necessary to maintain NVR in an operational state as specified for one year from formal written acceptance of system.

    b. Provide all necessary material required for performing scheduled adjustments or other non-scheduled work.

    c. Minimize impacts on facility operations when performing scheduled adjustments or other non-scheduled work.

2. *Description of Work:* Deployment of NVR includes installation and setup of NVR appliance hardware and software, plus any new and existing equipment specified in Article 2.1. OWNER-FURNISHED PRODUCTS.

3. *Schedule of Work:* Work shall be performed during regular workweek working hours, as determined by the deployment facility’s locale, excluding federal holidays.

4. *Emergency Service:*
[**SPECIFIER NOTE:** Use this article to describe owner requirements for Support Level Agreements (SLA). Delete if not applicable.]

a. Provide Owner with an emergency service center telephone number. Emergency service center shall be staffed 24 hours a day, 365 days a year and be located within 60 miles/kilometers of the deployment facility.

b. Owner shall initiate service calls whenever system is not functioning properly.

c. *Service Response:*

1) Owner has sole authority for determining catastrophic and non-catastrophic system failures.

2) Catastrophic system failure is defined as any system failure that Owner determines will place a facility at increased risk.

3) For catastrophic system failures, provide same-day four-hour service response with continued status updates at least every four hours.

4) For non-catastrophic failures, provide service response within eight hours with continued status updates at least twice a week.

5. *Verification of Operation:* As part of scheduled adjustments and repairs, verify operation of system as demonstrated by performance verification testing.

PART 2 PRODUCTS

2.1. OWNER-FURNISHED PRODUCTS

A. *New Products:*

1.

B. *Existing Products:*

1. [SPECIFIER: list existing products/systems furnished by owner, such as computers and network infrastructure, or delete paragraph B.]

2.2. MANUFACTURER

A. *Manufacturer:*

1. Arxys, Inc., 435 W. Bradley Avenue, Suite C, El Cajon, CA 92020 U.S.A.

a. Telephone: (619) 258-7800

b. Website: www.arxys.com

B. *Arxys Product Name*: Shield | Key.

C. *Substitution Limitations*: No Substitutions.

2.3. NETWORK VIDEO RECORDER SYSTEM

A. *Description:* High-performing server-class Network Video Recorder (referred to as “NVR”) system with component, storage and application redundancy for continuous uninterrupted operation, RAID protection. Hardware Accelerated Analytics, Hardware Accelerated Protection and Hardware Accelerated Encryption. Utilizing XProtect video management software, NVR offers proven capacity of 500 cameras with continuous recording, or 300 cameras with server-side motion detection, based on camera configuration to Full HD (1080p) video stream resolution at 25 frames per second and a data rate of 4 megabits per second. One or more PC or laptop workstations, or tablet or smartphone devices, provide user interface video management functionality via client software or web-based applications.

B. *System Architecture:* NVR system shall consist of:

1. *Appliance:* One or more NVR appliances containing:

a. Hardware Accelerated Analytics (HAA)

1) GPU based video decoding up to 4K

2) Server-side video motion detection

3) Metadata collection on motion

4) Smart motion search

b. Hardware Accelerated Protection (HAP)

1) Forensic-grade, zero frame loss 24/7 video recording

2) Double Drive Failure protection

3) Hardware XOR, Online Capacity Expansion & Patrol Read Repairs.

4) Enterprise Class hard drives

5) Engineered for 24/7 continuous operation

6) 2.5 million MTBF hours

7) Unrecoverable Bit Error Rate (UBER) of 1 in 10^15

8) Load / Unload Cycles - 600K

c. Hardware Accelerated Encryption (HAE)

1) Hardware Accelerated Advanced Encryption Standard (AES)

2) SSL/TLS certificate-based encryption

3) AES New Instructions (AES-NI) Set

d. Enterprise Class System

1) Remote management via IPMI including remote KVM

2) ECC protected DRAM

3) Intel Xeon Server CPUs, Iris Pro GPU

4) Microsoft Windows Server 2016

5) RAID protected, SSD based VMS storage

6) Storage expansion via SAS and iSCSI built-in

e. Hot-swap and redundant power supplies and cooling units

f. Rack-mountable in a standard rack with slide rails included

g. XProtect VMS software.

h. Uninterruptable power supply to be provided by Contractor.

2. *XProtect VMS Software Components:* A set of basic and failover Milestone XProtect server applications. Failover servers are intended for use on two or more networked NVRs.

a. *Management Server:* Central service component of the VMS responsible for handling system configuration, distributing the configuration to other system components, such as recording servers, and for facilitating user authentication.

b. *Failover Management Server:* Installation of the Management Server service in a Microsoft Windows Failover Cluster, or similar, which ensures that another server takes over the Management Server function, should the first server fail.

c. *Recording Server:* Service responsible for communications, recording and event handling for all devices (cameras, video and audio encoders, I/O modules, metadata sources, etc.).

d. *Event Server:* Service that handles various tasks related to events, alarms, maps and third-party integrations via the MIP SDK.

e. *Failover Event Server:* Implementation of Event Server service by installing Event Server in a Microsoft Windows Cluster, or similar, to ensure that another server takes over should the first server fail.

f. *Log Server*: Service that writes all VMS system, audit and rule-triggered log messages to database.

g. *Service Channel:* Service responsible for communicating the following:

1) Service and configuration messages to XProtect Smart Client.

2) Updates to a Smart Wall monitor layout.

3) Communicating that a specific Failover Recording Server is active.

h. *Milestone Mobile Server:* Service responsible for hosting the XProtect Web Client and for providing access to the VMS for XProtect Web Client and Milestone Mobile client users.

i. *Milestone ONVIF Bridge Server:* Optional server, including Milestone ONVIF Bridge service, Milestone RTSP Bridge service, and the Milestone ONVIF Bridge Manager, plus 64-bit plug-in for Management Client. This is to enable private-to-public video integration.

j. *Microsoft SQL Server:* Microsoft database server application for the Management Server, Event Server and Log Server services.

k. *Microsoft Active Directory (required for MFA):* Active Directory is not required for single-site systems but is recommended for cyber security purposes.

3. *PC or Laptop Workstations:* One or more PCs or laptops for Milestone XProtect client software applications intended to run on Windows-based PCs and laptops.

a. *Management Client:* The administration interface for all parts of the VMS, designed to be run remotely from, for example, an administrator’s computer.

b. *XProtect Smart Client:* Designed for day-to-day use by dedicated operators, to be run remotely on the operator’s computer. XProtect Smart Client provides dedicated task-oriented tabs for Live Video, Video Playback, Sequence Explorer, plus dockable tabs for System Monitor and Alarm Monitor. XProtect Smart Client supports definable keyboard and joystick button shortcuts for frequently-used actions, including window or camera selection.

c. *XProtect Web Client:* Browser-based application for the occasional or remote user that needs easy access to live video monitoring and audio listening with PTZ control including use of presets, and video and audio playback and export, with defined exports available for later usage or download.

4. *Tablets or Smartphones:* One or more tablets or smartphones using XProtect Web Client (see above) or Milestone Mobile client.

   a. *Milestone Mobile Client:* Native mobile app for smartphone or tablet users, for easy access to live and playback of cameras, and to activate system events and outputs. Additionally, for use as a remote recording device by using the mobile device's built-in camera, whereby video from the device's camera is streamed back to the VMS and recorded like a standard camera.

5. *Networks:*

   a. *Multiple Network Segments*: The VMS must support network segmentation into separate device, server and internet-connected networks.

   b. *Device Network:* Local network whose capacity and configuration are suitable for the level of video data transmission established by the system design and its intended usage.

   c. *Server Network:* Local network whose capacity and configuration are suitable for the level of video data transmission, systems integration, and user operations established by the system design and its intended usage.

   d. *Internet-Connected Network*: Internet-connected network providing connection to remote VMS sites and private-to-public connection via Milestone ONVIF Bridge. This network is also used for remote user access via the Milestone Mobile Server.

   e. *Network Traversal:*

      1) Enable software clients to access recording servers from outside a NAT firewall, by use of public addresses and port forwarding.

      2) Provide Remote Connect Services that enable secure remote connections to cameras across different types of private and public networks.

6. *Wide-Area Surveillance System:* Optionally one or more Husky NVRs and optional individual Milestone VMS servers connected to provide centrally managed surveillance operations across geographically dispersed sites. See paragraph 2.2 C Multi-System Architectures below.

C. *Multi-System Architectures:* Provide three architecture options for multi-site deployments:

1. *Distributed Recording Server Services:* Intended for sites with stable network connections between the central site and any number of remote sites. See Milestone Systems XProtect Corporate A&E specifications SECTION 28 23 00 PART 2 2.3 C.1 Distributed Recording Server Services.

2. *Milestone Federated Architecture:* Intended for sites with stable network connections between all sites, establishes central management of, and central surveillance operations for, geographically dispersed sites via one or more levels of parent/child system connections. See Milestone Systems XProtect Corporate A&E specifications SECTION 28 23 00 PART 2 2.3 C.2 Milestone Federated Architecture.

3. *Interconnected Architecture:* Suitable for providing central surveillance operations capabilities for a centrally XProtect Corporate-managed distributed system where some or all network connections between the local systems are unstable or intermittent, including vehicle mobile systems. See Milestone Systems XProtect Corporate A&E specifications SECTION 28 23 00 PART 2 2.3 C.3 Interconnected Architecture.

2.4. SYSTEM DESIGN CRITERIA

A. Computer Hardware Design Requirements:

1. *CPU Benchmark:* Utilize a motherboard CPU chip having a CPU PassMark rating of no less than 12,000.

2. *Hardware Accelerated Analytics:* Utilize a motherboard GPU chip that:

    a. Decodes H.265/HEVC video completely in hardware

    b. Supports video displays of up to 3840 x 2160 at 60 hertz.

    c. Includes Intel QuickSync version 5 video technology.

3. *Hardware Accelerated Protection:* Hardware XOR, Online Capacity Expansion & Patrol Read Repairs plus double drive failure fault tolerance with auto-rebuild.

4. *Hardware Accelerated Encryption with Secure Cryptoprocessor:* For compatibility with Owner and Manufacturer present and future cryptographic practices, provide a computer motherboard that contains a dedicated trusted platform module chip implementing TPM 2.0 (ISO/IEC 11889) functionality.

5. *OS and VMS Storage:* Utilize solid-state-drive storage to for high performance of the operating system and video management system software.

6. *Power Protection:* To protect NVR circuitry due in event of power supply failure resulting in excessive voltage, current or temperature, utilize hot-swap and N+1 redundant power supplies with over-voltage, over-current and over-temperature protection that performs power supply shutdown upon occurrence of such conditions.

B. *Computer Software Requirements:*

1. *Operating Systems:* Provide a 64-bit Microsoft Windows Server operating system version intended for embedded appliance use that contains a GUI interface.

2. *Windows Applications:* Provide server and client software applications that are native 64-bit Microsoft Windows applications.

3. *Mobile Device Applications:* Provide mobile device applications that are native applications for the mobile device operating system.

C. *Network Addressing:* Support both IPv4 and IPv6 addressing.

D. *Video Standards:* Provide simultaneous digital multi-channel live streaming and recording of video from IP cameras and IP video encoders with support for the following standards and options:

1. *Codecs:*

    a. H.264 and H.265.

    b. MPEG-4 and MPEG-4 ASP.

    c. MJPEG.

    d. MxPEG.

E. *Camera-Independent Motion Detection:* Provide real-time, camera-independent motion detection with:

1. *Configurable Sensitivity:* Configurable and automatic motion-detection sensitivity per camera.

2. *Searchable Metadata:* Searchable motion detection metadata created during motion detection.

3. *Exclusion Zones:* Multiple motion exclusion zones definable per camera to keep irrelevant motion from triggering recording.

F. *Multiple Language Support:* Provide support for multiple languages in these XProtect clients:

1. *Management Client User Interface:* American English, Chinese (Simplified), Chinese (Traditional), Danish, French, German, Italian, Japanese, Korean, Portuguese (Brazilian), Russian, Spanish, Swedish and Turkish.

2. *Management Client Built-In Help:* American English, Chinese (Simplified), French, German, Japanese, Korean and Portuguese (Brazilian).

3. *XProtect Smart Client, XProtect Web Client and Milestone Mobile Client User Interface:* American English, Arabic, Bulgarian, Chinese (Simplified), Chinese (Traditional), Croatian, Czech, Danish, Dutch, Farsi, Finnish, French, German, Hebrew, Hindi, Hungarian, Icelandic, Italian, Japanese, Korean, Norwegian (Bokmål), Polish, Portuguese (Brazilian), Russian, Serbian, Slovak, Spanish, Swedish, Thai and Turkish.

4. *XProtect Smart Client Built-In Help:* American English, Arabic, Chinese (Simplified), Chinese (Traditional), Czech, Danish, Dutch, French, German, Italian, Japanese, Korean, Polish, Portuguese (Brazilian), Russian, Spanish, Swedish and Turkish.

5. *XProtect Web Client and Milestone Mobile Client Built-In Help:* American English, Danish and Japanese.

G. *System Capacities:* Provide the following maximum capacities constrained only by the physical performance capabilities of selected hardware options and network infrastructure:

1. *Cameras:*

   a. 500 cameras with continuous recording.

   b. 300 cameras with server-side motion detection.

   c. For basis of camera capacity see 2.7 B.1.a Camera Configuration.

2. Unrestricted client software users.

3. Unrestricted user mobile devices.

4. Unrestricted client PCs or laptops.

5. Unrestricted NVR appliances.

6. Unrestricted system rules.

7. Unrestricted time profiles.

8. Unrestricted software client profiles.

9. Unrestricted video storage.

10. Recording rates of at least 25 frames per second per camera, limited only by hardware capabilities and number of cameras per NVR.

2.5. SYSTEM SECURITY

A. *Control and Information Security:* Provide the following data protection measures and user rights management capabilities in support of system confidentiality, integrity and availability:

1. *Device Data in Transit:*

   a. HTTPS connections from devices to Recording Server that support HTTPS connections.

   b. HTTPS connections from Recording Server to VMS clients, SDK clients and services that support HTTPS connections.

2. *Data at Rest Integrity and Encryption:* Provide encryption and digital signature settings per media storage container.

a. Two modes of video database encryption using AES-256 encryption:

1) *Light Encryption.* Encrypts only the first part of the MJPEG or MPEG-4/H.264 video, audio and metadata, to use less processing power for encrypting the video. Video cannot be decoded without the information contained in the encrypted header.

2) *Strong Encryption.* Encrypts all parts of the video, audio and metadata stored in the database.

b. Digital signing of media databases to establish a means of detecting modification of stored video, audio and metadata.

3. *Off-Premises Live and Recorded Video in Transit*: HTTPS connections from:

a. Mobile Server to browser-based XProtect Web Client and Milestone Mobile client app.

b. ONVIF Bridge to remote public systems.

4. *Data Integrity of Exported Video:*

a. Limiting viewing of recorded video to the XProtect Smart Client - Player application.

b. Per-export password protection for playback.

c. 56-bit DES, 128, 192 and 256-bit AES encryption.

d. Digital sign exported media with SHA-2 algorithm to establish a means of detecting modification of exported video.

e. XProtect Smart Client - Player's Verify Signatures function to validate authenticity of exported video recording.

5. *Digital Certificates Options:* Use of system default-generated or customer-provided digital certificates for connections to Mobile Server.

6. Data Access Control: Provide:

a. User profiles restricting device access and video viewing, playback and export, including by day and time-of-day.

b. Timestamped audit log of who logged in, viewed live or recorded video, or exported video.

7. *Device Discovery and Management:* Wizard function to automatically discover and upon approval add devices to system using Universal Plug and Play (UPnP) discovery, IP network range scanning, or manual device detection. Hardware wizard provides a few basic device management capabilities to support high device uptime (i.e. availability):

a. Swift replacement of malfunctioning devices with preservation of configuration settings and recordings, including those for attached cameras, microphones, speakers, inputs, outputs and metadata devices.

b. Moving of devices and attached devices between recording servers during runtime with no loss of settings, recordings, rules, permission, etc.

c. User ability to enable and disable devices for purposes of maintenance or temporary deactivation.

B. User Authentication:

1. *Log-in Options:* Log-in authentication via:

a. Microsoft Active Directory.

b. Local Windows user accounts.

c. Basic user system account (username and password credentials).

d. Dual authentication, a.k.a. two-person rule, requiring two verified persons to gain access.

2. *Auto-Log-In:* Use of last used credentials for authentication, with Auto-log-in and auto-restore of camera views.

3. *Kerberos Authentication:* Provide strong authentication via Kerberos support.

C. *Client Authentication:* Provide Management Server authentication and authorization of connecting clients (XProtect Smart Client, Management Client and MIP SDK clients) and use a session-limited access token for controlling access to the Recording Server.

D. *System Hardening:* System hardening guide that:

1. Describes data security, network security and physical security measures and best practices for securing the NVR and its VMS software against cyber-attacks. This includes security considerations for the hardware and software of servers, clients and network device components of a video surveillance system.

2. Incorporates standards-based and best-practice-based security and privacy controls and maps them to each hardening recommendation.

2.6. SYSTEM FUNCTIONALITY

A. Provide full NVR system functionality per specifications of the selected XProtect VMS software product.

B. XProtect software product options:

1. XProtect Corporate

2. XProtect Expert

3. XProtect Professional+

4. XProtect Express+

5. XProtect Essential+

2.7. NVR HARDWARE

A. *Hardware Options:*

1. *Shield | Key Units:*

a. Arxys Shield | Key R12E

b. Arxys Shield | Key R36E

B. *General Specifications:*

1. *Maximum Number of Cameras:*

a. *Camera Configuration:* Base camera capacity calculations on:

1) Video Image Resolution: HD (1080p).

2) Frame Rate: 25 frames per second.

3) Data Rate: 4 megabits per second.

b. *Continuous recording:* 500 cameras.

c. *Server-Side Motion Detection:* 300 cameras.

2. *Form Factor:*
    a. Shield | Key R12E: 2U rack-mount.
    b. Shield | Key R36E: 4U rack-mount.
3. *Dimensions:* Width x Height x Depth:
    a. 2U: 444mm(W) x 88mm(H) x 670mm(D) millimeters.
    b. 2U: 17 x 3.5 x 26.75 inches.
    c. 4U: 444mm(W) x 177mm(H) x 670mm(D) millimeters.
    d. 4U: 17 x 7 x 26.75 inches.

C. *Compute System:*

1. *CPU:*
    a. *Model:* Intel Xeon-E 3.6Ghz 8M Cache
    b. *CPU Passmark Rating:* 15,000.
2. *GPU:* Intel Pro Graphics P630.
3. *GPU Video Decoding:* Smart Client and server-side video motion detection.
4. *RAM: 32GB ECC DRAM*
5. *Credential and Key Encryption:* Trusted Platform Module (TPM 2.0).
6. *Operating System:* Windows Server 2016 Standard 64 bit

D. *Storage System:*

1. *Maximum Recording Rate:* 1,728 Mbps.
2. *Internal Video Storage:*
    a. *Hot-Swap HDD Drives:*
        1) *Type: Enterprise Class 7,200 RPM, 2.5M MTBF hours, 600k Duty Cycle*
        2) *Quantity:* 12 to 36.
        3) *RAID Level:* RAID 6.
3. *VMS/OS Storage:*
    a. *Type:* SSD Flash.
    b. *Quantity:* 2.
    c. *RAID Level:* RAID 1.
    d. *Raw Storage Capacity:* 250 GB.
4. *External Archiving:*
    a. *Standard:* NAS and SAN.
    b. *Optional via:* iSCSI and SAS

E. *Network System:*

1. *Network Interfaces:* Quantity x Type and Connector:
    a. *Standard:*

1) *Standard Port:* 2 x 1 GbE RJ45.

2) *Remote Management Port:* 1 x 1 GbE RJ45.

b. *Optional with 10Gb NIC*:

1) *High-Speed Port:* 2 x 10 GbE SFP+ including iSCSI.

2. *Remote Management Technology:*

a. *Type:* Intel Active Management Technology (AMT).

b. *Version:* 11.8.50 or above.

3. *Display Connections:*

a. *DVI:* Quantity: 1.

b. *HDMI:* Quantity: 2.

4. *USB Connections:*

a. *Type:* USB 3.0.

F. *Power System:*

1. *Power input:* 100~240V, 50/60 Hertz.

2. *Maximum Power Consumption:* 395 Watts.

3. *Redundancy:*

a. *Type:* Hot-swappable power supplies.

b. *Quantity:* 2.

4. *Protection:*

a. Over Voltage.

b. Over Current.

c. Over Temperature.

d. Short Circuit.

G. *Environmental:*

1. *Operating Temperature:* 0^0 – 40^0 Celsius, 32^0 – 104^0 Fahrenheit.

2. *Storage Temperature:* -20^0 – 70^0 Celsius, -4^0 – 158^0 Fahrenheit.

3. *Humidity:* 10 percent to 90 percent relative humidity (non-condensing).

H. *Regulatory Compliance:* CE (class A), WEEE, FCC (class A), RCM, UL, Mexico (CoC).

2.8. LICENSING

A. *License Activation:* NVR shall offer easy-to-use automatic or manual online activation via the Internet and alternatively, offline activation via email and web for closed surveillance networks.

B. *Server Base License:*

1. Require one mandatory XProtect VMS server base license for configuring the pre-loaded XProtect VMS available on the NVR.

C. *Hardware Device License:*

1. Require one license per hardware IP address to connect:

   a. Cameras.

   b. Audio devices.

   c. Video encoders.

   d. Other devices.

2. Support an unlimited number of hardware device licenses.

D. Licensing of Milestone Interconnect:

1. Require one Milestone Interconnect device license per camera in an interconnected site that is enabled in the central XProtect Corporate system.

2. Interconnect license shall be tied to the parent XProtect Corporate system showing the interconnected devices.

E. Licensing of Milestone Federated Architecture:

1. The use of Milestone Federated Architecture is free and not subject to licensing. This implies that unrestricted sites and licensed cameras can be included in the federated hierarchy, without the need for additional or special licenses.

F. *License Overview Information:* License overview shall include add-on products.

G. *License Administration:* Provide expanded license information for multi-site installations where both the total used licenses for the common base license is presented along with the license use in the specific system.

H. *Changes Without Activation:* A “Changes without activation” function shall allow additions and replacements of limited number of devices without requiring license device activation or reactivation.

PART 3 EXECUTION

3.1. EXAMINATION

A. Verification of Conditions:

1. Visit site and verify that site conditions are in agreement with design package. Report all changes to the site or conditions which will affect performance of the system to the Owner. Do not take any corrective action without written permission from the Owner.

2. *General:*

   a. Verify that existing site conditions are acceptable for product installation in accordance with manufacturer’s instructions.

   b. Verify that wire runs, related items, and conditions are ready to receive work of this Section.

3. *Cable and Wiring:*

   a. Examine pathway elements intended for cables. Check raceways, cable trays, and other elements for compliance with space allocations, installation tolerances, hazards to cable installation, and other conditions affecting installation.

b. Examine roughing-in for LAN and control cable conduit systems to PCs and other cable-connected devices to verify actual locations of conduit and back boxes before device installation.

4. *LAN / WAN:*

a. Verify LAN connections for server and workstation computers.

b. Provide access to the internet for the primary NVR server.

5. *Power Connections:*

a. Verify power circuits which are existing or have been previously installed under other sections are acceptable for product installation in accordance with manufacturer's instructions.

3.2. PREPARATION

A. Review configurable features of the NVR with the Owner's Representative and document the results of the meeting in the Project planning documents. The following configuration topics shall be resolved prior to configuring equipment and services:

1. Internet Service Provider, firewall, and IP schema for NVR devices.

2. Time server synchronization scheme for overall security system.

3. Plan for system testing, startup, and demonstration.

4. Acceptance test concept and, on approval, develop specifics of the test.

5. List of default user IDs and passwords (factory defaults) for NVR VMS application, servers and workstations.

B. Provide a schedule with a list of participants to attend monthly coordination and progress update meeting until job completion. Attendees shall include:

1. Owner's Representative of Facilities Management, Information Services, Security Management.

2. Contractor Project Manager.

3. Manufacturer(s) Employed Representative.

4. Architect / Engineer / Security Consultant.

C. At all coordination meetings with Owner's Representative, present Project planning documents and review, adjust, and prepare final setup documents. Use final documents to set up system software.

D. Owner's Representative and Owner shall assist in establishing procedural guidelines and in defining terminology and conditions unique to the Owner's operation.

E. Supervise installation to appraise ongoing progress of other trades and contracts, make allowances for all ongoing work, and coordinate the requirements of the installation of the Network Video Recorder.

F. Coordinate Owner installation or update of workstation operating system software and web browser software to a version as specified by the NVR provider.

G. Coordinate Owner-managed computer and network security practices as specified by the NVR provider.

3.3. INSTALLATION

A. Deploy NVR system in accordance with manufacturer’s deployment instructions, including workstation and integration instructions and requirements.

B. Collaborate with Owner’s Representative on the application of manufacturer’s hardening guide recommendations.

C. Supervise installation to appraise ongoing progress of other trades and contracts, make allowances for all ongoing work, and coordinate the requirements of the NVR installation.

D. *Drawings and Diagrams:*

1. System devices identified on building drawings are intended to generally indicate areas where such devices are to be located. Determine final location of these devices in accordance with Owner’s requirements.

2. Riser diagrams are schematic and do not show every conduit, wire box, fitting, or other accessories. Provide such materials as necessary for a complete and functioning installation.

E. Comply with manufacturer’s written data, including product technical bulletins, product catalog installation instructions and product carton installation instructions.

F. All firmware in products shall be the latest and most up-to-date provided by the manufacturer, or of a version as specified by the provider of the NVR to ensure approved integration compatibility.

G. Install, configure, and test NVR for complete and proper operation.

3.4. SITE QUALITY CONTROL

A. *Site Tests and Inspections:*

1. Submit documented test plan to Owner at least (14) days in advance of final acceptance test, inspection and check-off.

2. Perform acceptance reviews with Owner’s representative of camera and system configurations and their documentation.

3. Perform final acceptance testing in the presence of Owner’s representative, executing a point by point inspection against a documented test plan that demonstrates compliance with system requirements as designed and specified, including response times for control actions and sequences, and rules-based actions. Tests shall demonstrate the functionality of each individual device control item, including as camera alarm outputs and control relays.

4. Conduct acceptance tests in presence of Owner’s representative, verifying that each device point and sequence is operating correctly and properly reporting back to control panel and control center, and provide Owner’s Representative with written report of test results.

5. Specific tests shall be witnessed by Authorities Having Jurisdiction if necessary.

6. Consider NVR accepted only after all acceptance test items have been successfully checked-off.

   a. Beneficial use of part or all of the system shall not be considered as acceptance.

7. As required to sufficiently demonstrate the NVR functionality, request the console operator on duty and his/her superior to perform certain daily operations using the NVR.

8. Complete all required training prior to initiation of the final acceptance test.

9. Inspect the installation of all field computers and devices.

a. Point out general neatness and quality of installation, test the full functionality of each individual device, and show that mounting, backbox and conduit meet compliance requirements.

10. Owner’s Representative shall, upon successful completion of the final acceptance test (or subsequent punch list retest), issue a letter of final acceptance.

11. Owner’s Representative retains right to suspend and/or terminate testing at any time when the system fails to perform as specified.

a. Collaborate with Owner’s Representative prior to start of testing, to establish criteria pass/fail criteria and classification of test execution problems, such as:

1) *Pass/fail:* Criteria determining what constitutes a test pass or failure.

2) *Suspension and resumption:* Criteria determining when testing must be suspended and resulted later.

3) *Show Stopper:* Stop test, fix problem and restart test from beginning.

4) *Major Problem:* Fix problem before test can be resumed or concluded.

5) *Minor Problem:* Add problem to “punch list”, complete test.

6) *Special Issue:* Investigate to determine which problem category above category applies.

b. If it becomes necessary to suspend testing or inspections, work diligently to complete/repair all outstanding items to the condition specified in Specification and as indicated on related drawings.

c. Supply Owner’s Representative with detailed completion schedule outlining phase by phase completion dates and a tentative date for a subsequent punch list retest.

d. During final acceptance test, make no adjustments, repairs or modifications to system without permission of Owner’s Representative.

3.5. ADJUSTING

A. Perform field software changes after the initial programming session to “fine tune” operating parameters and sequence of operations based on any revisions to the Owner’s operating requirements.

B. Installer/Factory User Accounts:

1. Remove all default, installer, or temporary user accounts and passwords used during installation that are not part of End-user’s final operational requirements.

2. Assign new passwords that are substantially different from factory default passwords to user accounts that match factory-default user accounts.

3. Apply appropriate measures from manufacturer’s system hardening guide.

3.6. CLOSEOUT ACTIVITIES

A. Training:

1. *General:*

a. Submit training plans and instructor qualifications to Owner’s Representative for approval.

b. Coordinate with Owner’s Representative to accommodate owner shift schedules to reduce impact to regular operations.

B. Provide training as scheduled.

C. Deliver printed or electronic reference materials that cover the entire training presentation.

3.7. PROTECTION

A. Maintain strict site security during the installation of equipment and software.

1. *Equipment Rooms:* Lock and secure rooms housing accessible equipment that has been powered up.

2. *Dedicated Workstations:* Shut down, lock and secure rooms containing workstations during periods when a qualified operator in Contractor’s employ is not present.

B. Protect installed work of other trades when working in the same location, protecting all completed work prior to acceptance by Owner, unless Owner has specifically relieved Contractor from this responsibility.

C. Incremental and As-built Configuration Backup:

1. Perform full back-up of all configuration settings and system data from NVR at the completion of critical installation milestones, immediately prior to start of acceptance testing, and immediately after acceptance testing is completed.

2. Deliver instructions for restoration of the NVR VMS backups upon completion of acceptance testing.

3.8. MAINTENANCE

A. Provide maintenance updates by NVR manufacturer per agreed schedule.

END OF SECTION