



design groups, inc. p.s.

architecture
education facilities group
justice facilities group
security design group

828 - 7th Avenue SE
Olympia, WA 98501
p 360.352.8883
f 360.352.8853

ADDENDUM-1

To:
Washington State Department of Corrections
Security System Design Guidelines
Project No. 2011-320A

Addendum Date: May 24, 2013

Addendum Purpose:

Authorized under State Project 2011-330A, KMB design groups, inc., p.s. assisted DOC in developing its *Security Video System Standards for Correctional Facilities*. The Standards were in response to requirements outlined in Section 6 of Engrossed Senate Bill 5907, passed by the 62nd Legislature, signed into law by the Governor.

Development of the Standards occurred during and after the publication of Version 1.0 of the *Washington Department of Corrections Security System Design Guidelines*, dated June 30, 2011. The modifications described below and as attached, shall replace the referenced portions of the *Design Guidelines* to be consistent with, but not replace any portion of the *Security Video System Standards for Correctional Facilities*.

Part IV - Design Criteria

Item Description

1. **Paragraph L, Security Video System:** Replace entire paragraph with new Paragraph L. attached, 5 pages, dated 5/24/2013.

Part V. – Quality and Performance Requirements

Item Description

2. **Paragraph G, Security Video System:** Replace entire paragraph with new Paragraph G. attached, 6 pages, dated 5/24/2013.

[END OF ADDENDUM-1]

DESIGN CRITERIA

Washington Department of Corrections
Security System Design Guidelines

IV. Design Criteria

Replace Paragraph L. with the following:

L. Security Video System

1. Related Standards and DOC Goals

A separate document entitled *Security Video System Standards for Correctional Facilities* has been developed by DOC to provide more specific and detailed design guidance with regard to its requirements for Security Video Systems. The Standards supplement these Design Guidelines, and supersede any conflicting information expressed in the Guidelines.

It is the intent of DOC to move towards a facility-wide fully digital to-the-edge Internet Protocol (IP) Networked Video Management System (NVMS) with on-network archival storage, and software virtual matrix switching that allows for network-wide viewing of live and archived video. The Security Video System will operate over the Ethernet security system network.

Legacy all-analog, or analog with Digital Video Recorder (DVR), systems should be transitioned toward this goal, and Hybrid Video Recorders (HVR's) should only be used on a case-by-case basis, with such use to be proposed as an Alternative to these Guidelines.

2. Camera Deployment Purposes

It is essential that the cameras provide usable information for their intended purpose. The recognized purposes for deployment of cameras in WSDOC's prison facilities are:

- a) Movement Control Cameras: Every controlled door/gate in facilities of all custody levels should have cameras of a type and at a location on both sides of the opening, with acuity to provide for positive facial identification of the persons requesting movement. *(Note: Doors/gates which may have direct line-of-sight from a Control Point are generally not exempt from this requirement, unless it can be predicted with great certainty that control will never be transferred to another remote Control Point.)*

Requirements:

- Utilize fixed cameras configured and located to provide images presenting the subject's face
 - Provide 40-50 pixels per horizontal foot of camera coverage at the designed subject distance from the camera
 - Cameras are integrated for automated association to Door/Gate Control, and are, by operating procedures, expected to viewed as a pre-requisite to unlocking or opening the door or gate
 - Cameras are selectable from the Human-Machine-Interface (HMI) of the control panels having control or needing for situational awareness of area where camera is located
 - Cameras are selectable from the Network Video Management System (NVMS) Graphical User Interface (GUI) on monitor(s) in the area of control
 - Cameras are selectable from the NVMS GUI at Master Control
- b) General Surveillance Monitoring Cameras: The Security Video System can provide remote surveillance of areas where staff may not be present, or have clear lines of vision to all areas.

DESIGN CRITERIA

Washington Department of Corrections
Security System Design Guidelines

Requirements:

- Utilize fixed cameras for coverage
- Provide 10-20 pixels per horizontal foot of coverage through selection of camera type, quantity, and location
- Designated areas are supplemented by PTZ type cameras providing high-detail video acuity of 70-90 pixels per horizontal foot, or greater, over their designed coverage area - provide software and hardware for PTZ control
- Cameras are integrated for selective call-up for periodic live-viewing, but are primarily forensic (video is archived and reviewed as needed)
- Cameras are selectable from the NVMS GUI on monitor(s) in the area of control
- Cameras are selectable from the NVMS GUI at Master Control.

- c) Activity Monitoring Cameras: Similar to General Surveillance, but more specific to areas where offender activities take place. This monitoring is supplemental to, or in some cases may be in lieu of, direct staff supervision, depending on the facility's assessment of risks.

Guidelines:

- Utilize fixed cameras for coverage
- Provide 20-30 pixels per horizontal foot of coverage through selection of camera type, quantity, and location
- Designated areas are supplemented by PTZ type cameras providing high-detail video acuity of 70-90 pixels per horizontal foot, or greater, over their designed coverage area - provide software and hardware for PTZ control
- Cameras are integrated for selective call-up for live-viewing during activity, and may be monitored continuously or intermittently as determined by post procedures
- Cameras are selectable from the NVMS GUI on monitor(s) in the area of control
- Cameras are selectable from the NVMS GUI at Master Control.

- d) Specialized Monitoring Cameras: Some areas within prison facilities require extensive monitoring, including frequent or constant staff supervision. The Security Video System can be a means to provide or support the requirements for visual supervision, and additionally to provide a video record of the observed activities. Examples: Short-term holding cells, medical isolation, mental health, self-harm risk or suicide watch, etc.

Guidelines:

- Utilize fixed cameras located to provide full coverage of the area
- Provide 20-30 pixels per horizontal foot of coverage through selection of camera type, quantity, and location
- Designated areas are supplemented by PTZ type cameras providing high-detail video acuity of 70-90 pixels per horizontal foot, or greater, over their designed coverage area - provide software and hardware for PTZ control
- Cameras are integrated for selective call-up for live-viewing during active use of the cell or monitored space, and are to be intermittently or continuously monitored as determined by post procedures
- Cameras are selectable from the NVMS GUI on monitor(s) in the area of control
- Cameras are selectable from the NVMS GUI at Master Control.

DESIGN CRITERIA

Washington Department of Corrections
Security System Design Guidelines

- e) Alarm Association Cameras: The Security Video System can be electronically integrated such that another electronic security sub-system, when it detects a specified event, triggers the Video System to perform an action, such as display pre-defined camera images on a monitor. The cameras described herein are also selectable from the NVMS GUI at Master Control, and other Control Points as designated.

Guidelines:

- When integrated to the Perimeter Intrusion Detection system provides live-viewing of the associated detection zones upon an alarm event - utilizes fixed cameras providing 10-20 pixels per horizontal foot of coverage
- When integrated to Staff Duress devices (fixed duress alarm buttons or portable transmitting devices monitored on a dedicated system) provide for live-viewing of the associated site or building area upon an alarm event - utilizes fixed cameras providing 20-30 pixels per horizontal foot of coverage.

3. Camera Deployment

The facility staff should perform, during the project design phase, a Risk Assessment to determine the interior and exterior areas requiring video surveillance, and the degree of acuity required in each area. The Risk Assessment should also determine which areas require pan-tilt-zoom capability for supplemental surveillance. Pan-tilt-zoom cameras should NOT be used to meet the primary coverage requirements.

Appendix B of the *Security Video System Standards for Correctional Facilities* should be compared to the Risk Assessment by the Security System Designer, and any inconsistencies should be brought to the attention of the stakeholders at a Security Design Review worksession.

The Security Video System design should address:

- View obstructions (consider fixed and moveable equipment and furnishings, as well as permanent construction)
- Available illumination (particularly with megapixel cameras which have less sensitivity to low light levels)
- Shadows and glare
- Background
- Environmental conditions (wind, rain, snow, fog, etc.)
- Camera mounting stability

4. Camera Live Viewing

As a standard deployment, Security Video System equipment, integration, and capabilities should be provided at the following locations in a correctional facility, subject to applicability to the custody level:

- a) Master Control: Master Control (the facility's highest level central Control Point) is to be able to live-view any camera operating on the facility's Security Video System.
- b) Other Control Points: Other Control Points are to be able to live-view only the video originating from cameras located within their area-of-control (or related areas such as exterior approach ways and yards, as needed for situational awareness).

DESIGN CRITERIA

Washington Department of Corrections
Security System Design Guidelines

- c) Movement Control: Control Points having Movement Control functionality will have all cameras represented on the touchscreen HMI with graphic icons which indicate the view direction and the camera ID number. Pan-tilt-zoom cameras should have icons indicating that capability. The Control Point should have video viewing monitors as follows:
- One (1) quad-view (4 images) monitor, with one or more quadrants used for automated movement door/gate call-up and alarm live-view video display
 - movement control is normally two cameras displayed minimum – both sides of the controlled door/gate
 - alarm association is minimum 3 cameras displayed for Perimeter, 1 or more displayed for Staff Duress and other alarms
 - all quadrants are also assignable for live-view surveillance (viewing assignments may be overwritten by the automated movement control selections) by selection
 - from the touchscreen HMI
 - from the NVMS GUI
 - One (1) user-configurable and assignable video viewing monitor
 - user may configure number and size of viewports from menu of available choices (typically up to 16 images, but newest systems support up to 40 images per monitor)
 - user may select cameras for live-viewing
 - from the touchscreen HMI
 - from the NVMS GUI
- d) Large Areas of Control: Control Points having large areas of control, and specifically Major Control, should have additional video monitors to allow for greater live-view surveillance capabilities, with the control operator(s) able to set their viewing configuration and readily assign specific cameras to the viewports.
- e) Limited Control: Limited-control Control Points will normally not have video viewing monitors.
- f) Specialized Monitoring Points: Special facilities, such as prison hospitals, may have security stations where custody staff should have video system monitoring capability for areas where they have responsibility, but which may be remote or not easily viewed directly.
- Provide one or more monitors, and a means to control the display of cameras originating in the security station's area-of-responsibility.
- g) Perimeter Detection Alarms: Perimeter alarms should, through integration, cause the display of live video coverage of the zone in-alarm and the two (2) adjacent zones on one (1) or more video monitors dedicated for that purpose. The monitors should be located at Master Control, adjacent to the perimeter alarm management control panel.
5. Camera Recording

All cameras connected to the Security Video System are to be recorded to a video archive which is securely maintained on the System, and which has been configured for resilience and component failure tolerance, as well as to permit expansion. Recording of video data will be continuous 24/7/365.

DESIGN CRITERIA

Washington Department of Corrections
Security System Design Guidelines

Guidelines:

- Recording should be at the full resolution of the installed camera, which meets the acuity requirements set forth
- Record at not less than 7.5 frames per second (7.5fps); 10 video frames per second (10fps) is preferred
- System features which mitigate the storage requirements, such as compression and motion-detection with "on-motion" buffer recording, where a reduced frame rate is used during no-motion periods, may be utilized so long as no gaps in the recording are created
- The system should be configured to self-monitor and alarm for loss of a video signal from the cameras
- There should be no interruption, or degradation of quality of the recording, due to any number of system users accessing the system's live or archived video
- The "General Records Retention Schedule" adopted by the State of Washington, Disposition Authority Number GS 25003 specifies that Security Recordings of agency facilities and grounds be retained as an official copy for a period of 30-days
 - A further requirement is that, as with all public records, security recordings must be retained until final resolution of the case if they are requested or used in litigation
 - Video data with authentication may be exported from the system to provide support for civil litigation, prosecution or defense of criminal actions, or for other quasi-judicial actions
 - System useable archive capacity shall be not less than 1.2 times the calculated requirement
 - After 30 days have elapsed the archive data shall be overwritten by the system

6. Archived Video Viewing

Video archive viewing-capable Security Video System workstations (PC's) with appropriate software (which can also live-view any camera in the facility's Security Video System) are to be deployed at the following locations:

- Shift Office
- Investigations and Intelligence offices
- Emergency Response Management room(s).

QUALITY & PERFORMANCE REQUIREMENTS

Washington Department of Corrections
Security System Design Guidelines

V. Quality and Performance Requirements

Replace Paragraph G. with the following:

G. Security Video System

1. Definitions

- a. Video Camera – A commercially available, color, low light level capable, high resolution, progressive scan, CCD image sensor fitted with an appropriate fixed or variable focal length lens. May be fixed-view or motorized pan-tilt-zoom type.
- b. Digital Video Recorder (DVR) – A self-contained device that records as digital video data one or more streams of video images originated from analog video cameras. DVR's can playback the archived video locally, and may be connected to a network for remote playback viewing on a PC having the required software.
- c. Hybrid Video Recorder (HVR) – A self-contained device that records as digital video data one or more streams of video images originating from either analog or digital video cameras. HVR's can playback the archived video locally, and may be connected to a network for remote playback viewing on a PC having the required software.
- d. Network Video Management System (NVMS) – A distributed, network-based, software-controlled, video system that provides facilities for managing the output from many video cameras, recording the output as digital data, and for viewing selected live or archived digital video data.
- e. Network Video Recorder (NVR) – A digital recording management component of a Network Video Management System. NVR's may have data storage capability, or function as video servers without on-board storage.
- f. "Standards" or "Security Video System Standards" – References to the Washington Department of Corrections *Security Video System Standards for Correctional Facilities*, latest version, unless otherwise stated.

2. System Description

- a. Analog DVR or hybrid analog-digital HVR-based systems – should be specified only for expansion of an existing DVR or HVR-based system, or for implementation of a new *very small* video system which can achieve the required coverage and acuity with 16 or fewer total system cameras. Existing systems of this type should be migrated to a Network Video Management System whenever feasible within the project's scope.
 - 1) Expansion of these existing systems may include either analog or digital cameras, but digital IP cameras are preferred.
 - 2) For digital viewing these systems may have:
 - a) The DVR/HVR connected to a network with video monitoring PC's workstations using compatible viewing software, or
 - b) In very small systems video may be viewed directly from the DVR/HVR's video output port using the DVR/HVR's viewing software (with log-on privileges constraining operator access to recorded video).
 - 3) DVR/HVR devices should be installed in secured Security Electronics Rooms; relocate any existing devices being retained.
 - 4) New installations of analog matrix switchers or multiplexer video switching and analog display monitors are discouraged; existing systems should be migrated to an NVMS.
- b. A Network Video Management System (NVMS) – should be specified for all implementations other than as provided above. The NVMS consists of video cameras, video virtual-matrix servers providing virtual-matrix video switching, viewing client computer workstations (PC's), managed

QUALITY & PERFORMANCE REQUIREMENTS

Washington Department of Corrections
Security System Design Guidelines

network switches, and network video recorders or other data storage devices, all operating through the NVMS software.

- 1) Extensions of existing systems should match the characteristics, performance and features of the existing system. (Attention to the existing system software version, existing system hardware capabilities to operate with software version upgrading if required, the availability of new camera licenses, and the project's effect on any existing support agreements, is cautioned.)
 - 2) Systems should not utilize encoding devices for integration of analog cameras or decoding devices for video display on analog monitors. Existing encoding and decoding devices in systems should be phased out as soon as practical in favor of digital IP cameras directly connected to the network and digital viewing PC's.
 - 3) The NVMS should be delivered with software having capability to manage double (2x) the number of installed cameras without requiring upgrade to the next level.
(For example: 200 cameras are deployed, Commercial Level supports up to 250 cameras, Enterprise Level supports up to 1,000 cameras - project should provide Enterprise Level software.)
 - 4) The NVMS should integrate with the PLC/HMI control system to provide for live viewing camera selection switching, and automated live view "call up" capability in association with door/gate or device selection. Keyboard/joystick controls may supplement the PLC/HMI interface, but not substitute for it.
- c. All systems should be designed to provide video coverage of all of the facility and site areas designated in the Standards, or as determined by risk analysis performed by facility staff, and for delivery of the level of acuity (resolution) as established in the Standards for the operational purpose that each of the cameras are deployed.
- d. Provide activated camera licenses for 110% of the number of installed cameras, and for all installed ports of any system devices subject to a port licensing requirement.
- e. All system cameras should be recorded 24/7/365 at full camera resolution, with minimum frame rate and other system parameters as set forth in the Security Video System Standards.
- f. The recorded video may be searched, and authenticated copies made and exported without affecting realtime system operations.
- g. In addition to recording and storing video images, systems should display 'live', high resolution color video images on demand at any or all authorized workstations on the network. Available images at a given workstation may be restricted to local cameras, and access to archived video may similarly restricted. Individual workstations may select a preferred display format, including single image, 4 images, 9 images or 16 images simultaneously. In addition, images should be available for "call up" by other associated systems via digital signal or relay contact closure.
- h. Fixed focal length cameras, or cameras having a variable focal length lens which is adjusted at time of installation, are preferred, but some circumstances will require Pan-Tilt-Zoom arrangements. PTZ cameras should be controlled by a physical "joystick" and should be programmable to pan and zoom to at least twelve (12) preset fixed aim/zoom points at the press of a physical or virtual button, or by closure of a form 'C' remote contact.
3. Technology
- a. Cameras:
 - 1) Digital IP color video cameras are preferred for all applications, and should meet the technical requirements described below and include an integrated encoder providing a TCP/IP format output via a standard RJ-45 Ethernet jack. Megapixel IP cameras may be necessary to meet acuity standards.

QUALITY & PERFORMANCE REQUIREMENTS

Washington Department of Corrections
Security System Design Guidelines

- 2) Analog color video cameras should be used only where necessary for component replacement, or for limited-scope system expansion projects. Cameras should provide a 1v peak to peak composite video output signal at the camera into a 75 ohm load with the imager illumination described below. Sensor Resolution – 4 CIF (704 x 576 h/v), Frame Rate – H.264 @ 1 to 30 minimum for 4 CIF.
 - 3) All video cameras should support motion sensing and analysis based on pixel change in a region of the image that is selectable as to size and location within the total image.
 - 4) Cameras should employ automatic coverage control to switch from bright scene color image to dark scene monochrome image.
 - 5) Cameras with wide-dynamic-range (WDR) capabilities should be specified for installations where scene lighting is expected to create subject backlighting conditions.
 - 6) Power over Ethernet (PoE) should be utilized as the preferred camera power source whenever possible. Use of power injector devices is discouraged, and should be utilized for special circumstances only.
 - 7) Cameras not capable of being powered by PoE shall have dedicated camera power supplies.
 - 8) All video cameras should meet or exceed the following specifications:
 - a) Bright Scene Color Sensitivity – full video @ 0.3fc; useable picture @ 0.07fc
 - b) Dark Scene Monochrome Sensitivity – full video @ 0.12fc; useable picture @ 0.03fc
 - c) Automatic changeover from Bright to Dark Scene operation & reverse
 - d) Automatic white balance at 3200K indoors and 5500K outdoors
 - e) Backlight compensation
 - f) Dynamic range – 60dB
 - g) Signal to Noise Ratio – 50 dB
 - h) Synchronization – internal line lock
 - i) Vertical phase delay adjustment – 0 – 360 degrees
 - j) Shutter – Automatic ranging 1/50 to 1/5000 second
 - k) Withstand direct or reflected sunlight without detrimental effects
 - l) Video compression format support – H.264; M-JPEG; JPEG
 - m) Industry Standards compliance - ONVIF version 2 interoperability specification
 - n) Certification for operation with all required feature sets on the selected NVMS
- b. NVMS Software:
- 1) The Network Video Management System (NVMS) software should be a proven enterprise grade application that is server based. Deliver the latest released version of the software available on the date of the system Bench Test; upgrade existing system software (and make any required system hardware upgrades or replacement) to the latest version.
 - 2) System shall run on commercial off-the-shelf (COTS) computer and server hardware under an Operating System that is currently supported by DOC.
 - 3) The NVMS software features should include:
 - a) Distributed architecture for fully redundant recording,
 - b) Fully automated recording failover protection,
 - c) Support for analog video (NTSC at 1v p-p) via multiple encoders,
 - d) Allows a different format selection for each camera individually using common video compression formats, including H.264, JPEG, M-JPEG, MPEG2, MPEG4
 - e) Provide full recording and viewing operations using mixed CIF, 2CIF, VGA, 4CIF and Megapixel resolutions,
 - f) Allows live view monitoring at multiple workstations and recording simultaneously,
 - g) Allows search and copy/export operations without affecting the live monitoring and recording functions.

QUALITY & PERFORMANCE REQUIREMENTS

Washington Department of Corrections
Security System Design Guidelines

- 4) Systems should record all connected video cameras
- c. NVMS systems should be designed for resiliency and failure tolerance, through failover or virtualization strategies.
- d. NVMS systems should implement dedicated iSCSI Storage Area Network (SAN) storage architecture, utilizing RAID 5 or RAID 6 drive arrays to meet storage requirement. All storage systems should be scalable, to allow future increases in storage capacity without data loss.
- e. DVR and HVR systems should have online storage capacity configured in a RAID 5 or RAID 6 drive array.
- f. Storage capacity provided should be at least 1.2x the actual (verified after installation and operational in a live environment) requirement for recording all system cameras continuously at their highest resolution, 10 frames per second, for 30 days.
- g. System should be configured to automatically overwrite stored data after 30 days, in a "first in – first out" type of housekeeping.
- h. DVR, HVR, and NVMS systems should continuously stamp the recorded data with date and time, and store the information as a live archive in online storage. Schemes which re-process the data after a period of time to achieve greater storage are not acceptable to meet the 30-day requirement.
- i. The system should continue to monitor in real time, present live images in real time, and record in real time, while being searched by date and time, all simultaneously at one or more authorized and password protected workstations. Copies of selected segments with authentication (for evidence purposes) may be made and transferred to portable media at designated workstations only. System shall have a track record of providing authenticated video accepted in courts of law.
- j. Images or system functions in use at one location or workstation should not affect any function or operation at any other location or workstation. Pan-Tilt-Zoom control may be prioritized by workstation. The Search and Copy process should not affect any other feature or operation of the system.
- k. Where applicable, video equipment should conform to the most recent ONVIF version 2 interoperability specification.
- l. Video systems should use a single manufacturer's products wherever reasonably possible. Use accessory components specifically recommended and supported by the manufacturer for use with that equipment. All video components should be verified for compatibility with each other. Do not use generic I/O, power supplies, etc. For existing facilities with other video equipment installed, use the same manufacturer as the existing systems. For new facilities, or existing facilities with no video equipment, the preferred equipment should be products of the following manufacturers that conform to the requirements of these Guidelines:
 - 1) Cameras, ONVIF certified and certified for use on the selected software platform, as manufactured by:
 - a) Bosch
 - b) Axis
 - c) Pelco
 - d) Vicon
 - e) Owner Approved
 - 2) NVMS Software, ONVIF certified, with modules for system management, recording, and viewer client deployment:
 - a) Genetec "Omnicast"
 - b) OnSSI "Ocularis"
 - c) Owner Approved

QUALITY & PERFORMANCE REQUIREMENTS

Washington Department of Corrections
Security System Design Guidelines

- 3) Encoders:
 - a) Bosch
 - b) Axis
 - c) Pelco
 - d) Vicon
 - e) Owner Approved
 - m. Software and firmware used in conjunction with the video equipment should be licensed to the State. Any custom software or programming shall become the property of the State. Software provided should include programming applications that are required to make changes/adjustments to the programing.
4. Installation
- a. All video equipment (except cameras) should be installed in a secured Security Electronics Equipment Room, and be grounded in accordance with requirements found elsewhere in these Guidelines.
 - b. All powered components of the Security Video System should be connected to a UPS and generator backed source.
 - c. Camera installation locations and their views should be approved by the Owner. As a pre-condition to installation, the installer should demonstrate available images using a live camera provided with a manual vari-focal lens and a color display. Handhold the camera at the proposed installation location and demonstrate available images by changing focal length of the vari-focal lens until an acceptable image is identified by the Owner.
 - d. Cameras and lenses, and the conditions of installation, shall provide the requisite acuity and view for the camera's intended purpose.
 - e. Cameras mounted outdoors, or indoors where the field of view is influenced by changes in ambient lighting, should be provided with an auto-iris lens. Some design conditions may warrant provision of a camera having capabilities for overcoming strong backlighting.
 - f. Cameras should be rated by the manufacturer for installation under the environmental conditions expected at the installation location. Cameras may be provided with a heated and/or cooled environmental enclosure that will limit and/or control the camera environment to within the manufacturer's rating. In addition, security enclosures should be provided for cameras installed in offender accessible locations if less than twelve feet (12') above the highest access level within ten feet (10') of the camera. Enclosure/camera selections should assure the enclosure does not limit the camera view.
 - g. Not more than 75 percent (75%) of the number of video cameras recommended by the manufacturer as the maximum number, at full resolution and 10fps frame rate, should be connected to an NVMS server. Server resources, when in full operation, should not exceed 75% usage.
 - h. Systems with more cameras should use multiple video servers, which may be distributed throughout the facility, connected on a dedicated video network with managed virtual switching.
 - i. Failure of one video server should cause video images after the failure to be recorded at a different video server for the duration of the failure. This shall be without operator or technician intervention (automated failover), and the system shall report the failure to the Security System Management PC or server.
5. System Operation
- a. The Security Video System shall be designed and implemented in a manner that provides the operational support required by DOC, as set forth in the Security Video System Standards.

QUALITY & PERFORMANCE REQUIREMENTS

Washington Department of Corrections
Security System Design Guidelines

- b. Video system shall provide all of the following image types simultaneously, at any or all authorized workstations on the system:
 - 1) Dedicated Images - Images always on screen for observation
 - 2) 'Call Up' Images - Images displayed only when a related system triggers the need for a video picture (verification of persons desiring passage into or out of a facility)
 - 3) 'On Demand' Images – Images not displayed until specifically requested by a person having authorized access to the system
 - c. The video system should respond to commands and display the full resolution and full quality image requested within 750 milliseconds of a command transmitted by digital message or contact closure.
 - d. The image should not roll or tear, or display any degrading characteristics (snow, sound bars, etc) at any time, but should remain stable without a change in resolution or quality until cancelled by another digital message or contact closure, or through expiration of a timed operation.
6. Performance Testing
- a. Demonstrate proper operation, view, and quality image for all cameras. Images displaying sound bars or that roll or tear, or display degraded characteristics will be rejected.
 - b. Demonstrate acceptable response time as described above in the System Operation section.
 - c. Simulate utility power failure and demonstrate continuance of proper operation of the entire system under failure of normal power, and at return to normal power.