1. INTRODUCTION/BACKGROUND

1.1 The Washington Metropolitan Area Transit Authority (WMATA or the Authority) was created by an interstate compact in 1967 to plan, develop, build, finance, and operate a balanced regional transportation system in the national capital area. The Authority began building its rail system in 1969, acquired four regional bus systems in 1973, and began operating the first phase of Metrorail in 1976. Today, Metrorail serves 86 stations and has 106 miles of track. Metrobus serves the nation's capital 24 hours a day, seven days a week with 1,500 buses. Metrorail and Metrobus serve a population of 3.4 million within a 1,500-square mile jurisdiction. Metro began its paratransit service, MetroAccess, in 1994; it provides about 1.5 million trips per year.

1.2 WMATA is in the process of upgrading the Electronic Security Systems installed throughout the authority. As part of this process, WMATA wishes to evaluate and procure a new Video Management System (VMS). WMATA also has an interest in Physical Security Interface Management software and integration. Lastly, WMATA is interested in Video Analytic software and configuration for specific applications.

1.3 Due to the security sensitive nature of the subject, some aspects of the system design are expressed in general terms. Additional information shall be provided as the procurement and/or contract process develops.

1.4 A large portion of this project is to be funded by different DHS grants. As such, WMATA must be able to invoice in such a manner that costs may be traceable to specific grants. Additionally, many of the grants have different expiration dates. As such, WMATA must be able to schedule tasks to ensure the project is completed prior to grant expiration dates.

2. OBJECTIVE / PURPOSE

2.1 The objective of this contract is to acquire a Video Management System (VMS) which consists of a Video Management Software package, a Physical Security Interface Management (PSIM) software package, a Video Analytic software package, and Contractor supplied services to configure and maintain an Electronic Security System (ESS) for fixed infrastructure.

2.2 The VMS software shall allow for a minimum of 64 cameras or other devices to be connected to each NVR Storage machine. A redundant Authentication and Authorization Master Server shall allow for a minimum of 20,000 NVR Storage machines to be connected.

2.3 WMATA currently uses a wide range of cameras, and as such, requests a VMS solution that can record and view most cameras on the market today. WMATA also has an
aggressive program underway to install more cameras throughout the rail system. In the future, the majority of the cameras shall be IP, megapixel cameras.

2.4 WMATA seeks a video analytic package to help with observation of cameras. WMATA seeks video analytic solutions that use server processing. Specific applications which must be addressed by video analytics include detecting unauthorized intrusion at the End of Platforms, detecting a breach in the perimeter at Bus Garages and Rail Yards, and detection of persons entering or exiting the wayside at station platforms and other applications to be defined later in the program. Video analytics shall be demonstrated before acceptance by WMATA. Full scale deployment of the video analytics shall be implemented, upon acceptance by WMATA.

3. CURRENT ENVIRONMENT

3.1 WMATA has 90 rail stations, 10 rail yards, 10 bus garages, 35 Parking Garages, and 10 miscellaneous buildings. A typical station will have 50 cameras. A typical rail yard and bus garage will have 75 cameras. A typical miscellaneous building will have 100 cameras. A typical parking garage (lot) will have 35 cameras.

3.2 WMATA currently uses a distributed architecture to collect and record video. At each location, a Communication Equipment Room (CER) exists that is outfitted with HVAC, electronic racks, Ethernet connectivity, and emergency power. WMATA prefers to install the VMS NVR Storage machines in these CERs.

3.3 At each rail station, there are kiosk(s) where the station manager is located. Each kiosk will be provided with four (4) 21-inch touch screen displays connected to two workstations. There are approximately 150 kiosks within the current WMATA rail system.

3.4 At each bus garage and rail yard, there are guard shacks where Special Police Officers are stationed. Each guard shack will be provided with four (4) 21-inch touch screen displays connected to two workstations. There are approximately 20 guard shacks within the authority. Additionally, there is at least one viewing station (possibly two) inside each bus garage / rail yard for the building/facility manager to view.

3.5 At each of the miscellaneous buildings, at least one viewing station is provided. Additionally, WMATA has several functional locations where video is viewed. Although the capability to view all cameras from these locations must be provided, in reality, only about 200 cameras are ever viewed at one time. Functional locations where video is to be displayed real time include the Rail Operational Control Center (ROCC) at both the Jackson Graham Building (JGB) and the Carmen Turner Facility (CTF), the Bus Operational Control Center (BOCC) at both JGB and CTF, the Security Operational Control Center (SOCC) at CTF, the Emergency Command Center at JGB and CTF and several other centers throughout the authority. Typically, these locations have a wall of large screen monitors and multiple workstations to support the video feeds.

4. CONTRACTOR REQUIREMENTS
Independently and not as an agent of the Authority, the Contractor shall furnish all the necessary services, qualified personnel, methods and means, materials, equipment, and facilities, not otherwise provided by the Authority, and do all things necessary for or incident to the performance of work as described in the contract.

The Contractor shall have designed and installed and Electronic Security System, with at least 500 edge devices, within the last three-two (23) years.

The prime contractor must perform at least 51% of the work if subcontractors are utilized. This 51% may not be strictly administrative in nature.

4.1 Video Management Software

The Contractor shall provide a VMS, in accordance with the characteristics and specifications contained in this statement of work, to monitor and record from fixed infrastructure locations. The VMS shall be a fully distributed solution designed for multi-site, multi-server installation requiring continuous surveillance with support for devices from different Contractors. All software components shall be part of the manufacturer’s standard software product offering and shall be thoroughly tested and proven by the manufacturer.

Components of the VMS shall include Video Recording Software, Real-time Video Viewing software, Video Retrieval Software, System Administration Software, Alarm Management/Interfaces Software/Situational Awareness, and WEB Based Remote Video Viewing Software

4.1.1 Video Recording

WMATA currently uses a distributed architecture to collect and record video. At each location, a Communication Equipment Room (CER) exists that is outfitted with HVAC, electronic racks, Ethernet connectivity, and emergency power. WMATA prefers to install and maintain the VMS NVR Storage machines in these CERs.

4.1.2 Real-Time Video Viewing

The Contractor shall provide a VMS that provides the ability to view data at several different locations and several different layouts. Screens shall be developed for the following viewing locations:

4.1.2.1 At each rail station, there are kiosk(s) where the station manager is located. Each kiosk will be provided with four (4) 21-inch touch screen displays connected to two workstations. There are approximately 180 kiosks within the current WMATA rail system.

4.1.2.2 At each bus garage and rail yard, there are guard shacks where Special Police Officers are stationed. Each guard shack will be provided with four (4) 21-inch touch screen displays connected to two workstations. There are approximately 20 guard shacks within the
authority. Additionally, there is at least one viewing station (possibly two) inside each bus garage / rail yard for the building/facility manager to view.

4.1.2.3 At each of the miscellaneous buildings, at least one viewing station is provided. Additionally, WMATA has several functional locations where video is viewed. Although the capability to view all cameras from these locations must be provided, in reality, only about 100 cameras are ever viewed at one time. Functional locations where video is to be displayed real time include the Rail Operational Control Center (ROCC) at both JGB and CTF, the Bus Operational Control Center (BOCC) at both JGB and CTF, the Security Operational Control Center (SOCC) at CTF, the Emergency Command Center at JGB and CTF and several other centers throughout the authority. Typically, these locations have a wall of large screen monitors and multiple workstations to support the video feeds.

4.1.2.4 The Contractor shall provide a desktop viewing application to allow WMATA staff to monitor video from any camera or recorder at office workstations.

4.1.2.5 At several locations throughout WMATA, local jurisdiction and partners will need to monitor video. A viewing application shall be developed for these situations. Viewing streams shall be controlled based on permissions, data flow rates, and other requirements. The vendor shall work with WMATA’s IT Security Department and Network group to deliver the required service.

4.1.3 Video Retrieval

The Contractor shall provide a video retrieval toolkit to support WMATA’s post incident investigation and video retrieval efforts.

4.1.4 System Administration

The contractor shall provide a comprehensive set of system administration, monitoring, controlling, and maintenance tools supplied with the system to support WMATA’s operation and maintenance of the VMS.

4.1.5 Alarm Management/Interfaces

WMATA is seeking to develop a situation awareness application to help employee provide effective service to the public. As such we are evaluating a Physical Security Interface Manager (PSIM) type system throughout the authority. The Video Management System must interface with such software. Any PSIM system deployed by the authority will be gradually phased in. Until such time as the PSIM is fully deployed, the VMS must be able to provide situational awareness, operator interface functionality, alarming, and interface with video analytical and other software packages to perform the functionality required by WMATA.

WMATA wishes to improve its situation awareness. As such, we are looking for ways to integrate systems. In the technical proposal, the Contractor should identify examples of
situational awareness that their system has provided to other customers and can provide for WMATA. Examples of integration that WMATA requests are as follows:

4.1.5.1 When a Call-for-Aid button is depressed anywhere in the system, (whether it be from the platform, Government Emergency Telecommunications Service (GETS) phone, elevator landing, elevator cab, etc) then the views from cameras which have a view of the Call for Aid device shall be displayed at the response point for the Call For Aid system. The current Call For Aid system is designed around a Commend audio system.

4.1.5.2 The existing CBRE system is CBEMIS by Smiths Detection and must interface with the new VMS either alone or through the PSIM.

- The Contractor shall ensure that any camera that can be displayed in the VMS and PSIM is integrated in the CBEMIS software and can also be displayed in CBEMIS.
- The Contractor shall ensure that any camera displayed in the VMS and PSIM with PTZ and preset functionality can also be controlled in the CBEMIS software.
- The Contractor shall ensure that there is a user based permission system that prevents a camera being moved by a user other than the user of the CBEMIS applications during emergency situations.
- The Contractor shall be responsible to work with the CBEMIS supplier to design the integration using the SDK of any VMS and PSIM solution provided.
- The Contractor shall be responsible to work with the CBEMIS supplier to develop a complete integration using the SDK of any VMS and PSIM solution provided.
- The Contractor shall be responsible to work with the CBEMIS supplier to complete testing of any integration performed.

4.1.5.3 When someone enters a protected service room, an alert will pop up on the kiosk viewing screen and at the SOCC viewing station. Functionality shall vary based on threat level.

4.1.6 WEB Viewing

4.1.7 The Contractor shall provide a VMS system that shall support and allow WEB viewing or mobile device viewing with proper credentials and permissions.

4.2 Physical Security Interface Manager Software

4.2.1 The Contractor shall provide, in accordance with the characteristics and specifications contained in this statement of work, Physical Security Interface Manager (PSIM) Software for an Electronic Security System. The PSIM shall be a fully distributed solution designed for multi-site, multi-server installation requiring continuous surveillance with support for devices from different Contractors. All software components shall be part of the manufacturer’s standard software product offering and shall be thoroughly tested and proven in reference installations.

4.2.2 The PSIM must provide visualization across a wide spectrum of electronic systems and act as a force multiplier by increasing situational awareness. Systems which the PSIM must interface with include, but not limited to, access control, video surveillance, intrusion detection, Call-for-Aid, LADAR, SCADA, dispatch, ROCC and other type
systems. The Contractor shall provide a list of interfaces which have been developed in their technical proposal. A listing of desired interfaces are listed in section 5.2.22 of the SOW.

4.2.3 The proposed solution shall provide an integrated secure, scalable and easily accessible software-based solution for the management of the complete physical security infrastructure – for example: CCTV images, access control systems, intruder systems, fire systems, Building Management Systems, video wall processors, Global Information Systems.

4.2.4 The software shall provide authorized users access to the various systems managed by the solution and be capable of providing bi-directional control of managed systems, and management information.

4.2.5 The PSIM shall feature an integrated visual process and policy designer allowing system administrators to implement security processes and policies within the system, which respond in accordance with sub-system cause and effects. Policies may be executed by several means: automatically as part of a process, manually as part of a scenario or according to a specified schedule.

4.2.6 Supplier must demonstrate that the PSIM solution is being continually developed and enhanced according to market requirements, industry and technological advances.

4.3 Video Analytics Software

The Contractor shall provide, in accordance with the characteristics and specifications contained in this statement of work, Video Analytic Software for an Electronic Security System. The Video Analytic Software shall be a fully distributed solution designed for multi-site, multi-server installation requiring continuous surveillance with support for devices from different Contractors. All software components shall be part of the manufacturer’s standard software product offering and shall be thoroughly tested and proven in reference installations. The contractor shall have deployed the video analytic software in one or more installations with requirements of behavior and performance similar to the WMATA requirements. Generally speaking, all video analytics shall have a false alarm rate of one (1) alarm per camera per day and a 99.5% detection rate.

A brief description of the specific solutions to be developed and provided by the Video Analytic Software is detailed in the following section. After award of the contract, the Contractor shall review current and planned camera placement and submit a report to WMATA with recommendations to WMATA for camera placement to optimize the performance of the Video Analytic system. A detailed description of operation (and required integration effort) shall be developed by WMATA and the Contractor after award of the contract.

4.3.1 End of Platform (EOP) Gates

The contractor shall configure the Video Analytic Software to assure the detection of individuals who jump into the track bed or bypass the End of Platform Gates in rail stations. Multiple cameras will be installed by others throughout the station to be used by
the Video Analytic supplier. The Video Analytic supplier (through integration efforts with the PSIM and/or VMS interfacing to an access control device) shall determine if the detected individual is an adversary.

If it is determined that the detected individual is a bad guy, then an alarm will be generated at the station manager kiosk and the SOCC (and other places to be determined by WMATA). Additionally, visual and audible devices (installed by others near the end of platform gates) shall be activated for a predetermined amount of time.

4.3.2 Perimeter Security System (PSS) – Rail Yards

The Video Analytic Software shall detect individuals who breach the perimeter of Rail Yards. Multiple cameras shall be installed along (and interior to) the perimeter fence line by others for use by the Video Analytic supplier. If an intruder is detected, then an alarm will be generated at the guard shack and the SOCC (and other places to be determined by WMATA). Additionally, PTZ cameras shall be controlled (or slewed) by the PSIM software of the Electronic Security System to identify and track the intruder.

4.3.3 Perimeter Security System (PSS) – Bus Garages

The Video Analytic Software shall detect individuals who breach the perimeter of Bus Garages. Multiple cameras shall be installed along (and interior to) the perimeter fence line by others for use by the Electronic Security System. If an intruder is detected, then an alarm will be generated at the guard shack and the SOCC (and other places to be determined by WMATA). Additionally, PTZ cameras shall be controlled (or slewed) by the PSIM software of the Electronic Security System to identify and track the intruder.

4.3.4 Intrusion Detection System – Shaft/Portal

The contractor shall configure the Video Analytic Software to assure the detection of individuals who enter the underground through portals or vent shafts. Multiple cameras will be installed by others near the portals and vent shafts to be used by the Video Analytic supplier. The Video Analytic supplier (through integration efforts with the PSIM and/or VMS interfacing to an access control device) shall determine if the detected individual is an adversary.

If it is determined that the detected individual is a bad guy, then an alarm will be generated at the station manager kiosk and the SOCC (and other places to be determined by WMATA). Additionally, visual and audible devices (installed by others near the end of platform gates) shall be activated for a predetermined amount of time.

4.3.5 Service Room Hardening

The contractor shall configure the VMS software to alert at the SOCC (and display video) when someone enters a hardened service room without using an access card. At higher threat levels, alarms shall be generated based on motion detection.

4.3.6 The Contractor shall develop a prototype for each Video Analytic solution. WMATA and the Contractor shall fully test each prototype solution prior to full scale deployment.
of any Video Analytic solution. If WMATA finds the Video analytic solution to be acceptable, then WMATA shall exercise the option to purchase the specific Video analytic solution.

4.4 Contractor Services

4.4.1 The Contractor shall configure, setup, commission, and test the video management software. The Contractor shall maintain an office within a 50 miles radius of WMATA and shall provide all labor, documentation, and testing for a fully functional VMS, physical security interface manager, and a video analytic system. Subcontractors are not required to maintain an office within 50 miles of WMATA.

4.4.2 The Contractor shall configure, setup, commission, and test the physical security interface manager software. The Contractor shall maintain an office within a 50 miles radius of WMATA and shall provide all labor, documentation, and testing for a fully functional VMS, physical security interface manager, and a video analytic system.

4.4.3 The Contractor shall configure, setup, commission, and test the video analytic software. The Contractor shall maintain an office within a 50 miles radius of WMATA and shall provide all labor, documentation, and testing for a fully functional VMS, physical security interface manager, and a video analytic system.

4.4.4 The Contractor shall provide project management services, hardware coordination services and system integration services and shall be responsible for the design, configurations, commissioning and testing of the VMS. As part of the technical proposal, the Contractors shall provide system architecture. After award of contract, the Contractor shall submit a formal System Architecture as a contract deliverable.

4.4.5 The Contractor shall perform recording and storage calculations and work with WMATA to develop hardware specifications for recording, storage and viewing equipment required to support the VMS. Recording and storage calculations shall be based on 30 days of storage at 4CIF and 30 frames per second. H264 codec shall be used for megapixel cameras and MPEG codec shall be used for analog cameras unless otherwise approved by WMATA. A preliminary Storage Analysis shall be provided as part of the technical proposal. After award of contract, the Contractor shall submit a formal Storage Analysis as a contract deliverable. This Storage Analysis shall be measured and verified as part of the acceptance test process. The Contractor shall submit a test plan to WMATA for approval.

4.4.6 The Contractor shall perform network loading calculations to determine the impact on WMATA network. A preliminary Network Analysis shall be provided as part of the technical proposal. After award of contract, the Contractor shall submit a formal Network Analysis as a contract deliverable. This Network Analysis shall be measured and verified as part of the acceptance test process. The Contractor shall submit a test plan to WMATA for approval.

4.4.7 The Contractor shall work with WMATA IT department to ensure that security requirements are satisfied. The Contractor shall develop and submit a security analysis
for approval by WMATA. This Security Analysis shall be measured and verified as part of the acceptance test process. The Contractor shall submit a test plan to WMATA for approval.

4.4.8 The Contractor shall customize the Video Management Software and/or PSIM software for WMATA’s unique viewing needs. Furthermore, the Contractor shall develop customized viewing stations for multiple unique WMATA situations. Some examples of these customized viewing situations are station kiosk, guard booths, yard masters, bus division managers, and Rail and Bus OCC, Security OCC and similar type applications. For each unique viewing screen, the contractor shall provide a solution (map, floor plan, etc.) that shows each sensor, camera, or security device. When the operator selects the device, the operator will be able to drill down to the detailed data provided by the sensor, camera, or device. Response plans shall be implemented if the PSIM option is selected.

4.4.8.1 Custom overview screens shall be developed. These screens shall be submitted to WMATA for approval. For estimating purposes, a total of ten (10) unique screens shall be assumed. A typical overview screen shall start with the WMATA System Map. As the operator selects a location, the operator will be able to drill down to the detailed screen for each location.

4.4.8.2 Custom screens shall be developed for each kiosk and station. For estimating purposes, a total of 160 unique screens shall be assumed. A typical kiosk screen shall start with a floor plan of the station which displays alarm conditions. From there, the operator will be able to select a camera or other security device for additional information. In addition, the operator will be able to arrange all camera views for observation from the operator.

4.4.8.3 Custom screens shall be developed for each guard shack location at the Bus Garage. For estimating purposes, a total of 12 screens shall be assumed.

4.4.8.4 Custom screens shall be developed for each guard shack location at the Rail Yard. For estimating purposes, a total of 12 screens shall be assumed.

4.4.8.5 Custom screens shall be developed for the many different Control Center locations. For estimating purposes, a total of 20 screens shall be assumed. Screens developed for all viewing locations shall be displayed in the different display centers.

4.4.8.6 Custom screens shall be developed for many locations not yet defined. For estimating purposes, a total of 50 screens shall be assumed.

4.4.9 The Contractor shall customize the Video Management Software and/or PSIM software for WMATA’s unique viewing needs. Furthermore, the Contractor shall develop customized reports for multiple unique WMATA situations. For estimating purposes, assume that ten (10) reports shall be developed.

4.4.10 The Contractor shall provide integration interfaces with existing WMATA electronic systems. Specific systems that shall interface include, but not limited to, CBEMIS; COMMEND Call-for-Aid; Edwards EST3 Fire Alarm and Access Control; Allen-Bradley SLC-500 PLC; QEI RTU’s; and other systems to be determined.

4.4.11 The Contractor shall develop a Video Retrieval Console for use by MTPD to analyze, record, search and document incidents throughout the authority. This may require the development of custom software. The console shall have long term storage and video
analyses tools. The vendor shall provide a detailed description of the Video Retrieval console and video retrieval process in the technical proposal.

4.4.12 The Contractor shall develop an Acceptance Test Plan. An outline of the Acceptance Test Plan shall be provided as part of the technical proposal. After award of contract, the Contractor shall submit a formal Acceptance Test Plan as a contract deliverable. The Acceptance Test Plan shall be submitted for approval by WMATA.

4.4.13 The Contractor shall provide a training program for operators, users, administrators, and maintainers. An outline of the training program shall be provided as part of the technical proposal. After award of contract, the Contractor shall submit a formal Training Plan as a contract deliverable. The Training Plan shall be submitted for approval by WMATA.

4.4.14 The Contractor shall have designed and installed and Electronic Security System, with at least 500 edge devices, with the last three years.

4.4.15 The Contractor shall submit a 60%, a 90%, and a 100% design for approval. The design shall contain a complete system architecture drawing, a listing and naming convention for edge devices, a listing of viewing clients, details on specific viewing screens for use by WMATA, a listing of integration interfaces, and other specific details required for a fully functional system.

4.5 Software Maintenance - Option

4.5.1 The Contractor shall provide on-site software maintenance support for a period of 12 months, with four (4) 12 month option periods. This support shall start upon successful completion of the Substantial Completion Inspection (SCI) and include support for the Video Management software, The Physical Security Interface Management software, and the Video Analytic software.

4.5.2 This support shall include screen development, report generation, software upgrades, OS patches, virus protection, system configuration, response plan implementation and other such support required for operation.

4.5.3 An outline of the On Site Software Maintenance Program shall be provided as part of the technical proposal. After award of contract, the Contractor shall submit a formal On Site Maintenance Program as a contract deliverable. The On Site Maintenance Program shall be submitted for approval by WMATA engineering.

4.5.4 The Contractor shall maintain an incident log as part of the software maintenance program, recording therein all deviations from normative operations, and all corrective actions taken. The incident log shall be submitted to WMATA annually and at the end of the contract period.

4.6 As-Built Documentation

The Contractor shall provide a complete set of AS-Built documentation in printed and electronic format. Documentation shall include drawings depicting system architecture, operating procedures, maintenance procedures, recovery procedures, and other necessary
documentation. Drawings shall be in both AutoCAD (or native) and PDF format. All drawings shall be readable on 11 X 17 inch paper.

The contractor shall provide all software licenses to fully outfit a software development lab.

4.7 Training

4.7.1 The Contractor shall provide all materials and documentation for training for operation and maintenance of the system for approximately ten (10) WMATA personnel at WMATA, and shall not be concurrent with the stand-up assistance and training. After award of contract, the Contractor shall submit a formal Training Plan as a contract deliverable. The training plan shall be submitted for approval by WMATA engineering.

The contractor shall provide all software licenses to fully outfit a training lab.

4.8 Computer Hardware Requirements

The Contractor shall submit a list of hardware requirements for the major components of the system to include, but not limited to, the Network Video Recorder (NVR) Storage machines, the Video Viewing Stations, the Video Retrieval Stations, and the Authentication and Authorization (A&A) Master Servers.

4.9 Periodic In-Process Review (IPR).

The Contractor shall participate in formal and informal In-Process Reviews (IPR) concerning performance related issues on an as needed basis.

4.10 Monthly Status Report.

The Contractor shall prepare a Monthly Status Report (MSR) containing all program and cost information. The format shall include the contract number and project number, a brief task description, and the reporting period. It shall also contain staffing, cost, deliverable data and a summary of activity accomplished by individuals in Specific Tasks. It may also include any significant issues, problems and resolutions. This report shall also cover but is not limited to the following categories of information; Labor Hours for the Reporting Period and Cumulative to Date, Other Direct Costs for the Reporting Period and Cumulative to Date, Staffing and turnover rate, as applicable.

4.11 Project Schedule

4.11.1 The contractor shall submit a formal project schedule as a contract deliverable. This schedule shall be in MS Project. The schedule shall be updated and included with the monthly status report. As part of the technical proposal, a detail listing of tasks to be performed by the Contractor shall be submitted.
## 4.12 Deliverables

<table>
<thead>
<tr>
<th>REF</th>
<th>Deliverable Title</th>
<th>Due Date/Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.4.4</td>
<td>System Architecture &amp; 60% Design Submittals</td>
<td>NTP + 30 days</td>
</tr>
<tr>
<td>4.4.15</td>
<td>90% Design Submittals</td>
<td>As Required</td>
</tr>
<tr>
<td>4.4.15</td>
<td>100% Design Submittals</td>
<td>As Required</td>
</tr>
<tr>
<td>4.11</td>
<td>Project Schedule</td>
<td>NTP + 30 days</td>
</tr>
<tr>
<td>4.2.2</td>
<td>System Interface Listing</td>
<td>NTP + 30 days</td>
</tr>
<tr>
<td>4.8</td>
<td>Hardware Requirements/Coordination/Integration</td>
<td>NTP + 30 days</td>
</tr>
<tr>
<td>4.4</td>
<td>System Configuration</td>
<td>As Required</td>
</tr>
<tr>
<td>4.4</td>
<td>System Commissioning</td>
<td>As Required</td>
</tr>
<tr>
<td>4.4.12</td>
<td>System Acceptance Testing</td>
<td>As Required</td>
</tr>
<tr>
<td>4.4.8.1</td>
<td>Customization WMATA Unique Screens - Overview</td>
<td>NTP + 90 days</td>
</tr>
<tr>
<td>4.4.8.2</td>
<td>Customization WMATA Unique Screens - Kiosks</td>
<td>NTP + 365 days</td>
</tr>
<tr>
<td>4.4.8.3</td>
<td>Customization WMATA Unique Screens - Guard Shack - Bus</td>
<td>NTP + 90 days</td>
</tr>
<tr>
<td>4.4.8.4</td>
<td>Customization WMATA Unique Screens - Guard Shack - Rail - Option</td>
<td>NTP + 90 days</td>
</tr>
<tr>
<td>4.4.8.5</td>
<td>Customization WMATA Unique Screens - Multiple OCC</td>
<td>NTP + 300 days</td>
</tr>
<tr>
<td>4.4.8.6</td>
<td>Customization WMATA Unique Screens - Undefined</td>
<td>As Required</td>
</tr>
<tr>
<td>4.4.9</td>
<td>Customization WMATA Unique Reports</td>
<td>As Required</td>
</tr>
<tr>
<td>4.4.6</td>
<td>Network Analysis &amp; Design</td>
<td>NTP + 30 days</td>
</tr>
<tr>
<td>4.4.6</td>
<td>Network Testing</td>
<td>As Required</td>
</tr>
<tr>
<td>4.4.5</td>
<td>Data Storage Analysis &amp; Design</td>
<td>NTP + 30 days</td>
</tr>
<tr>
<td>4.4.5</td>
<td>Data Storage Testing</td>
<td>As Required</td>
</tr>
<tr>
<td>4.4.7</td>
<td>Security Analysis &amp; Design</td>
<td>NTP + 30 days</td>
</tr>
<tr>
<td>4.4.7</td>
<td>Security Testing</td>
<td>As Required</td>
</tr>
<tr>
<td>4.4.13</td>
<td>Training Plan</td>
<td>NTP + 90 days</td>
</tr>
<tr>
<td>4.4.13</td>
<td>Training Program</td>
<td>NTP + 180 days</td>
</tr>
<tr>
<td>4.6</td>
<td>System Documentation</td>
<td>As Required</td>
</tr>
<tr>
<td></td>
<td>Miscellaneous Material</td>
<td>As Required</td>
</tr>
<tr>
<td></td>
<td>Software Licenses</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>-----------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>Redundant A&amp;A Master Server</td>
<td>NTP + 90 days</td>
</tr>
<tr>
<td>4.1</td>
<td>NVR Storage Machines - Station - Grant Metro Security Cameras</td>
<td>NTP + 120 days</td>
</tr>
<tr>
<td>4.1</td>
<td>NVR Storage Machines - Station - Grant WMATA CCTV/Alarm Detection Integration and Central Monitoring</td>
<td>NTP + 365 days</td>
</tr>
<tr>
<td>4.1</td>
<td>NVR Storage Machines - Rail Yard - Option</td>
<td>NTP + 300 days</td>
</tr>
<tr>
<td>4.1</td>
<td>NVR Storage Machines - Bus Garage</td>
<td>NTP + 120 days</td>
</tr>
<tr>
<td>4.1</td>
<td>NVR Storage Machines - Misc Bldg</td>
<td>As Required</td>
</tr>
<tr>
<td>4.1</td>
<td>NVR Storage Machines - Parking Garage</td>
<td>As Required</td>
</tr>
<tr>
<td>4.1</td>
<td>System Admin Console</td>
<td>NTP + 90 days</td>
</tr>
<tr>
<td>4.1</td>
<td>Viewing Station - Kiosk</td>
<td>NTP + 365 days</td>
</tr>
<tr>
<td>4.1</td>
<td>Viewing Station - Guard Shack - Bus</td>
<td>NTP + 120 days</td>
</tr>
<tr>
<td>4.1</td>
<td>Viewing Station - Guard Shack - Rail - Option</td>
<td>NTP + 300 days</td>
</tr>
<tr>
<td>4.1</td>
<td>Viewing Station - Control Center Major</td>
<td>NTP + 365 days</td>
</tr>
<tr>
<td>4.1</td>
<td>Viewing Station - Office</td>
<td>NTP + 120 days</td>
</tr>
<tr>
<td>4.1</td>
<td>Viewings Station - Local Partners - Metro Security Cameras</td>
<td>NTP + 120 days</td>
</tr>
<tr>
<td>4.1</td>
<td>Viewings Station - Local Partners - WMATA CCTV/Alarm Detection Integration and Central Monitoring</td>
<td>NTP + 365 days</td>
</tr>
<tr>
<td>4.1</td>
<td>Video Retrieval Console</td>
<td>NTP + 90 days</td>
</tr>
<tr>
<td>4.1</td>
<td>Video Wall License - OPTION</td>
<td>NTP + 365 days</td>
</tr>
<tr>
<td>4.1</td>
<td>Video Wall Configuration Services - OPTION</td>
<td>NTP + 365 days</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Video Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2</td>
<td>Video Analytic Configuration Services - Prototype - Grant Shaft / Portal Detection and Sonet Ring - Option</td>
</tr>
<tr>
<td>4.2</td>
<td>Video Analytic Configuration Services - EOP Prototype - Grant Smart CCTV and Enhanced Gate Security at Rail Station Platform Ends - Option</td>
</tr>
<tr>
<td>4.2</td>
<td>Video Analytic Configuration Services - PSS Bus Prototype</td>
</tr>
<tr>
<td>4.2</td>
<td>Video Analytic Configuration Services - PSS Rail Prototype - Option</td>
</tr>
<tr>
<td>4.2</td>
<td>Video Analytic License - Grant Shaft / Portal Detection and Sonet Ring - OPTION</td>
</tr>
<tr>
<td>4.2</td>
<td>Video Analytic Configuration Services - Deployment - Grant Shaft / Portal Detection and Sonet Ring - OPTION</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>4.2</td>
<td>Video Analytic License - EOP - Grant Smart CCTV and Enhanced Gate Security at Rail Station Platform Ends - OPTION</td>
</tr>
<tr>
<td>4.2</td>
<td>Video Analytic Configuration Services - EOP Deployment - Grant Smart CCTV and Enhanced Gate Security at Rail Station Platform Ends - OPTION</td>
</tr>
<tr>
<td>4.2</td>
<td>Video Analytic License - PSS Bus - OPTION</td>
</tr>
<tr>
<td>4.2</td>
<td>Video Analytic Configuration Services - PSS Bus Deployment - OPTION</td>
</tr>
<tr>
<td>4.2</td>
<td>Video Analytic License - PSS Rail - OPTION</td>
</tr>
<tr>
<td>4.2</td>
<td>Video Analytic Configuration Services - PSS Rail Deployment - OPTION</td>
</tr>
<tr>
<td></td>
<td><strong>PSIM</strong></td>
</tr>
<tr>
<td>4.3</td>
<td>PSIM Servers License - Grant Supplemental Bus Garage - OPTION</td>
</tr>
<tr>
<td>4.3</td>
<td>PSIM Clients License - Grant Supplemental Bus Garage - OPTION</td>
</tr>
<tr>
<td>4.3</td>
<td>PSIM Configuration Services - Grant Supplemental Bus Garage - OPTION</td>
</tr>
<tr>
<td>4.3</td>
<td>PSIM Servers License - Grant WMATA CCTV/Alarm Detection Integration and Central Monitoring - OPTION</td>
</tr>
<tr>
<td>4.3</td>
<td>PSIM Clients License - Grant WMATA CCTV/Alarm Detection Integration and Central Monitoring - OPTION</td>
</tr>
<tr>
<td>4.3</td>
<td>PSIM Configuration Services - Grant WMATA CCTV/Alarm Detection Integration and Central Monitoring - OPTION</td>
</tr>
<tr>
<td>4.3</td>
<td>PSIM Servers License - Grant Rail Yard Hardening - OPTION</td>
</tr>
<tr>
<td>4.3</td>
<td>PSIM Clients License - Grant Rail Yard Hardening - OPTION</td>
</tr>
<tr>
<td>4.3</td>
<td>PSIM Configuration Services - Grant Rail Yard Hardening - OPTION</td>
</tr>
<tr>
<td>4.3</td>
<td>Integration Interfaces - CBEMIS - OPTION</td>
</tr>
<tr>
<td>4.3</td>
<td>Integration Interfaces - COMMEND - OPTION</td>
</tr>
<tr>
<td>4.3</td>
<td>Integration Interfaces - Edwards EST3 - OPTION</td>
</tr>
<tr>
<td>4.3</td>
<td>Integration Interfaces - Other 1 - OPTION</td>
</tr>
<tr>
<td>4.9</td>
<td>In-process Review (IPR)</td>
</tr>
<tr>
<td>4.10</td>
<td>Monthly Status Report</td>
</tr>
</tbody>
</table>
5. PERFORMANCE REQUIREMENTS

5.1 Video Management Software and Hardware

5.1.1 VMS Architecture

5.1.1.1 The VMS shall have a flexible, open Video over IP architecture built on accepted industry standards that facilitate integration with IT infrastructures.

5.1.1.2 The VMS shall have flexible, open architecture that supports unified workstation logon based on Windows authentication.

5.1.1.3 The VMS shall have flexible, open configuration architecture that facilitates NAT Traversing for the Viewing and Client SDK connections.

5.1.1.4 The VMS shall have flexible, open configuration architecture that facilitates Firewalls Traversing for the Viewing and Client SDK connections.

5.1.1.5 The VMS shall have flexible configuration architecture that facilitates video resolution transcoding in order to stream video in a low bandwidth (as low as 56 kbps) connection to the Viewing and Client SDK applications.

5.1.1.6 The VMS shall have flexible, throttling technology that facilitates video streaming support for both software and hardware VPN for Viewing and Client SDK remote application connections.

5.1.1.7 The VMS shall have flexible, open architecture built on accepted industry standards that facilitate DNS/DHCP support for servers.

5.1.1.8 The VMS shall support Multiple NIC for Servers from a different Network that allows Viewing or Client SDK to reach the Video LAN.

5.1.1.9 The VMS shall have a distributed fault-tolerant, failover database architecture. The distributed server architecture allows for each subsystem to operate in an independent mode, without affecting video recording or live viewing.

5.1.1.10 The database shall be redundant, using two separate servers, and shall be initially and continuously synchronized with a master server database.

5.1.1.11 The Master Server shall be redundant, using two separate servers, and shall be initially and continuously synchronized with a master server database.

5.1.1.12 The VMS shall possess an internal watchdog to detect and recover from the unlikely occurrence of system lockup.
5.1.1.13 The VMS shall provide support for IP (network) cameras from multiple third party manufacturers including H.264.

5.1.1.14 The VMS shall not use multiplexing or timed division technology for analog video recording. All analog camera sources shall be digitally recorded.

5.1.1.15 The VMS shall be able to support video motion detection natively. This operation can be executed by the edge device or the IP Camera. Enabling motion detection shall be performed either:

5.1.1.16 On a continuous basis
5.1.1.17 Scheduled for particular times, dates, days, months, etc.
5.1.1.18 Defined areas of interest through an easy-to-use user interface using simple editing tools
5.1.1.19 At a defined level of sensitivity.

5.1.1.20 Not Used

5.1.1.21 All text displayed in the user interface shall be stored in a database to allow for easy translation to another language.

5.1.1.22 The VMS shall be designed to work with cameras that generate a standard NTSC or PAL composite video signal.

5.1.1.23 The VMS shall support a variety of video matrix switcher devices, code generators, and PTZ cameras from different manufacturers.

5.1.1.24 The Recorders will use a standard Ethernet connection for video input via TCP/UDP/IP.

5.1.1.25 The Recorders will use standard COTS server technology and storage attachments.

5.1.1.26 The VMS shall be capable of supporting large organizations with systems at multiple site locations linked via LAN / WAN connections.

5.1.2 VMS Interfaces

5.1.2.1 The VMS shall support dual video encoding of different edge devices. the interface of standard NTSC or PAL cameras that support dual video encoding.

5.1.2.2 The VMS shall support the ability to support third-party IP cameras via the Service SDK which can be used to develop adaptors for any IP camera.

5.1.2.3 The VMS shall support H.264 MJPEG and MPEG-4 compression from edge devices and IP cameras.
5.1.2.4 The VMS shall support H264 de-compression on the Workstations.

5.1.2.5 The VMS shall support an asynchronous serial port for the RS-422 or RS-485 signal levels that can be programmed for data rates of up to 230 kbps.

5.1.2.6 The RS-485 mode shall support the 2-wire and 4-wire interfaces.

5.1.2.7 The VMS shall support an unlimited number of RS-232 asynchronous serial ports that can be programmed for data rates of up to 230 kbps.

5.1.2.8 The VMS shall support an unlimited number of dry-contact inputs.

5.1.2.9 The VMS platform shall support an unlimited number of dry-contact outputs.

5.1.2.10 The VMS shall operate over a Local Area Network (LAN) / Wide Area Network (WAN), using a standard Ethernet 100/1000 Base-T connection.

5.1.2.11 The VMS shall support both Unicast and multicast over the enabled network.

5.1.2.12 The VMS shall transmit video using the UDP/IP or TCP/IP communication protocol.

5.1.2.13 The VMS shall transmit all command and control messages using the TCP/IP protocol.

5.1.2.14 The VMS shall generate alerts on disabled camera inputs.

5.1.2.15 The VMS shall support the ability to support third-party keyboards via the Service SDK which can be used to develop adaptors for any third party Keyboard.

5.1.2.16 The VMS shall support additional PTZ Keyboard Camera Commands such as:

5.1.2.17 Call up Patterns
5.1.2.18 Camera Menu Commands
5.1.2.19 Auxiliaries
5.1.2.20 Home Position
5.1.2.21 Flip Camera 180 degrees.

5.1.3 VMS Video Device Support

5.1.3.1 Authentication and Authorization (A&A) Master Servers

5.1.3.2 The A&A Master Server shall maintain cohesive operations of all of the components in the VMS, including the VMS database.

5.1.3.3 The A&A Master Server cluster shall support an unlimited quantity of cameras.
5.1.3.4 The Master Server shall be hosted on a Commercial-Off-The-Shelf (COTS) computer server.

5.1.3.5 The Master Server shall be redundant, separated geographically, and connected via a fiber optic link.

5.1.3.6 The hardware requirements for the Master Server shall be identified in the technical proposal

5.1.4 NVR Storage machines

5.1.4.1 The VMS Recorders shall store video on Commercial Off-The-Shelf (COTS) equipment using hard drives as storage medium. The recorders also have the capability to support the attachment of external storage devices.

5.1.4.2 The VMS Recorder Server shall have the ability to run Master Server functions, Recording and the Viewing application simultaneously for cost-effective deployments.

5.1.4.3 The Recorder shall run autonomously and continue to Recorder once configuration is received.

5.1.4.4 The Recorder shall Fail-over to another recorder or group of Recorders dynamically without user intervention.

5.1.4.5 The VMS Recorder Server shall have the ability to record simultaneously 48 cameras at full H.264 resolution 4CIF @ 30 FPS.

5.1.4.6 The hardware requirements for the NVR Storage machines shall be identified in the technical proposal.

5.1.5 Enterprise Storage Manager - Option

5.1.5.1 The Enterprise Storage Manager (ESM) shall be capable of offering long-term video storage.

5.1.5.2 The ESM shall receive important video from multiple Recorders for offsite or long-term storage.

5.1.5.3 ESM shall allow for the support of long-term video storage using hard drives as storage medium. It shall support virtually any central disk storage device, including disk arrays with iSCSI connectivity and Storage Area Network (SAN) devices

5.1.5.4 The ESM shall be redundant, separated geographically, and connected via a fiber optic link.
5.1.5.5 The hardware requirements for the Enterprise Storage Manager shall be identified in the technical proposal.

5.1.6 Media Gateway Server – Option

5.1.6.1 The Media Gateway Server shall be capable of running all video transcoding and WAN transport services. The Media Gateway Server shall transcode received video from IP cameras or edge devices at a certain resolution and then convert and send the low resolution video through a bandwidth limited WAN link.

5.1.6.3 The Media Gateway shall properly packetize video to transverse NAT’s and Firewalls using IP with a maximum of 2 ports.

5.1.6.4 The Media Gateway shall support Viewing User Priorities when multiple remote Viewing user requests for video exceed the bandwidth of the WAN/LAN link.

5.1.6.5 The hardware requirements for the Media Gateway Server machines shall be identified in the technical proposal.

5.1.7 Administration Console

5.1.7.1 The VMS shall provide an Administration Console client application to configure cameras, recorders, schedules, users and system functions.

5.1.7.2 The hardware requirements for the Administrative Console shall be identified in the technical proposal.

5.1.8 Viewing Stations

5.1.8.1 The VMS shall provide a Viewing Station client application to operate and view live/recorded video.

5.1.8.2 Customized viewing stations shall be developed for

- Kiosks
- Guard shacks
- Bus garages
- Rail yards
- Miscellaneous buildings
- Other - TBD

5.1.8.3 The hardware requirements for the viewing stations shall be identified in the technical proposal.

5.1.8.4 Not Used
5.1.10 Retrieval Console

5.1.9.1 The VMS shall provide a Video Retrieval client application that allows video retrieval and analysis services.

5.1.9.2 The hardware requirements for the Video Retrieval shall be identified in the technical proposal.

5.1.10 Control Console

5.1.10.1 The VMS shall have a Control Console graphical user interface (GUI) that allows the user to quickly configure and apply the following parameters:

- All cameras configurations
- All recorder configurations
- All work schedules
- User and access rights and privileges
- Create schedules and apply them to specific camera groups
- Configure cameras and recorders individually and as a group in system components.

5.1.10.2 The user shall have the ability to add and edit interactive site plans and Maps.

5.1.10.3 The Control Console shall be controlled by access rights assigned by the System Administrator.

- Full access to all functions
- Limited to only System Configuration
- Limited to only Health Check viewing

5.1.11 Viewing

5.1.11.1 The VMS shall have a Viewing GUI which shall allow users to view live video, retrieve recorded video, and export video from a workstation PC.

5.1.11.2 The VMS Viewing application shall enable users to manage multiple windows and perform multiple tasks simultaneously, including the following:

- Select time preference format AM/PM or 24H
- Quick video query button
- Hot function keys
- 8x Playback
- Change Camera Name
- Viewing live or recorded video in multiple windows, including video from multiple Digital Video Recorders and multiple sites
- Control PTZ cameras
- Able to lock the PTZ control for a camera based on user rights and priority levels.
- The ability to takeover a PTZ function based on user rights and priority levels.
- Export video to digital media output device such as a CD
- Submit and manage multiple requests for video
- Support for time synchronized play back of video on up to 16 windows
- Support for camera groups and maps
- Support for camera presets in a user-defined, multi-level tree structure. The following guidelines shall apply:
  (i) Each group has a user-defined name and user-defined contents.
  (ii) A group can contain cameras and/or other groups.
  (iii) Users can define multiple levels of groups and maps.
  (iv) A camera can be included in more than one group.
  (v) Users can select or drag-and-drop individual cameras to request video for playback or to open live video windows.

5.1.11.3 The VMS shall allow the user to open, move, and size multiple independent video windows as needed:

- Single window
- 2 x 2 windows arranged in two rows of two windows each
- 5 x 1 windows arranged in one large window, surrounded by multiple tiles
- Quad: 4 windows arranged in two rows of two windows each
- 3 x 3: 9 windows arranged in three rows of three windows each
- 4 x 4: 16 windows arranged in four rows of four windows each

5.1.11.4 The VMS shall support the ability to preserve aspect ratio.

5.1.11.5 The VMS shall support digital zoom on live or recorded video, without requiring a video pause.

5.1.11.6 The VMS shall enable/disable video de-Interlacing

5.1.11.7 Image Toolkit software shall include the following capabilities:

- Add the date and time to the image
- Add text annotation to the image
- Copy the image to the clipboard so that it can be pasted into other applications
- Print the image
- Save the image to disk in various standard file formats
- Adjust the brightness and/or contrast of the image
- Convert a color image to grayscale
- Apply filters to the image to smooth or sharpen
- Apply edge detection to highlight borders and surfaces of objects within the image
5.1.11.8 The VMS Viewing application shall allow users to select video to be exported and from a precise start time and end time.

5.1.11.9 The VMS shall provide a default digital certificate for signing video clips that are exported.

5.1.11.10 The VMS shall export an image in Windows Bitmap format.

5.1.11.11 The VMS shall export an image in JPEG (Joint Photographic Experts Group) format.

5.1.11.12 The VMS shall enable a user to open live video windows.

5.1.11.13 The VMS shall enable a user to view live video from multiple digital recorders and sites.

5.1.11.14 The VMS shall enable users to request video from one camera or a group of cameras at a specified date and time and for a specified duration:

- Include drag-and-drop from the camera tree for camera selection
- Provide typical calendar control to ease selection of the year, month, and day
- Provide time and duration specified by data entry or by dragging the mouse over a time range
- Include video request defaults to the last five minutes of video from the selected camera or group
- View live or historical alarm events and associated video.

5.1.11.15 The VMS shall support attachment of video to documents such as incident reports and ease retrieval of reports and associated video.

5.1.11.16 The VMS shall support processing of video requests.

5.1.11.17 The VMS shall support control of video playback including:

- Buttons to start and stop playback from the current video position
- Button to step forward or backward through the video in single time increments
- Button to step forward or backward through the video in single frame increments
- Button to step forward or backward through the video in multiple frame increments
- Button for moving through video in reverse
- Ability to cause video to loop continuously
- Positioning controls: Slider bar and buttons to quickly and conveniently position to the beginning, end, or any other time, within the video clip
- Speed control: Slider bar to control the rate of playback
5.1.11.18 The VMS shall support scanning of recorded video for activity thru an energy graph that indicates levels of activity.

5.1.11.19 The VMS shall support scanning of recorded video for motion in all or specific Areas of Interest and shall have the ability to set the motion sensitivity and sampling time.

5.1.11.20 The VMS shall authenticate video to enable users to verify that the video has not been modified since it was recorded.

5.1.11.21 The VMS shall have live video windows consistent with video playback windows in appearance and operation.

5.1.11.22 The VMS shall control PTZ cameras.

5.1.11.23 The VMS shall allow the entire live video window to be a mouse-sensitive area for PTZ control.

5.1.11.24 The VMS shall provide an optional “heads up display” (HUD) to overlay the video in order to provide a visual indication of the window areas that control zoom, focus, and iris functions.

5.1.11.25 The VMS shall support camera presets by providing a toolbar or other GUI method for working with camera presets when viewing live video from a PTZ camera.

5.1.11.26 The VMS shall provide the ability to view camera tours through a graphical, icon-based user interface.

5.1.11.27 The VMS shall allow the user to access a calendar view to query by month, day, and year, and by hour, minute, and second.

5.1.11.28 The VMS shall allow the user to access a hierarchical tree to manage icons that represent cameras.

5.1.11.29 The VMS shall allow the administrator to configure access privileges and rights for every user. Based on their log on to any workstation the user rights access and privileges will follow them.

5.1.11.30 It will be possible to restrict the operations that are available in the Viewing application. It shall be possible to restrict or enable the following functionality:

- Live Video
- PTZ Control
- Assign PTZ priorities for take over function
- Digital zoom
- Camera Menu
• Recorded Video
• Export Video
• Investigation Management
• Alarm Notification
• Alarm viewing
• Alarm History
• Cameras
• Tours
• Salvos
• Maps
• Sites
• Remote Viewing Access
• Remote Viewing Maximum Bandwidth
• Remote Viewing Priority

5.1.11.31 The VMS shall allow the user to select the following patterns functionality:

• Configure PTZ Presets
• Call up Camera Patterns
• Record Patterns
• Stop Recording Pattern

5.1.11.32 The VMS shall allow the user to access a third-party camera menu:

• Allow a user to access the internal menu of a camera directly from Viewing.
• Menu will be available for any of the supported protocols.

5.1.11.33 The VMS shall allow the user to call up PTZ Presets.

5.1.11.34 The VMS shall allow the user to call up PTZ Patterns.

5.1.11.35 The VMS shall allow the user to defines patterns can be run and recorded from Viewing.

5.1.11.36 The VMS shall support HD resolution.

5.1.11.37 The VMS shall allow support MJPEG support in Viewing.

5.1.11.38 The VMS shall allow support H.264 support in Viewing

5.1.12 Client SDK Access Privileges and user Rights

5.1.12.1 The Client SDK shall be controlled by access rights and privileges assigned by the System Administrator.
• Live Video
• PTZ Control
• PTZ priorities
• Camera Menu
• Recorded Video
• Export Video
• Investigation Management
• Alarm Notification
• Alarm viewing
• Alarm History
• Cameras
• Tours
• Salvos
• Maps
• Sites
• Remote Viewing Access
• Remote Viewing Maximum Bandwidth
• Remote Viewing Priority
• Bi-Directional bookmark
• Investigation Management
• Activity Scan energy graph
• Audit for SDK client functionality and use

5.1.13 Analytics Functions

5.1.13.1 The VMS analytics shall be tightly integrated with the VMS solution.

5.1.13.2 Not Used

5.1.13.3 The VMS shall provide the ability to acquire and track an object within a predefined field of view on selected cameras.

5.1.13.4 The VMS shall support object-based algorithms and shall provide the following functionality:

• Learn the scene
• Detect and track objects
• Adapt to a changing outdoor environment
• Ignore environmental changes including rain, hail, wind, swaying trees, and gradual light changes
• Classify objects
• Detect tripwire events
• Detect multi-line tripwire events
• Detect “enters”, “exits”, “appears”, “disappears”, “inside of”, “loitering”, “leave behind”, “taken away” events
- Detect scene change events
- Create object size and size change filters

5.1.13.5 The VMS shall be able to combine object tracking with object classification to allow the detection of specific objects in a region of interest, while ignoring other object types.

5.1.13.6 The VMS shall support alarming and actions based on the VMS rule engine when an object is detected, classified, and tracked.

5.1.14 Analytics Rule Builder

5.1.14.1 The VMS shall provide the ability to configure multiple rules on a per camera basis.

5.1.14.2 The VMS shall provide the ability to set up security rules for surveillance cameras.

5.1.14.3 The VMS shall display the video of the rule violation and graphically depict how and which object triggered the event, including vector information. The alert and violation object shall be displayed in the VMS Viewing application with pre- and post-video.

5.1.15 Virtual Matrix

5.1.15.1 The VMS shall automatically distribute live and recorded video to video walls, and computers across dispersed user locations in a bandwidth-efficient manner, effectively replacing the most commonly used features of legacy cross-point matrices.

5.1.15.2 The Virtual Matrix shall have the capability to interface with video walls via a CCTV keyboard connected to a decoder.

5.1.15.3 The Virtual Matrix shall have the ability to play back a video sequence on an analog monitor upon activation of an alarm or event. The length of the playback sequence shall be configurable, and may include pre- and post-video.

5.1.15.4 The Virtual Matrix shall have the capability of creating camera sequences with the following functionality:

- Each sequence shall support up to 100 cameras.
- Each camera in the sequence shall have its own individual dwell time, from 1 to 60 seconds.
- Each entry in a sequence shall have the capacity to trigger camera presets, patterns, or auxiliaries.
- Multiple users shall be able to view the same camera sequence simultaneously; users are able to pause the sequence without affecting other viewers.
- The operator shall be able to control, through an integrated CCTV keyboard, pan-tilt-zoom, iris, focus, dome relays, and dome presets to an analog monitor.
The VMS shall enable the user to assign cameras to monitors by attaching any adapted CCTV keyboard using the following methods:
- Select a camera from the camera tree in the Control Center onto an associated monitor
- Enter a camera number from the keyboard
- Enable the user to switch between monitor views on the analog monitors by using the specified keyboard buttons for multiple cameras
- Provide a function to start a tour that can be programmed through the CCTV keyboard
- The VMS shall support camera tours. It shall provide comprehensive features to take advantage of camera tours, including:
  - Providing configuration functionality to enable authorized users to view and modify camera tour definitions
  - Providing configuration functionality to enable authorized to takeover or lock out other lower priority users.
- Allowing the creation of multiple camera tours and salvos
- Allowing multiple cameras in each camera tour
- Allowing the definition of a preset and dwell time for each camera
- Allowing the definition of dwell time for all cameras in one operation

5.1.16 Event Management

5.1.16.1 The VMS shall have a sophisticated rule-based engine with powerful analytics capabilities that provide the following actions in response to events and behaviors:

- Automatic event notification
- Video distribution
- Process activation

5.1.16.2 The automated responses to behaviors shall be:

- Call a Camera Preset
- Run a Camera Pattern
- Change Output Relay State
- E-mail notification
- Send messages
- Output alarms to the Client Software Development Kit (SDK) interface

5.1.17 Video Recording

5.1.17.1 The VMS Recorder shall be capable of performing multiple tasks simultaneously, and within practical limits, no task shall interfere with any other task. The VMS shall be able to perform the following tasks simultaneously:

5.1.17.2 It shall be able to perform the following tasks simultaneously:
• Digitizing and compressing video and calculating digital signatures for video authentication.
• Writing video to files on local hard disks and maintaining an accurate index of the stored video files.
• Deleting older video files as needed, to free up space to record newer video files.
• Selectively transferring recorded video to long-term storage media.

5.1.17.3 The VMS shall be capable of supporting dual streaming.

5.1.17.4 The VMS shall be capable of performing the following tasks related to alarms:
• Executing video image analysis algorithms, including activity detection and video loss detection.
• Receiving signals from alarm inputs and generating alarm messages.
• Processing alarm response instructions including calling, changing recording modes, and controlling alarm relay outputs.
• Forwarding alarms to a Viewing workstation, analog video monitor, or video wall that supports MPEG-4.

5.1.17.5 The VMS shall be capable of performing the following tasks and shall support the following recording modes:
• Continuous recording: In the simplest mode, the Digital Video Recorder units must record video 24 hours per day, 7 days per week, or as per user defined schedules
• Event recording
• Augment the Recording Quality based on an event.

5.1.17.6 The VMS shall be capable of scheduled recording, enabling system administrators to:
• Establish a recording schedule based on hours of the day and days of the week.
• Specify the times during which each camera will be recorded, along with the recorder settings to be used during each period, including the frame rate, resolution, and quality settings.
• Define alarms or event responses, including instructions to trigger recording of specified cameras at specified frame rates and quality settings. Alarm response shall include the following recording capabilities:
  1) Start recording camera not currently being recorded.
  2) Supplement continuous scheduled or event recording by changing the recording mode or triggering recording of the same camera on a different recorder in a different video format. For example, the VMS may be configured to record cost-effective low frame rate video during non-alarm
periods, and then start recording on high frame rate real-time recorders in response to alarm events.

- Selectively copy video to long-term storage to ESM (Enterprise Storage Manager). System administrators shall be able to determine whether video will be retained on long-term storage media for each continuous or scheduled recording instruction.
- Automatically retain video on long-term storage media when video is recorded as part of a defined response to an alarm event.
- Perform activity recording: the VMS shall support an event recording mode designed for handling activity detection events during periods when frequent activity is expected but does not constitute an alarm event. Activity detection events shall be handled internally by the Digital Video Recorders instead of triggering an alarm response. This mode preserves online video storage space by only retaining video in which activity has been detected.

5.1.17.7 The VMS shall be capable of supporting multiple recorders, including the ability to:

- Add, modify, and remove recorders from the system
- Perform failover of recorders
- Apply global recorder settings or edit existing individual recorder properties
  1) Associate cameras, recorders, and schedule assignments

5.1.17.8 The VMS shall support failover recording.

The failover recorder shall act as a hot standby, ready to take over the functions of a primary Recorder. No action from the user shall be required.

5.1.18 Long Term Storage

5.1.18.1 The VMS shall offer Long Term Storage for supporting long-term or off-site storage to any central disk storage device. It shall support any central disk storage device, including disk arrays with iSCSI connectivity and Storage Area Network (SAN) devices.

5.1.19 Alarm Configuration

5.1.19.1 The VMS shall process alarms from a variety of alarm sources. Each type of alarm source shall have an “OFF” state (normal) and an “ON” state (triggered). The VMS shall monitor the state of alarm sources and generate alarm messages based on state changes.

5.1.19.2 The VMS system components shall provide alarm contacts to receive signals from electrical devices. Contacts are configurable as “normally open” or “normally closed”.

Page 29 of 65
5.1.19.3 The VMS shall be capable of generating an alarm based on video image analysis to detect activity through motion detection or object recognition in the areas of interest, or directional vectors. The absence of activity shall correspond to the OFF state of the alarm source; when activity is detected, the state of the alarm source shall be ON.

5.1.19.4 The VMS shall be capable of providing a way to define the areas of interest for activity detection for a particular camera.

5.1.19.5 The VMS shall be capable of enabling activity detection sensitivity to be configurable.

5.1.19.6 The VMS shall be capable of alarming when video loss is detected from the devices due to lost camera signals.

5.1.20 Alarm Responses

5.1.20.1 The VMS shall be able to configure alarm sources and responses in a schedule. The alarm source configuration and response shall depend on the time of day and/or day of the week.

5.1.20.2 The alarm response shall consist of various types of instructions to be executed by the VMS in response to an alarm message that can be generated by an alarm source.

5.1.20.3 The VMS shall support the following recording instructions: start recording or change the recording mode for one or more cameras connected to one or more Recorders.

5.1.20.4 The VMS shall support the following relay output instruction: control the state of one or more alarm relay outputs on Recorders or other system components such as edge devices or IP cameras.

5.1.20.5 The VMS shall support the following responses:

- Call a Camera Preset
- Run a Camera Pattern
- Assign a camera to a monitor
- Change output relay state
- Send a message with Net Send
- Send a e-mail
- Trigger an alarm

5.1.20.6 The VMS shall trigger contact closures on edge devices or IP cameras that are hardware equipped with this capability.

5.1.20.7 The VMS shall be able to display a text message to the users at the alarm monitoring station if they are using analog monitors.
5.1.20.8 The VMS shall be able to display/send an Alarm message to the Application Programming Interface for the Client SDK.

5.1.21 Video Storage Management

5.1.21.1 The VMS shall be capable of managing online storage. Storage shall be intelligently managed so that the video that is most likely to be requested by users will be retained online.

5.1.21.2 The VMS shall be capable of immediate storage on local hard disks.

5.1.21.3 The VMS shall be capable of circular overwrites: Online storage on the Recorder units shall be managed on a continuous circular overwrite basis.

5.1.21.4 The VMS shall be capable of event recording and selective online storage.

5.1.21.5 The VMS shall be capable of retaining non-event video online for a minimum amount of time, based on the Recorder hard disk space.

5.1.21.6 The VMS shall be capable of retaining video online after transfer to long-term storage (ESM); video shall be retained online on the Recorder to support immediate playback, even if the video has been successfully copied to long-term storage media.

5.1.22 Managing Long-Term Storage and Archiving

5.1.22.1 The VMS shall support automatic long term storage with Enterprise Storage Manager (ESM).

5.1.22.2 Long-term storage shall be implemented using separate storage attachments.

5.1.22.3 The VMS shall support multiple long-term storage devices.

5.1.22.4 The VMS shall be capable of independent operations between storage servers.

5.1.22.5 The VMS shall be capable of immediate transfer to long-term storage.

5.1.22.6 The VMS shall support the “ability to catch up” after storage server downtime: If a storage server must be taken out of service temporarily for maintenance, the VMS shall retain video designated for long-term storage online on Recorders. When the storage server is placed back in service, the storage server shall transfer video data to long-term storage faster than the rate at which new video is being recorded.

5.1.22.7 The VMS shall be capable of variable retention times, i.e., it shall support the segmentation of cameras into groups based on the video retention requirements so that video is retained for some cameras longer than for others.
5.1.23 Archived and Bookmarked Video

5.1.23.1 The VMS shall allow disks to be reserved for video archiving.

5.1.23.2 The VMS shall support the copy of bookmarked video to the appropriate archive storage media and ensure that the video will not be overwritten or deleted for the specified number of days.

5.1.23.3 The VMS shall allow any video clip that is attached to a report to be archived automatically. The video retention time shall be 60 days.

5.1.23.4 The VMS shall allow reports to include a data entry and reporting facility that enables users to enter data for reports, query the database to find reports, view reports, and export a HTML page with the ability to attach video clips and still images to a report.

5.1.24 Health Check

5.1.24.1 The VMS shall provide a Health Check application for live monitoring and detailed system performance metrics on system components, including all server-side software applications, edge devices, and IP cameras.

5.1.24.2 The VMS shall be capable of exporting performance analysis results.

5.1.24.3 The VMS shall offer a user interface designed to enable the management of the following:

- System logs
- System alerts
- Audit trail
- Performance
- Redirection to various outputs such as windows event log and e-mail

5.1.24.4 The VMS shall be capable of leveraging Microsoft Operations Manager (MOM) integration and service packs that can cover all aspects of the operating system software, application software, IT functions, and hardware platforms.

5.1.24.5 The VMS shall support configurable notification of any alert to administrators via email, net-send, console message, or any other MOM support responses.

5.1.24.6 The VMS shall support integration into enterprise-wide IT management systems such as HP Open View and Tivoli Enterprise Server though MOM or windows events.

5.1.24.7 The VMS shall be capable of real-time performance analysis capture.

5.1.25 Maps
5.1.25.1 The VMS shall support the mapping functionality where digital maps are used to represent the physical location of cameras and other devices throughout the surveillance system.

5.1.25.2 Maps shall have the ability to contain hyperlinks so as to create a hierarchy of interlinked maps.

5.1.25.3 The mapping functionality shall be able to import maps from any graphical software supporting BMP, JPEG, or GIF image formats.

5.1.25.4 Once a map is integrated, it can be viewed in the Viewing applications.

5.1.26 Audio

5.1.26.1 The VMS shall support the inclusion of audio in the video. The VMS Enterprise support unidirectional synchronized audio support for Live and Playback video. It allows for the following functions:

- Export of the audio along with the video
- Audio support with the Virtual Matrix
- Audio support using the Client SDK
- Supports 3 Compression modes: PCM, ULAW, GSM

5.1.27 Client Software Development Kit (SDK)

5.1.27.1 The VMS shall provide the ability to develop custom applications to access and control the system using an Application Programming Interface (API). Complete documentation of the API shall be provided.

5.1.27.2 Examples of API features shall include:

- Pre-Integration of Access Control Systems:
  1) Command Intercom System
  2) Pre-Integration Integration to Command and Control Systems
- The development of a custom Viewing application
- Integration with access control systems, to generate alarms and events in the VMS system
- Perform Virtual Matrix operations, for example, display live or playback video on analog monitors
- Play live video or query recorded video from cameras in a client application
- Query the alarm list from the VMS system, acknowledge VMS alarms, and subscribe to alarms to receive them in real time
- PTZ Commands supported in the Service SDK are available in the Client SDK
- Call up Camera Patterns from Client
- Access to Camera menu’s via Client
- Stream HD to Client example; Axis (1280x720) & SXGA (1280x1024)
- MJPEG streaming to Client
- Event Notification to Client example; Video Lost, Motion Detection, Input Relay
- Trigger a contact closure on any edge device or IP cameras that is hardware equipped with this capability.
- IP Camera Integrations such as Sony & Axis
- The interface shall be functional for any type of codec used (Verint, Axis, etc.)
- Support PTZ overlay
- Support Digital Zoom

5.1.28 Service SDK

5.1.28.1 The VMS shall provide the ability to develop custom adapters for hardware, using a complete application development interface. Complete documentation of this application development interface shall also be provided. Examples include:

- Integration of PTZ protocols
- Integration of IP cameras
- Integration of third party CCTV Keyboards

5.1.29 Mosaic Virtual Switching

5.1.29.1 The VMS shall provide the capability of a Mosaic Viewing workstation application which will provide the ability to automatically or manually stitch up to 4 adjacent standard NTSC or PAL cameras into a wide panoramic view.

5.1.29.2 The VMS shall provide the ease of use and speedy definition of 2-4 Cameras (adding cameras) to be stitched together to produce a panoramic view. This process shall take seconds to achieve.

5.1.29.3 The VMS shall provide the ability to save up 15 scenes.

5.1.29.4 The VMS shall provide the ability to automatically “stitch” views from pairs of adjacent cameras.

5.1.29.5 The VMS shall provide the ability to manually “stitch” views from pairs of adjacent cameras.

5.1.29.6 The VMS shall provide the ability to combine stitching methods to achieve the best possible scene.

5.1.29.7 The VMS shall provide the ability to save stitched scenes.

5.1.29.8 The VMS shall provide the ability for global scene transformations, including:
- Rotation of scene
- Correction of scene distortions caused by the stitching process

5.1.29.9 The VMS shall provide the ability to retrieve previously saved scenes for live viewing.

5.1.29.10 The VMS shall provide the ability to create up to three virtual PTZ cameras on the scene, allowing the user to drag and drop specific areas in separate windows.

5.1.29.11 The VMS shall provide the ability to provide a virtual PTZ including zoom in/out on the full panorama.

5.1.30 Camera Tampering Detection

5.1.30.1 The VMS shall support Camera Tampering Detection that is on the recorder and resident on the edge devices. The VMS shall monitor two types of tampering alerts that are communicated by the edge devices:

- Camera blocked fully or partially
- Out of Focus (OoF) or Camera Defocus – Image becomes blurred because of camera being defocused

5.2 PSIM Specifications

5.2.1 Contractor shall furnish and install Physical Security Interface Management system (PSIM) for handling all security operations-related tasks and improve work efficiency without changing the existing security systems’ functionality from a centralized workstation.

5.2.2 The system shall be able to integrate, connect and correlate information from security data and information from the following security subsystems:

5.2.2.1 CCTV management and control systems
5.2.2.2 Digital video recording systems
5.2.2.3 Physical access control systems
5.2.2.4 Intrusion Detection Systems
5.2.2.5 Badge management systems
5.2.2.6 Video analytics systems
5.2.2.7 Response Systems
5.2.2.8 Chemical/biological detection systems
5.2.2.9 Radioactivity detection systems
5.2.2.10 Phone Systems
5.2.2.11 Intercom systems
5.2.2.12 Motion detection systems
5.2.2.13 Radar Systems
5.2.2.14 Location based device systems (RFID, GPS devices, etc)
5.2.2.15 Computer Aided Dispatch Systems
5.2.2.16 Notification Systems
5.2.2.17 Building Management Systems
5.2.2.18 IT Systems Management Systems
5.2.2.19 Other related systems

5.2.3 The system shall be able to display alarms from security subsystems based on predefined policies and business logic.

5.2.4 The system shall enable the operator to quickly visualize the environment and assess alarm by reviewing related security information.

5.2.5 The system shall enable the operator to take action by sending an email, printing a report, dispatch with necessary information, etc.

PSIM Performance and Operating Requirement

5.2.6 General PSIM Display Functionality - The PSIM solution shall have the following general display functionality:

5.2.6.1 View and handle multiple alarms at one time

5.2.6.2 View multiple video windows at one time. Operators shall be able to resize and move video windows.

5.2.6.3 View windows in a single monitor, across multiple monitors or video walls

5.2.6.4 Access, display and manage events/alarms and related security data and information from subsystem based on priority and authority level.

5.2.6.5 View and manage detailed response procedures and tasks

5.2.6.6 Enable a single operator or multiple operators to monitor and control commands from connected subsystems, including all operational capabilities for detection, assessment, notification, entry control, and communications

5.2.6.7 Provide the rapid annunciation and display of alarms to facilitate evaluation and assessment

5.2.6.8 Enable different graphical user interface “skins” to be customized to provide a different look ’n feel.

5.2.7 Map Display - The PSIM solution shall have the following map display functionality:
5.2.7.1 View security environment through geospatial or fixed composite computer generated (JPEG, BMP, AutoCAD, etc.) map

5.2.7.2 Allow user to interactively drill down to specified security zones and sub-zones

5.2.7.3 Allow user to view sensor and related name from map console

5.2.7.4 Allow resources and objects to be tracked on map with geo-referenced “breadcrumb” trail.

5.2.7.5 Allow all resources, objects, sensors and elements on the map to be geo-referenced such that they have a real world coordinate.

5.2.7.6 Visually display a camera sensor with related camera orientation, camera range and camera field of view angle

5.2.7.7 Visually display an alarming sensor on map

5.2.7.8 Visually differentiate sensor alarm severities on map through different color and icon identifiers

5.2.7.9 Immediately view alarm details (including description, video, etc.) and investigate the alarm from the map

5.2.7.10 Allow user to choose camera from map to view live video

5.2.7.11 Allow user to choose camera and take live video image snapshot and save to file from any camera

5.2.7.12 Allow user to choose camera from map to move PTZ cameras

5.2.7.13 Allow user to choose camera icon from map to view recorded video from console

5.2.7.14 Allow user to choose camera to play, pause, stop, fast-forward, rewind, and play recorded video from preset time

5.2.7.15 Allow user to choose camera and take recorded video image snapshot and save to file or print from any live or recorded video

5.2.7.16 Allow user to take action on Access Control door from console to open unlock door, relock door, allow momentary access for door, lock down door, release lock down

5.2.7.17 Allow user to take query Access Control door from console to get last 5 activities for door, get activities for door in the last 5 minutes, get door activities for last hour, get door activities for the last day, etc.
5.2.7.18  Allow user to view badge photo ID from door activity results

5.2.7.19  Allow user to jump from one map to the next with a single click of a mouse with map links

5.2.7.20  Allow map information “layers” to be displayed/hidden on items such as:

- Sensor names
- Sensors
- Sensor range (camera – orientation, range, field of view angle)
- Security areas and zones
- Perimeter ranges
- Resource tracks

5.2.7.21  Allow user to zoom in/out on different regions of map graphic

5.2.8  Navigation - The PSIM solution shall have the following navigational display functionality:

5.2.8.1  Allow user to navigate maps in a hierarchical list or tree based security zones or logical groups

5.2.8.2  Allow user to navigate to a map or security zone through the map interface and through a graphical hierarchical tree view

5.2.8.3  Allow user to quickly navigate to an open alarm through a hierarchical tree and related map.

5.2.8.4  Allow user to navigate to search by sensor name and be directed to related graphical map

5.2.8.5  Allow user to sort hierarchical tree by name of zone or area

5.2.8.6  Visually indicate in the hierarchical tree/list if a sensor in a security zone is in an alarm state.

5.2.8.7  Visually display the number of open alarms in a security zone or area in the hierarchical tree

5.2.8.8  “Bubble up” the visual indication of the highest severity alarm to the next higher level in hierarchical tree.

5.2.9  Search and Trace Capabilities

5.2.9.1  Allow user to search and find sensor(s) names with text “wildcards”
5.2.9.2 Allow user to search and find security zones and areas names with text “wildcards”

5.2.9.3 Allow user to search and find alert ID to quickly find alert and alert details

5.2.9.4 Allow user to search and trace all user activity related to a specific badge ID or user name

5.2.9.5 Allow user to search and trace all user activity related to a specific user name

5.2.9.6 Video Display - The PSIM solution shall have the following video display functionality:

5.2.9.6.1 View live or recorded video from resizable and movable windows

5.2.9.6.2 View live or recorded video from any monitor connected to PSIM workstation

5.2.9.6.3 Display the same video controls irrespective of video system manufacturer

5.2.9.6.4 Ability to perform video controls for video systems from PSIM workstation:

- Play, fast-forward, rewind, pause, and specify time to play recorded video
- Take a video still image (snapshot) from live or recorded video
- Export video for user specified time and duration
- Move PTZ cameras (if available)

5.2.9.6.5 View Video in Video Matrix

- Display in 1x1, 2x2, 3x3 and 4x4 window formats
- Enable predefined video windows to be displayed in matrix
- Enable operator to specify video windows to be displayed in matrix
- Enable matrix settings to be saved per user
- View either live or recorded video can be displayed in the video matrix window.
- Enable video snapshot to be taken and saved from any window pane in the matrix view

5.2.9.6.6 Rotate video in “virtual” video guard tour

- Rotate through multiple video views based on predefined video camera sequence and duration.
- Enable the user to pause the rotation of video and resume the video rotation again
- Enable times between new video to be adjusted
- Enable both live video and recorded video to be played through the video guard tour.
- Enable alarms to be generated from any video pane
5.2.9.6.7 Enable user to only view and control video for which they have been assigned permissions by the administrator

5.2.9.6.8 Manually create an alarm from the live or recorded video with specified severity and description

5.2.10 Summary Dashboard

5.2.10.1 Provide alarm summary of each monitoring zone or monitoring area in graphical chart format

5.2.10.2 Display the following charts per global area, monitoring zone or monitoring area
   • Open Alert Count by Monitoring Zone/Monitoring Area
   • New vs. Viewed (Opened Alerts)
   • Open Alert Count by Alert Severity
   • Highest Severity Alert

5.2.10.3 Enable Monitoring Zone or Monitoring area default to Summary view dashboard or to a map when the zone or area is selected.

5.2.11 Sensor List View

5.2.11.1 Provide a tabular list of sensors in each monitoring area

5.2.11.2 Enable each column in the table to be sorted

5.2.11.3 Enable each column to be filtered based on criteria

5.2.11.4 Enable actions to be taken on each sensor similar to the icon on the map
   • For video cameras, choose the camera to view live video, recorded video, launch tracking capability, generate alert
   • For access control door choose the door to unlock door, relock door, allow momentary access for door, lock down door, release lock down, get last 5 activities for door, get activities for door in the last 5 minutes, get door activities for last hour, get door activities for the last day, etc.

5.2.12 Alarm Display - The PSIM solution shall have the following alarm display functionality:

5.2.12.1 Display real time, dynamic, iconic status of alarm point indications, overlaid onto a computer generated or GIS graphic map of the detection area and zone

5.2.12.2 Display textual alarm description alarm status, severity, activity, operator actions, tasks and procedures, and time/date status.
5.2.12.3 Allow users to view digital video scenes, automatically or manually, related to alarm for both live and recorded video

5.2.12.4 Allow users to handle alarms based on priority

5.2.12.5 Allow users to handle and view multiple alarms in individual windows or in a list

5.2.12.6 Allow users to view alarm notification in system tray

5.2.12.7 Allow users to view alarm notification and alarm summary in alert list window pane

5.2.12.8 Allow users to view alarm notification in the hierarchical tree view

5.2.12.9 Allow users to view alarm in a specific security zone and associated with specific sensor on the map

5.2.12.10 Allow users to view a list of alarms associated to a sensor on the map

5.2.12.11 Sort alarms list status by time/date

5.2.12.12 Sort alarm list by severity (i.e. highest severity on top)

5.2.12.13 Sort alarm list by alarm type

5.2.12.14 Sort alarm list by location

5.2.12.15 Allow users to choose which columns (details) are shown in the alarm list

5.2.12.16 Allow users to scroll through multiple queued alarms

5.2.12.17 Display associated queued video with each alarm

5.2.12.18 Filter alarms by severity, status, sensor name, alert types

5.2.12.19 Group alarms by type, location, sensor, etc.

5.2.12.20 Subgroup alarms by type, location, sensor, etc.

5.2.12.21 Have the same “look and feel” for different alarms generated or alarms generated from different systems

- All alarm details are displayed in the same places and information is consistent
- Video windows and controls are in the same place and can be displayed with the same controls
- Notes are in the same location for different alarm types
Acknowledgement of alarms can be performed in the same way for different alarms types
Contractor specific information is displayed in the same portion of the user interface

5.2.13 Alarm Handling - The PSIM solution shall have the following alarm handling functionality:

5.2.13.1 Ability to display alarm condition through visual display and audible tone

5.2.13.2 Ability to simultaneously handle multiple alarms from multiple workstations

5.2.13.3 Ability to prioritize and display multiple alarms and status conditions according to pre-defined parameters such as alarm type, location, sensor, severity, etc.

- Display the highest priority alarm and associated video in the queue as default, regardless of the arrival sequence
- Place subsequent alarm in a queue according to predefined priorities without covering up or higher priority alarm

5.2.13.4 Ability to automatically present an integrated window of the incident and access to the following incident related information and actions with a single mouse click or less

- Related queued recorded video
- Related live video from related camera
- Related video PTZ controls (if camera is PTZ)
- Related local map image with location of alarm
- Related door activity
- Related alarm notes
- Acknowledge/close alarm
- Take a visual image snapshots of live or recorded video to be printed, saved to disk or saved as a part of the alarm
- Contractor specific sensor information (i.e. video analytics alarms may generate marked up images, etc.)

5.2.13.5 Ability to automatically display related response instructions and tasks for each alarm

- Tasks in checklist format
- When tasks have been updated
- Completion progress
- Provide option to require operator to complete specific task(s) before alarm can be acknowledged or closed
5.2.13.6 Ability to acknowledge or close alarms from central console and updates to be synchronized with related alarming security subsystems

5.2.13.7 Ability to enter notes during the alarm and notes information to be shared with other users of the system

5.2.13.8 Ability to view historical alarms that have been closed or acknowledged in the system to view activity, video, etc. (for duration of video being captured in the system)

5.2.13.9 Ability to automatically stamp note entries with time/date and operator user name

5.2.13.10 Enable new alerts to automatically open alert details window when alerts are received or for alerts to remain in the alerts list until a user clicks on the alert.

5.2.13.11 Ability to generate comprehensive alarm report within 30 seconds of alarm occurrence including alarm description, time/date, severity, location, maps, door activity (if available), video image snapshots (if taken), and response instructions (if available)

5.2.13.12 Ability to print comprehensive alarm report within 30 seconds of alarm occurrence including alarm description, time/date, severity, location, maps, door activity (if available), video image snapshots (if taken), and response instructions (if available)

5.2.13.13 Ability to email comprehensive alarm report within 30 seconds of alarm occurrence including alarm description, time/date, severity, location, maps, door activity (if available), video image snapshots (if taken), and response instructions (if available)

5.2.13.14 Ability to send comprehensive alarm report to wireless mobile device within 30 seconds of alarm occurrence including alarm description, time/date, severity, location, maps, door activity (if available), video image snapshots (if taken), and response instructions (if available)

5.2.13.15 Ability for operator to quickly export associated video upon alarm occurrence.

5.2.13.16 Ability to automatically and manually escalate alarms

- Automatically escalate alarms if alarm is not addressed within a predefined time frame. Enable alarm to be escalated to new group or user and actions to be taken.
- Operator can escalate and redirect alarm directly from the PSIM workstation while working on the alarm
- Alarms can be redirected or escalated to pre-configured user group or user.

5.2.13.17 Enable operator to generate a new alarm from map

- Automatically capture the alarm time and date
- Automatically capture the location of the alarm on the map
• Enable operator to specify severity, alarm type, and alarm description
• Enable appropriate response tasks to be associated with the alarms
• Enable other operators to see and handle alarm similar to other alarm types

5.2.13.18 Enable operator to generate a new video alarm while watching live or recorded video

• Automatically capture the alarm time and date
• Automatically capture the location of the alarm
• Automatically capture video image snapshot and link to related video
• Enable operator to specify severity and alarm description
• Enable other operators to see and handle alarm similar to other alarm types
• Enable appropriate response tasks to be associated with the alarms

5.2.13.19 Provide multiple alarm details display types based on operator experience

• Simple view which defaults to alarm details and response tasks where operator chooses icons to view additional information such as video, notes, etc
• All-in-one detailed views to provide operator with all relevant information at one time

5.2.13.20 Enable administrator to configure pop-up message if response tasks have not been completed for alarms before they are acknowledged or closed

5.2.13.21 Enable different sound types and sound files to be associated with different alarm types

5.2.13.22 Enable electronic voice playback of alarm and alarm description

5.2.14 Historical Alarm Handling - The PSIM solution shall have the following historical alarm handling functionality:

5.2.14.1 Ability to view historical alarms details even after the alarm has been acknowledged or closed.

5.2.14.2 Ability to sort alarms according to date/time, severity, type, and sensor ID or location.

5.2.14.3 Ability to group alarms according to date/time, severity, type, and sensor ID or location.

5.2.14.4 Ability to view associated alarm description, time/date, severity, location, maps, door activity (if available), video image snapshots (if taken), and response instructions (if available) and related queued video from time of alarm.

5.2.15 Auditing - The PSIM solution shall have the following auditing capabilities:

5.2.15.1 Ability to store and log all activities related to alarm
- When alarm is created in PSIM system
- When alarm is viewed by operator
- When alarm is acknowledged, closed, or deleted
- Actions taken on related sensor resources
- Video snapshot images taken by operator
- Notes entered by operator for alarm
- Reports generated

5.2.15.2 Ability to display all activities while alarm is open

5.2.15.3 Ability to display all activities after alarm is acknowledged or closed

5.2.15.4 Ability to display activities on monitor and print report

5.2.15.5 Ability to export alarm report in various formats including pdf, jpeg, html, txt, and mht formats

5.2.16 Alarm Reporting - The PSIM solution shall have the following alarm reporting capabilities:

5.2.16.1 Ability to generate a full incident report within 30 seconds of the alarm being generated.

5.2.16.2 Ability to display report on monitor and print report

5.2.16.3 Ability to select information to be included in report at time of report generation.

- Details of alarm including severity, time/date, description and location
- Map of surrounding area associated with alarm
- Associated door activity and badge holder information if access control alarm
- Captured video image snapshots
- Response instructions
- Alarm activities (audit trail)

5.2.16.4 Ability to export alarm report in various formats including pdf, jpeg, html, txt, and mht formats

5.2.16.5 Ability to generate an alarm incident package including the full incident report and exported video from the incident in a specific folder location.

5.2.17 Trend Reporting - The PSIM solution shall have the following trend reporting capabilities:

5.2.17.1 The PSIM system shall allow generation of security trend reports to provide insight for proactive in resource planning and pinpoint specific problem areas and sensors.
• Alarm Count Daily Report
• Alarm Count Hourly Report
• Alarm Detail Report
• Alarm Response Time by Alarm Type Report
• Operator Alarm Count Report
• Operator Alarm Response Time Report
• Operator End of Shift Report
• Top X Alarm Response Time Report
• Top X Alarms by Alarm Type Report
• Top X Alarms by Area Report
• Top X Alarms by Sensor Report
• Top X False Alarms by Sensor Report
• Top X Simulated Alarms By Sensor Report

5.2.17.2 Ability to display report on monitor and print report

5.2.17.3 Allow reports to be generated and filtered based on different criteria including

• Time
• Date
• Area/Location(s)
• Sensor(s)
• Alarm type and source
• Alarm severity
• Simulated alarms

5.2.17.4 Create predefined report templates based on different criteria

5.2.17.5 Ability to customize the look and feel of the report

• Chart Type
• Enable/Disable Chart
• X-Axis and Y-Axis labels
• Color Scheme

5.2.17.6 Ability to save report templates to be reused at a later time

5.2.17.7 Ability to export report in various formats including pdf, jpeg, html, txt, and mht formats

5.2.18 Video Tracking - The PSIM solution shall have the following video tracking capabilities:
5.2.18.1 When operator is viewing video from an existing camera, automatically display video from adjacent cameras

- Select the direction of movement to show adjacent video
- Follow a suspect/object moving from one camera view to the next camera view by selecting one of the next camera views
- Simultaneously watch current field of view while also viewing video from adjacent cameras
- Should not require operator to memorize or enter in camera names/IDs or times.
- Support live or recorded video
- Fast-forward, rewind, pause or stop recorded video
- Ability to track suspect/object forwards and backwards (if supported by VMS)

5.2.18.2 Ability to automatically build a track report when the operator moves from one camera to the next camera

- Record camera ID and name
- Record time and date
- Record and update video still image

5.2.18.3 Ability to replay the path of the object suspect including

- Camera ID and name
- Time and date
- Video still image
- Animated map with associated camera location on map
- Breadcrumb trail showing the path of the object/suspect from camera to camera
- Recorded video for each video track

5.2.18.4 Ability to generate ‘track’ report including camera IDs, video snapshots, times/dates, and map locations

5.2.18.5 Ability to export report in various formats including pdf, jpeg, html, txt, and mht formats

5.2.19 Device Tracking - The PSIM solution shall have the following device tracking capabilities:

5.2.19.1 Track latitude and longitude or geospatial location of devices or objects (e.g. GPS enabled cellular phones, RFID devices, etc.)

5.2.19.2 Allow devices to be associated with resources for resource tracking

5.2.19.3 Enable multiple devices to be simultaneously tracked
5.2.19.4 Enable device locations to be displayed in the PSIM geospatial map
5.2.19.5 Enable details of devices to be called up from the map
5.2.19.6 Enable tracked objects to be displayed/hidden
5.2.19.7 Enable multiple objects to be tracked, but only show tracks of object when the object enters an alarm area/zone.
5.2.19.8 When object enters alarm area/zone, show alarm details and geo-referenced breadcrumb tracks leading up to the alarm
5.2.19.9 When object enters alarm area allow real-time updates of geo-referenced breadcrumb trail.

5.2.20 Resource Tracking - The PSIM solution shall have the following resource tracking capabilities:
5.2.20.1 Track latitude and longitude or geospatial location of resources (e.g. people, vehicles, water vessels, etc.) if associated with location based device
5.2.20.2 Enable multiple resources to be simultaneously tracked
5.2.20.3 Enable resource locations to be displayed in the PSIM geospatial map if associated with location based device
5.2.20.4 Enable details of resources to be called up from the map
5.2.20.5 Enable tracked resources to be displayed/hidden
5.2.20.6 Enable search and find tracked objects by name.
5.2.20.7 Automatically display the location of the resource on the map with single mouse click

5.2.21 Mobile Device Support
5.2.21.1 The PSIM solution shall have the following wireless/cellular mobile device capabilities:
5.2.21.2 Provide mobile operator in-context alarm information including all alarm details on mobile device
5.2.21.3 Enable mobile operator the ability to view all alarms assigned to him/her on mobile device.
5.2.21.4  Enable mobile operator to enter notes on the mobile device to be updated with central PSIM system

5.2.21.5  Enable the mobile operator to view and update alarm on mobile device when wireless connectivity is lost and for information to be synchronized when wireless connectivity is reestablished

5.2.21.6  Ability for mobile operator to receive escalated alarm on mobile device.

5.2.21.7  Ability for mobile operator to create a new alarm in to the PSIM solution based on a photo taken by mobile device.

5.2.21.8  Enable mobile operator to pull up cardholder information/credentials by entering in name or employee badge ID on mobile device.

5.2.21.9  Enable mobile device to communicate securely with PSIM system

5.2.22  Data Integration - The PSIM solution shall have the following data integration capabilities:

5.2.22.1  WMATA seeks interEnable the bi-directional management of data sharing among security subsystems such as:

- CCTV management and control systems
  1) Bus CCTV System
  2) Rail Vehicle System
  3) FirstView (existing CCTV System)
- Digital video recording systems
- Physical access control systems
  1) Edwards EST3
  2) Pro Watch
- Intrusion Detection Systems
- Badge management systems
- Video analytics systems
  1) BRS Systems
  2) TBD
- Response Systems
- Chemical/biological detection systems
  1) CBEMIS by Smiths Detection
- Radioactivity detection systems
- Phone Systems
  1) AVAYA
- Intercom systems
  1) Commend / Raimax
- Motion detection systems
- Location-based device systems (RFID, GPS devices, etc)
1) Bus AVL – Orbital
2) Radio - Motorola
- Computer Aided Dispatch Systems
- Notification Systems
  1) Passenger Information Displays - COM NET
- Radar Systems
- Panic Buttons
- AED Devices
- IT Systems
- Building Management Systems
- Automated Energy Management System (AEMS) – QEI Corporation
- Advanced Information system (AIM) - ARINC
- Automatic Fare Collection – Cubic
- WMATA Network Operation Center

5.2.22.2 Provide an open web services-based Application Programming Interface (API) and Software Development Kit (SDK) to enable other systems to be easily integrated with the PSIM solution. The PSIM API and SDK will:

- Enable a Contractor subsystem to raise new alarms in to the PSIM solution
- Enable a Contractor subsystem to deliver alarm details in to the PSIM solution
- Enable the PSIM solution to browse a list of sensors (doors, alarm points, etc.) and add the sensors to the appropriate maps, sensor groups, monitoring areas, etc.
- Enable the PSIM solution and the Contractor subsystem to synchronize alarm status updates in real time
- Provide the PSIM system to take actions on the Contractor system such as retrieving ACS door information, control ACS doors, move cameras, etc.
- Enable object or resource geo-coordinate locations to be associated with the alarm or resource and tracked on the PSIM map
- Enable a Contractor system to retrieve escalated, correlated PSIM alarm detail information
- Enable the PSIM console to be launched through a programmatic command
- Enable a particular video window in the PSIM console to be displayed through a programmatic command
- Launch a particular alarm window and alarm details in the PSIM console to be displayed through a programmatic command.

5.2.23 Other Users - The PSIM solution shall have the following user capabilities:

5.2.23.1 Enable multiple users to access system simultaneously

5.2.23.2 Enable multiple users to handle the same alarm at one time

5.2.23.3 Enable single or multiple users to view and manage alarms in defined areas
5.2.23.4 Enable changes (acknowledge/close/escalate/add comment) by one user to be seen by other users

5.2.24 Permissions and Groups - The PSIM solution shall have the following user and group permission capabilities:

5.2.24.1 Ability to utilize Windows security and Microsoft SQL Server security (Windows Authentication or SQL Server Authentication)

5.2.24.2 Ability to provide multiple security groups and roles:

- Operators – to access operational functionality in the user interface.
- Administrators – to access both the operational functionality and administrative and system related configuration functionality in the user interface.
- Power Users – to access operational functionality and some limited administrative functionality
- Video Viewer – to access video console only, and granted scope of hierarchy only
- Mobile Operator – to access alarms via PDA or SmartPhone

5.2.24.3 Ability to create new users with login and passwords and assign users to the appropriate security groups

5.2.24.4 Ability to search and auto-filter user lists to find specific users

5.2.24.5 Ability to assign security groups/roles to

- View individual security zones and maps
- View alarms in specific security zones and locations
- View and control sensors in specific security zones and locations
- Configure system including maps, sensors, policies, permissions, users

5.2.24.6 Ability to grant or revoke the permission of the following functionalities to each security group/role

- Access Administration Console
- Access Operation Console
- Access Video Console
- Access Mobile PDA or SmartPhone
- Access Business Logic Console
- Access Alert Manager
- Access Video Tracking / Pursuit
- Access Report Wizard
- Acknowledge Alert
- Close Alert
- Delete Alert
5.2.25 System Administration - The PSIM solution shall have the following system administration capabilities:

5.2.25.1 Allow systems administration functionality to be configured through a graphical user interface

5.2.25.2 Ability to configure alarm policies and properties through user interface

5.2.25.3 Ability to configure maps through user interface

5.2.25.4 Ability to configure sensor locations through user interface

5.2.25.5 Ability to configure sensor properties through user interface

5.2.25.6 Ability to establish user access and permission levels through user interface

5.2.25.7 Ability to create new users, logins and passwords specific for each user through user interface

5.2.25.8 Ability to configure security zones through user interface

5.2.25.9 Ability to easily add/remove/edit sensors as a part of a security zone through user interface

5.2.25.10 Ability to configure all alarm priorities, text and graphics information, locate display alarm points, video displays/video recording and playback characteristics, password management, report generation and configuration and other related information
5.2.25.11 Ability to archive, retrieve database via database tools

5.2.26 Configuration Wizard and Setup - The PSIM solution to be able to be configured through a GUI based configuration wizard.

5.2.26.1 Ability to have entire PSIM solution configured and functional through the configuration wizard

5.2.26.2 Ability to have a checklist of items that need to be completed for each step

5.2.26.3 Ability to have a progress meter to view progress of installation

5.2.26.4 Ability to stop and resume the configuration at a later time

5.2.26.5 Ability to view configuration tips and tricks

5.2.26.6 Ability to link to the specific PSIM configuration screen for setup if required

5.2.27 Map Administration - The PSIM solution shall have the following map administration capabilities:

5.2.27.1 Ability to import map images from AutoCAD, BMP, JPEG and other standard image files

5.2.27.2 Ability to geospatially reference maps and sensors on maps to real-world coordinates

5.2.27.3 Ability to logically group maps and organize hierarchically

5.2.27.4 Ability to add sensors to map, such as cameras and ACS doors, etc,

5.2.27.5 Ability to display camera properties on map such as camera orientation, camera field of view angle, and camera range.

5.2.27.6 Ability to represent different sensors types with different icons

5.2.27.7 Ability to create security zones on map represented by polygon shapes to allow the operator to visually distinguish the different regions

5.2.27.8 Ability to apply permissions to maps such that different groups and authority levels can only see the maps for which they have privileges to view

5.2.27.9 Ability to display only security maps, sensors and alerts associated with security zone
5.2.27.10 Ability to create links on the map to move back to the previous map views, move to another map, adjacent map (left, right, up, down, custom link), or go to the top level map with a single click of a button

5.2.27.11 Ability to search and auto-filter security zones and areas to find specific zones/areas in large environments

5.2.28 Sensor Administration - The PSIM solution shall have the following sensor administration capabilities:

5.2.28.1 Ability to sustain frequent additions/removal/changes to sensors and sensor properties

5.2.28.2 Ability to easily accommodate new sensor types such as access control alarms, intrusion alarms, video systems, etc. which may be added at a later date

5.2.28.3 Ability to browse sensor subsystem for related sensor name or ID to add the sensor to the PSIM system

5.2.28.4 Ability to update maps and graphical elements through graphical user interface

5.2.28.5 Ability to define properties and details of sensors

- Name
- Description
- Location
- Position
- Camera Specific - Field of view angle, distance, direction, type
- Mapping to subsystem

5.2.28.6 Ability to create sensor groups such that related sensors such as access control sensor and camera sensor can be in a sensor group to display appropriate video when alarm occurs or to correlate multiple alarms together in the group

5.2.28.7 Allow more than one of the same type of sensor (camera, access control, intrusion alarm, etc.) to be added to the same group such that multiple cameras can be displayed per alarm or multiple alarms from similar devices can be correlated.

5.2.28.8 Ability to search and auto-filter sensor lists to find specific sensor(s) in large sensor lists

5.2.28.9 Ability to bulk import sensors and sensor configuration from xml, excel, or CSV file

5.2.28.10 Ability to bulk monitoring area names with members from xml, excel, or CSV file

5.2.28.11 Ability to bulk export sensor configurations for any sensor types
5.2.29 Alarm Policies and Business Logic Administration - The PSIM solution shall have the following ability to handle the workflow alarms through Visio-like graphical user interface:

5.2.29.1 Ability to create an alarm policy to raise alarm in the PSIM system by defining conditions through configurable GUI-based business logic designer

- Ability to match keywords or text from the alarming subsystem’s event description to raise an alarm using criteria including exact match, exact NOT match, contains match, wildcard match and regularly expression match (such as forced door alarm, denied access, door open too long, etc.)
- Ability to optionally match alarming subsystem’s event status, event severity, and sensor type
- Ability to customize the alarm description the PSIM system to use the exact description from the Event Source, a predefined Alert Description, or any customer description.
- Ability to customize the alarm severity in the PSIM system based on the type of alarm subsystem event

5.2.29.2 Ability to apply the alarm policy across all alarm subsystems or only selected alarm subsystems with a single alarm policy

5.2.29.3 Ability to apply any alarm policy to one or more monitoring area(s) or zone(s) without having to reapplying the policy multiple times.

5.2.29.4 Ability to apply any alarm policy to one or more sensors without having to reapply the policy multiple times.

5.2.29.5 Ability to assign specific actions for each alarm

- Email
- Command line action
- Correlation and fusion of additional incident related information
- Alarm escalation

5.2.29.6 Ability to automatically correlate related data and information to be displayed in real-time for each alarm and related rule

- Correlate data or information from any security subsystem such as related live video, related recorded video, door activity, door commands, operator response instructions, map location, badge images, etc.
- Automatically display information in real-time when an alarm is generated.
- Display all correlated information together in attached windows when an alarm is generated.
- Automatically display related response instructions and tasks for each alarm and related rule

5.2.29.7 Ability to assign and apply business logic policy to specific sensors and or security zones

5.2.29.8 Ability to create business logic policy to support multi-decision, multi-action workflow for any alarm through a drag and drop GUI-based designer

5.2.29.9 Enable the following activities to be included in the business logic policy:

- Enable business logic activity to display live video
- Enable business logic activity to display recorded video based on a relative time offset from the alarm time
- Enable business logic activity to display door activity based on configurable amount of time and/or events
- Enable business logic decisions based on time of day
- Enable business logic decisions based on severity
- Enable business logic decisions based on location
- Enable business logic decisions based on regular expression text matches
- Enable business logic decisions based on security threat level
- Enable business logic activity to escalate alarm after predefined time
- Enable business logic activity to generate a new alarm
- Enable business logic activity to make a call
- Enable business logic activity to send email
- Enable business logic activity to take action on sensor subsystem (ACS, camera commands, etc.)
- Enable a custom Microsoft Powershell activity to be created and included in the business logic flow
- Enable business logic to correlate multiple alarms together and take follow on action such as auto-acknowledging/closing prior alarms, creating new alarms, etc.
- Enable business logic to activity to generate a report
- Enable business logic to escalate an alert to notification service
- Enable business logic to execute a web services call
- Enable business logic to execute ODBC database call
- Enable business logic to invoke an external method call
- Enable business logic to generate a report on an incident in multiple report formats and with different customizable information
- Enable business logic to automatically send report to a predefined email
- Enable business logic to take a HTTP SEND or GET action on predefined URL with or without authentication
- Enable business logic to take a HTTPS SEND or GET action on predefined URL with or without authentication
- Enable business logic to determine whether the current location of an alarm is within a specific geographic boundary/area
- Simulate an alert and follow the step-by-step execution of the business logic prior to application of business logic in production environment
- Enable business logic to call another child business logic policy as a part of the main business logic activity
- Enable business logic activity to aggregate RSS or ATOM feeds, filter the feeds and create corresponding alert in the PSIM system
- Enable business logic to change the alarm context to that of another alarm
- Enable business logic to lock a specified door, relative door defined in an area or sensor group, or multiple doors defined in an area or group
- Enable business logic to open a specified door, relative door defined in an area or sensor group, or multiple doors defined in an area or group
- Enable business logic to open momentarily a specified door, relative door defined in an area or sensor group, or multiple doors defined in an area or group

5.2.29.10 Enable business logic policies to be saved, loaded and reused as necessary as business logic templates

5.2.29.11 Ability for simulate alarms through business logic designer

5.2.29.12 Enable multiple business logic policies to be deployed and to be processing at any one time

5.2.29.13 Ability to schedule business logic policies to run at specified times of the day, days of the week, monthly, or yearly within a specified or endless time range.

5.2.29.14 Ability to collapse multiple duplicate alarms to reduce alarm clutter

- Ability for administrator to apply collapsing policies through PSIM administrative user interface
- Ability to assign different collapsing policies to be assigned to different security zones and locations
- Ability for alarms to be collapsed based on time duration, matches to sensor name, severity, and alert description regular expression
- Allow user to view number of collapsed alerts through the operational user interface
- Allow user to view the collapsed alerts and collapsed alerts details through the operational interface if required

5.2.29.15 Ability to set up automated escalation policies for different areas and locations

- Escalate alarm if no activity is taken on alarm within predefined time period
- Escalate alarm to predefined groups or users
- Take actions on escalated alarms
- Re-escalate alarm if no activity is taken on escalated alarm with new groups or users and actions.
5.2.30 Automated Sensor Updates

5.2.30.1 Ability to automatically add newly found subsystem sensors as a new sensor PSIM system

5.2.30.2 Ability to automatically add the newly found sensor to a corresponding monitoring area

5.2.30.3 Ability to automatically apply a business logic policy to the newly found sensor

5.2.31 Permission Administration - The PSIM solution shall have the following permission administration capabilities:

5.2.31.1 Ability to assign the following permissions to maps and security areas

- Operator’s permission to perform all functions within that client software. These users cannot access the Administrator Console.
- Administrator permission to access both the Operator Console and the Administration Console. This allows them to perform the same actions as Operators, as well as create, configure, modify and view the entire PSIM system.

5.2.32 Communications with Security Subsystems - The PSIM solution shall have the following communication capabilities with security subsystems:

5.2.32.1 Ability to view alarms and events in PSIM system from subsystems such as access control, video analytics, VMS, intrusion systems, etc.

5.2.32.2 Ability to send alarm status updates (acknowledgements, closing, deletion, etc.) from PSIM systems to each underlying subsystem

5.2.32.3 Ability to send action commands to underlying subsystems to take action such as move PTZ cameras, unlock/lock ACS doors, etc.

5.2.32.4 Ability to receive other alarms through an open web services interface.

5.2.32.5 Support multiple NVR/DVR Contractors/models simultaneously

5.2.32.6 Support multiple Physical Access Control Systems simultaneously

5.2.32.7 Support multiple Video analytics Systems simultaneously

5.2.32.8 Support multiple Intercom Systems simultaneously

5.2.32.9 Support multiple other subsystems simultaneously
5.2.32.10 Integrate with News Feed via RSS

5.2.32.11 Integrate SNMP traps in to PSIM solution

5.2.32.12 Integrate WMI alerts in to PSIM

5.2.32.13 Integrate Syslog alerts in to PSIM

5.2.33 High Availability Capabilities - The PSIM solution shall have the following high availability capabilities:

5.2.33.1 Ability for redundancy and data Integrity

- Database redundancy
- Web services redundancy
- Server components redundancy
- Operator and Administrator consoles

5.2.33.2 Ability for fault tolerance

- Support redundant server configuration with hot swappable power supplies, cooling fans, PCI slots, and hard drives in minimum RAID-5 configuration

5.2.33.3 Ability for system failover

- Ability for multiple operators including those from remote locations to simultaneously log in to the system and have full control of monitoring and access of data for detection, assessment, notification, entry control, communication
- Ability for operator to reconnect to a redundant database in case of the main database system failure. This feature requires specific underlining hardware, OS and database.
- Ability to view maps from secondary site
- Ability to view alarms from secondary site

5.2.34 Security Functionality - The PSIM solution shall have the following security capabilities:

5.2.34.1 Ability to secure system through password and privilege protection provided by the operating system(s) using Windows authentication and by Microsoft SQL Server using SQL Server authentication.

5.2.34.2 Ability to communicate among major components utilizing SOAP (Simple Object Access Protocol). SOAP is a protocol for exchanging XML-based messages over a computer network, and the communication can be configured as HTTP or HTTPS for a more secure environment.
5.2.34.3 Ability to communicate over Secure Sockets Layer (SSL)

5.2.35 System Operations - The PSIM solution shall have the following system operations capabilities:

5.2.35.1 Ability to support unattended Operation

- PSIM server services run even if a user is not logged in
- PSIM server to return to normal activity after reboot without administrator intervention

5.2.35.2 Ability for administrator without database administration skills to configure and set up system

5.2.35.3 Ability for system to be easy to use and administer

5.2.36 Performance

5.2.36.1 Ability to support over 20,000 configured sensors in the PSIM console

5.2.36.2 Ability to support over 10,000 open alerts in the console

5.2.36.3 Ability to support over 100 PSIM operations consoles from a single PSIM server

5.2.36.4 Ability to support alert bursts of over 500 alerts per second

5.2.36.5 Ability for business logic policies to be deployed in less than 10 seconds for 20,000 sensors

5.2.37 Installation

5.2.37.1 Ability for all components of PSIM solution to be installed through self-extracting installation files

5.2.37.2 Ability for new subsystem integrations to be installed without having to reinstall the base PSIM solution

5.2.37.3 All installation files should be self-guided GUI-based wizards allowing installation parameters to be entered during the installation

5.2.37.4 PSIM system shall have a GUI-based integration manager that allows

- One or more integration with subsystem to be configured
- Multiple instances of subsystem to be configured
- Parameters for integrated subsystem to be specified
- Connectivity and calls to subsystems to be automatically checked
• Integration with subsystem to be removed

5.2.37.5 PSIM system shall have a GUI-based services configuration wizard that allows each of the PSIM services and components to be configured.

5.2.37.6 Ability for PSIM database, services and web servers to all be installed on a separate servers if necessary

5.2.37.7 Ability for PSIM system to be upgraded to the PSIM version while maintaining all previously configured components - the maps, policies, sensors, and response workflow.

5.2.38 Documentation and Help - The PSIM solution shall have the following documentation and help files

5.2.38.1 PSIM installation guide

5.2.38.2 PSIM administrator guide

5.2.38.3 PSIM user/operator guide

5.2.38.4 Subsystem integration installation guide

5.2.38.5 Online context sensitive help

5.2.39 HARDWARE REQUIREMENTS AND INTERFACES - The PSIM software shall run on industry-standard computer platforms and software, and support video cameras which comply with industry standards.

5.2.39.1 Server Operating System

5.2.39.1.1 The operating system requirements for the PSIM server operating system shall be identified in the technical proposal.

5.2.39.2 Client Operating System

5.2.39.2.1 The operating system requirements for the PSIM client operating system shall be identified in the technical proposal.

5.2.39.3 Server Relational Database

5.2.39.3.1 The relational database requirements for the PSIM server operating system shall be identified in the technical proposal.

5.2.39.4 Hardware
5.2.39.4.1 The hardware requirements for the PSIM server operating system shall be identified in the technical proposal.

5.2.39.5 System Vulnerability Checks

5.2.39.5.1 The PSIM system shall be tested by security compliance software and vulnerable assessment tools, such as tools from Symantec, McAfee and Microsoft.

5.2.39.6 Network Standards

5.2.39.6.1 The PSIM system shall be compatible with IEEE TCP/IP and 802.3 Ethernet series standards. Network bandwidth to be determined by others based on the number and types of video cameras, video frame sizes and frame rates, video recording requirements, number of simultaneous users, and other factors.

6. SECTION 508 COMPLIANCE FOR IT SOLUTIONS

6.1 The Contractor shall comply with Section 508 of the Rehabilitation Act Amendments of 1998 to ensure IT accessibility to disabled persons, unless exempted. Only in situations where an approved exception to Section 508, provided by the Chief Information Officer (CIO) of the requiring agency/organization, may requirements be issued that exempts the Contractor from complying with Section 508 requirements contained in the contract. As applicable, the following specifications are incorporated:

- § 1194.21 – Software Applications and Operating Systems
- § 1194.22 – Web Based Intranet and Internet Information and Applications
- § 1194.23 – Telecommunication Products
- § 1194.24 – Video and Multimedia Products
- § 1194.25 – Self Contained, Closed Products
- § 1194.26 – Desktop and Portable Computers
- § 1194.31 – Functional Performance Criteria
- § 1194.41 – Information, Documentation and Support

7. PAYMENT FOR UNAUTHORIZED WORK

No payments shall be made for any unauthorized supplies and/or services or for any unauthorized changes to the work specified herein. This includes any services performed by the Contractor of their own volition or at the request of an individual other than a duly appointed Contracting Officer or their designated representative.

8. CONFIDENTIALITY

The project and all material provided to the Contractor by the Authority and results, conclusions, and recommendations obtained thereof shall be considered confidential in nature and treated with the same level of care that the Contractor treats its own
confidential business information. The information shall not be disclosed, copied, modified, used (except in completion of this project) or otherwise disseminated to any other person or entity at any time to include, but not limited to inclusion in any database external to the Authority without the Authority’s expressed consent.

9. QUALITY CONTROL

The Contractor shall be responsible for quality control while performing under this contract and adhere to the requirements of the contract as specified. All documentation of support and related activities shall provide traceability to enable Authority review and verification. The Contractor shall provide interim reviews of the work accomplished to permit determination of the quality of the effort performed and/or receive guidance from the COR. If deficiencies are found, the COR will ask the Contractor to provide timely, corrective action.

10. QUALITY ASSURANCE

The Authority will monitor the Contractor's performance using contract deliverables. The Contractor shall report progress on this contract in the Monthly Status Report (MSR) using the description of contents for the MSR. The IPR process shows and discusses performance, progress, problems, issues and concerns on the contract in an open forum. The contract manager/program manager is required to schedule an IPR each month of contract performance.

11. SECURITY REQUIREMENTS

11.1 All Contractor personnel in performance of this contract shall obtain a WMATA Contractor badge. Badges are available at the Jackson Graham Building ID office M-F between the hours of 8:30 AM and 4:00 PM.

11.2 MTPD will provide escorts to all personnel working in the security sensitive portions of the facility.

11.3 The Contractor, with assistance from WMATA’s IT department, shall ensure all security patches and WMATA security software is loaded on all computer equipment.

12. TRAVEL

All travel shall have prior written approval from the COR. Any travel performed without prior COR approval is unauthorized. When travel may be required, the Authority will include funds in the travel line item. During the course of performance, the CO or COR will identify any travel requirements and notify the Contractor in writing.

13. EQUIPMENT TRANSPORT AND PURCHASE
Property and equipment transportation costs necessary to accomplish the tasks while traveling shall normally be furnished by the Authority, however, as required and authorized by the COR, such transportation and equipment purchase costs may be paid by the Contractor and billed to the Authority. At the end of the contract, any equipment purchased on contract remains the property of the Authority.

14. NON-DISCLOSURE AGREEMENTS

Due to the interrelationship of our Contractor workforce, all Contractor employees assigned to a contract shall sign a non-disclosure agreement, as applicable. The Contractor is bound by all NDAs signed by its employees. In the event a Contractor employee violates any of the terms of the NDA, the Contractor will be considered in breach of contract. This could result in a termination for default.

15. NON-PERSONAL SERVICE STATEMENT

Contractor employees performing services under this order will be controlled, directed and supervised at all times by management personnel of the Contractor. Contractor management will ensure that employees properly comply with the performance work standards outlined in the performance work statement. Contractor employees will perform their duties independent of, and without supervision of, any Authority official. The tasks, duties, and responsibilities set forth in the contract may not be interpreted or implemented in any manner that results in any Contractor employee creating or modifying policy, obligating appropriated funds, overseeing the work Authority employees, providing direct personal services to any Authority employee. Authority will control access to the facility and will perform the inspection and acceptance of the completed work.

16. SPECIAL INSTRUCTIONS / CONSIDERATIONS

16.1 The Contractor agrees to enter into a written agreement with any firm whose proprietary data is used in connection with the performance of the contract, to protect all proprietary information from unauthorized disclosure or use for as long as it remains proprietary, to furnish the contracting officer with executed copies of all such agreement, and to refrain from using any proprietary information in supplying to the Authority goods or services, or for any purpose other than that for which it was intended.

16.2 The Contractor agrees that any information furnished by the Authority to the Contractor not generally available to other Contractors shall be used only for performance under this contract, and all copies of such information shall be returned to the Authority upon completion of the effort. Any information furnished by the Authority containing trade secrets or commercial or financial data of other Contractors shall be treated as proprietary data. Additionally, the Contractor shall not disclose outside the Authority any information generated in the performance of this contract.

17. PERSONNEL
17.1 **PROGRAM MANAGER.**

17.1.1 The Contractor shall provide an overall program manager who shall be responsible for the performance of the work. The name and telephone number of the program manager and an alternate shall be provided to the Contracting Officer and Contracting Officer Representative (COR) in writing prior to the contract start date. The alternate shall act in the capacity of the program manager in the event the program manager is absent. Any change in program manager and alternate shall be provided, in writing, to the Contracting Officer and COR upon replacement of the manager and/or alternate.

17.1.2 The program manager shall have full authority to act for the Contractor on all matters pertaining to the operation of this contract. The program manager shall be available to meet, as necessary, with the COR and/or Contracting Officer to discuss contract performance and/or problem areas.

18. **NON-COMPLIANCE**

18.1 Memorandum For Record (MFR) – If the COTR/QAP finds that the Contractor has deviated from established standard but the deviation has little bearing on the service, the COTR/QAP will document the finding in a MFR. However, if the COTR/QAP repeatedly identifies the same minor finding, it may be an indication that a major finding is occurring because the Contractor has not taken proper steps to prevent recurrence.

18.2 Contract Discrepancy Report (CDR) - When the Contractor fails to meet contract performance requirements, the COTR, QAP, CA, or CO may prepare a CDR. This report is forwarded to the CO for review, and subsequently processed through the Contractor for action/explanation before being returned to the CO. Upon receipt, the CO will review the response and determine whether to accept the Contractor's position, determine corrective action (reduction in the monthly payment due to unacceptable performance, cure notice, show cause, etc.), or take other appropriate contractual action. The Authority reserves the right to make a partial payment for services performed prior to receipt and evaluation of the Contractor's response to a CDR.