

Newport-Mesa
Unified School District

Motorola-Avigilon RFI Response
Install & Integration of a District Wide Integrated Security
System

April 5, 2021

Submitted By:

Ryan Ta

Business Development Manager- Education

(619) 519-6618

ryan.ta@motorolasolutions.com

Avigilon

1717 McKinney Ave, Suite 1590

Dallas, TX 75202

+1 (888) 281-5182

April 5, 2021

Jonathan Geiszler
Director of Purchasing & Warehouse
2985 Bear St. Bldg. A
Costa Mesa, CA, 92626

RE: RFI #104-21 Install and IMplementation of a Districtwide Integrated Security System

Dear Mr. Geiszler

Motorola Solutions, Inc- Avigilon is proposing to enhance campus safety and prepare Newport Mesa Unified to respond to emergencies with our Safe Schools solution. Tailored to Newport Mesa Unified's priorities, Safe Schools includes products to detect threats, analyze available information, communicate with staff, and coordinate emergency responses.

Motorola Solutions' proposal is conditional upon Newport Mesa Unified's acceptance of the terms and conditions contained in the Communications System and Services Agreement (CSSA) included in this proposal, or a negotiated version thereof. Pricing will remain valid for 90 days from the date of this proposal.

Any questions Newport Mesa Unified has regarding this proposal can be directed to Ryan Ta, Business Development Manager-Education, at (619) 519-6618 or ryan.ta@motorolasolutions.com

Our goal is to provide Newport Mesa Unified with the best products and services available to support school safety. We thank you for the opportunity to present our proposed solution. We hope to strengthen our relationship by implementing this project.

Sincerely,



Ryan Ta
Business Development Manager- Education

MOTOROLA SOLUTIONS, INC.

Table Of Contents

Executive Summary	4
Motorola-Avigilon Solution Narrative	5
Detect	6
Video Security	6
Access Control Manager	8
Radio Connectivity with Orchestrate	9
Orchestrate	9
Analyze	10
Unusual Motion Detection	10
Focus of Attention	11
Appearance Search	11
Identity Search	12
Self-Learning Video Analytics	13
Elevated Temperature Detection	14
Communicate	14
Respond	15
Sample Network Topology for ACC	16
Sample Topology for ACM	16
Glossary	18
RFI Questionnaire	21
Additional RFI Response Requirements	30
Similar and Completed Solution Deployments in K-12 Schools with 20,000 ADA or higher	30
Budgetary Costs for Purchasing	32
Supplemental Data	34

Executive Summary

High-resolution cameras with edge-based intelligence, A.I.-powered video analytics, facility access control, and improved radio technology can be powerful tools for keeping schools safe. But if all of those tools are designed to operate alone, they will only create a bigger influx of data – in need of a coordinated solution to make it practically useful.

With the industry's largest R&D investment and an aggressive strategy of acquisitions and partnerships, Motorola Solutions has developed an integrated portfolio of applications, devices, and services to provide vital operational intelligence for campus protection – channeling a flood of emergency data into a steady stream of safety information.

These tools cover a wider area with better technology - enabling you to detect threats accurately, analyze data quickly, communicate information easily, and respond to incidents decisively.

In February of 2018, Motorola continued to build its portfolio by acquiring Avigilon, a leader in Video Security and Access Control. Avigilon designs, develops, and manufactures solutions in video analytics, cloud, security cameras, video management software, video management hardware, and access control solutions. Avigilon is an industry leader and, together with Motorola Solutions, provides integrated solutions for video security, access control, and critical communications.



Motorola-Avigilon Solution Narrative

Motorola-Avigilon understands Newport-Mesa Unified School District's need to consolidate and integrate access control, alarm monitoring and security video surveillance systems for the District as NMUSD welcomes students and staff back on campus. Through Motorola Solution's Safety Reimagined Solution, Newport-Mesa Unified will be able to unify their security systems into one ecosystem.

To help meet these challenges, Motorola-Avigilon Solutions is pleased to present this proposal for a next-generation School safety solution. As the industry leader in public safety communications, technology, and software, responsible for many Safe Schools solutions in California, including Irvine Unified. Motorola-Avigilon Solutions is ideally suited to meet Newport-Mesa Unified's safety communication requirements.

Our solution design uses high-resolution cameras, leading-edge mobile communications technology, and next-generation dispatch consoles, along with self-learning video analytics and artificial intelligence to help you detect threats more accurately, analyze data more effectively, communicate more efficiently, and respond to incidents more decisively. By adopting Motorola-Avigilon Solutions' proposal, Newport-Mesa Unified will accomplish its stated goals of increased safety and security, while upgrading current infrastructure and equipment to prepare for future needs.

The following pages provide a detailed description of the tools and applications that Motorola Solutions is proposing. To aid in understanding how these tools work together, the description has been organized under four strategic headings:



Each category provides a different kind of support, with tools that will give you better situational awareness, more insight into the data that is available, high-performance on-campus communication, and better responses to incidents.

DETECT



A school campus is a difficult place to keep safe. Threats can arise anywhere; but with limited resources and limited personnel, there's no way for school districts to cover everything all of the time. Giving students and faculty the protection that they need requires detection tools that can flag events for further investigation. With the right technology in place, personnel can see what's happening and act decisively to protect your community.

Anonymous tip submission – Learn about suspicious activities in the area.

Video security – Monitor for significant events site-wide.

License plate recognition – Detect unwanted visitors before they can enter.

Watch list alerting – Find and track known threats on campus.

Face mask detection – Proactive, real-time monitoring for face mask use.

Advanced, video-based detection technology can detect objects, classify them as human, and scan for protective face coverings. Policy violations trigger automated alerts.

Access control – Manage access to an area, blocking unauthorized persons from proceeding through entry points.

Contact tracing – For access controlled areas, trace contacts with exposed students, teachers, and staff to quickly and effectively mitigate risk and curb the spread of infection.

Radio Connectivity - Send video, access control, and sensor alerts from Avigilon Control Center (ACC)™ software to your compatible MOTOTRBO™ radios. Eliminate the need for staffing a video wall, and keep your security officers in the field.

Our solution can bring together the different facets of detection -the community, on-site cameras, and intelligent detection software-to keep your campuses, staff, and students safe.

Video Security

Video Security	
	
☑ ☑ ☑ ☑	One interface for viewing live video from across facilities. Records events for later reference. Intuitive, analytical interface. Recognition, watch list, and analytical capabilities to detect threats early.

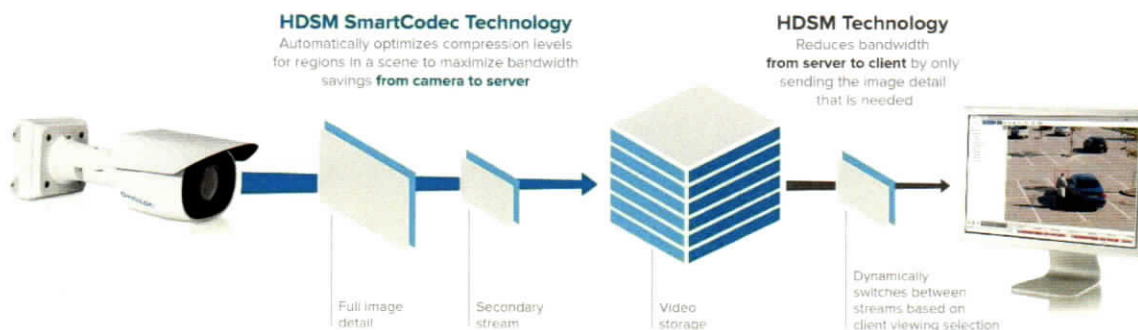
Strategically deployed video cameras and easy-to-operate software provide insight into who is on campus, where they have been, and where they are headed. This puts your team one step ahead of developing threats by directing attention where it belongs.

Avigilon cameras and software record and store video across facilities, using artificial intelligence to direct focus onto potential threats and abnormal events. The proposed video security system will increase situational awareness without creating excess data.

Staff will be able to view live video and review archived footage in a single video management application: Avigilon Control Center (ACC)™. The ACC software is easy to navigate and understand, and offers an additional native user interface called Focus of Attention (FoA). FoA uses color coding and markers to direct Newport-Mesa Unified users' attention to urgent alerts and key sections of recorded video.

FoA organizes cameras into site honeycombs, with nodes for each camera that indicate the status of a scene. Statuses include camera online/offline, motion detected, analytic event detected, face match event, license plate match event, and alarms pertaining to analytic rules or access control events. Staff can hover over a node or click through to view live video from that camera. When an alarm is generated in FoA, it pushes the video feed to the left hand side of the screen, allowing the operator to view the incident and determine proper response. ACC software archives recorded video with timelines, using time markers to indicate video relevant to the user.

The proposed cameras, chosen to address Newport-Mesa Unified's needs, include key video quality and hardware specifications. For situations that call for a high megapixel camera, Avigilon's patented High Definition Stream Management (HDSM)™ technology reduces the bandwidth and storage needed, making efficient use of network resources.



Access Control Manager

Access Control Manager	
	
☒ Enforces badge or biometric-based access to facilities. ☒ Represents events on facility maps, contextualizing alerts. ☒ Integrates with ACC, linking live or recorded video to access events. ☒ Temporary facility access	

Knowing who belongs on campus is a powerful first step towards keeping unwanted visitors out. Badge and biometric scanners allow the administration to manage access to any area by defining the credentials required for admission, times for appropriate access, and keeping track of lost or stolen IDs.

With an Avigilon Access Control Manager (ACM)™ system and access control devices, staff will be able to detect and prevent unauthorized or suspicious visitors from accessing restricted areas. ACM uses badge and biometric readers to match individuals with the permissions database and determine what areas they have access to. Temporary, timed access settings enable staff to issue access badges to visitors or restrict access to a badge that has been lost or stolen.

Access control settings are mapped to Newport-Mesa Unified facilities in ACM, visually representing access points and records. From the map, staff can control doors, monitor access solution hardware status, and check who has accessed an area. ACM links any reported events or alarms to the map. Mapping places events in context and makes it easy to access details.

Combining an ACM system with Avigilon cameras and ACC software adds visual context to access records, and helps detect potential or in-progress attempts to breach security. Security personnel can use cameras at an access point to verify the identity of someone attempting to enter an area. To easily locate video of any past access attempts, ACC tags recorded video of access events detected by ACM.

The proposed video and access control capabilities will funnel detected information into AI analytics, transforming those alerts into actionable intelligence.

Radio Connectivity with Orchestrate

Radio Connectivity	
	
☒	Automatically alerts users via radio.
☒	Alerts include event details.
☒	Alerts can require user acknowledgement.

Radio connectivity proactively notifies staff members of unusual activity, potential threats, and possible hazards by sending voice, text and/or video alarms from Avigilon ACC software to MOTOTRBO radios. A range of events can be configured to trigger radio messages, including video analytics events, license plate watch list matches, unauthorized attempts to access a site, sensor events, and custom flags. The resulting message informs recipients of what event triggered the alert, and where that event took place.

Radio messages inform staff of suspicious activity without needing to monitor activity on a computer screen. Security personnel can patrol the premises, and investigate any alerts they receive on their MOTOTRBO radios. Other members of staff can also receive alarm notifications, automatically communicating potential security information to them so they can take appropriate actions. The connection also accepts messages from MOTOTRBO radios, enabling staff to acknowledge that they have received an alert.

Orchestrate

Creating and automating workflows for a comprehensive incident response and school safety solution is complicated. Orchestrate simplifies it. Orchestrate is a cloud-based platform that connects across voice, data, video, software, and analytics, helping administrators to control their integrated technology ecosystem more effectively. Using its intuitive, drag-and-drop user interface, administrators can create rule-based, automated workflows to enhance efficiency, shorten response times, and improve overall safety.



ANALYZE



With so many people on campus, it can be hard to know what's really a threat. Administrators and teachers are always on the lookout, but even the best personnel cannot predict the future. Schools need a way to sort through the data and find the information that points to a developing incident. Avigilon's self-teaching AI applications help administrators to understand available data and deploy resources as needed – before threats have a chance to develop.

Motion detection and Focus of Attention capabilities – Monitor low-traffic areas for intrusion and immediately capture information about possible threats.

Appearance and identity search – Organize event responses more quickly, sorting through video records to locate footage of known threats.

Video analytics – Scan the campus in real time for evidence of developing incidents.

Elevated temperature detection - Locate individuals with symptoms of an illness to screen entry and avoid outbreaks.

Ultimately, these solutions and insights are crucial to cutting through the noise, proactively locating points of interest and recognizing which events are important – so you can have eyes on the scene to evaluate and make an informed decision to take action. Together, this suite of applications applies pattern recognition, search, and self-learning capabilities to make your staff more effective at identifying potential threats.

Unusual Motion Detection

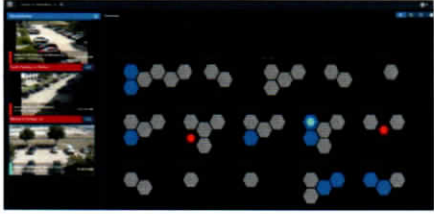
Unusual Motion Detection	
	
	Alerts staff to unusual activity patterns.
	Classifies alerts by type, rarity, and duration.
	Shifts staff away from passive video monitoring.

Schools operate based on rigidly timed schedules, and students follow well-defined traffic patterns. Knowing what to expect helps to identify irregular activity, and may offer insight into developing security threats.

With ACC software's Unusual Motion Detection (UMD) technology, artificial intelligence takes on the mind-numbing task of monitoring areas for abnormal activity. UMD filters out video feeds of routine footage, focusing staff on potential threats or abnormal activity. This feature uses recorded video to establish a typical motion pattern in an area without user input. UMD then alerts

staff members if it detects motion that does not fit that pattern. Pattern recognition develops over a period of up to two weeks and, once established, flags areas based on abnormal movement. ACC software logs events based on detected movement anomalies, and tags video of an event for later reference. Staff can search for events based on type, as well as event rarity and duration.

Focus of Attention

Focus of Attention	
	
☒	Overview of system status at a glance.
☒	Directs staff attention to video of important events.
☒	Quick access to alert details

With a flood of video footage from across campus, your staff cannot watch and analyze video from every camera. ACC's interface uses AI analysis to filter out camera feeds showing routine activity and direct your staff's focus to areas where their evaluation of events is crucial.

The ACC interface uses color-coded camera tags to direct staff members' attention to the most pressing ongoing events. Each camera's detection status is displayed on the "Overview" screen of ACC, providing staff members with a clear picture of the state of events across sites. When a camera reports an event, staff can select it in the interface to actively view video from it. Events use a specific color to let staff know what a camera detected, helping them determine what camera video feeds to actively view.

Appearance Search

Appearance Search	
	

- ☒ Locates video of a person or vehicle based on characteristics.
- ☒ Video bookmarking.
- ☒ Video sharing.

Building a record of locations and activities for unwanted or suspicious visitors can be critical for understanding how to respond, or for helping outside agencies to respond more effectively. Avigilon Appearance Search™ technology reviews hours of video in minutes to find a person or vehicle based on appearance characteristics. This saves time for staff members, reduces response times, and reduces the potential for human error. Criteria for finding people include: clothing color, gender, hair color, and age category, with categories for adults and children. Criteria for vehicles include: color, model, and type of vehicle. Available vehicle type categories include: car, bus, truck, motorcycle, and bicycle. Whether searching for a specific individual or an unknown person based on a partial description, staff can narrow results down to relevant video. Equipped with this technology, personnel can zero in on a person or vehicle of interest and follow their activities as long as they are in the building.

After locating relevant video, staff can play and bookmark it, building a narrative related to persons of interest. If needed, staff can export and share video, images, search results, or bookmarked narratives from ACC software.

Identity Search

Identity Search



- ☒ Locates video using ID records.
- ☒ Search refinement options.

To effectively control access to school facilities, your staff needs to be able to verify the identity of cardholders and quickly locate any imposters. Linking facility access attempts with recorded video makes it easy for staff to determine if a badge has been stolen or if an abnormal access attempt represents a developing threat.

Identity Search combines the facility protection capabilities of ACM with video analytics included with ACC software. Using a person's name or badge ID, staff can retrieve a record of a person's movements within Newport-Mesa Unified' facilities based on what doors they attempted to open.

Staff can refine results by changing what doors to include results for, and setting a date range for access events.

Self-Learning Video Analytics

Self-Learning Video Analytics	
	
	Key object and motion classification in video.
	Improved alert accuracy over time.
	Accepts user feedback to learn faster.

Artificial intelligence can enhance your team's surveillance capabilities by reviewing hours of video input to "learn" what to expect and identify pattern disruptions that may indicate a developing threat or hazard.

The self-learning feature supports Avigilon video analytics, better recognizing people and vehicle movement patterns over time without user input to provide more accurate alerts. Video analytics review past motion detection events to build up patterns that indicate whether a person or vehicle is in motion. Video analytics use those patterns to filter out background movement. In addition to reducing false alarms, self-learning analytics simplify searching archived video. Video analytics highlight videos with moving people or vehicles, filtering out video of unimportant background movement.

Though Avigilon video analytics learns patterns without input, staff can help speed the learning process and improve object classification using the Teach By Example function. With this function, staff apply markers to recorded video of a moving person or vehicle so that video analytics can compare that footage with live video. As more markers are added in different environmental conditions, video analytics becomes increasingly accurate in classifying people or objects in motion.

Elevated Temperature Detection

Elevated Temperature Detection	
	
- Alerts staff if an individual with an elevated temperature is detected. - Smart analysis focuses camera on faces and filters out other heat sources.	

Sometimes, the most potent threat to students and teachers is illness. If undetected, it can spread across campus, putting some at risk. With the H4 Thermal Elevated Temperature Detection camera, Newport Mesa Unified can more efficiently screen individuals for elevated temperatures.

The Avigilon H4 Thermal Elevated Temperature Detection camera is embedded with edge-based analytics to detect faces, measure the temperature of the inner canthus region, and notify operators if individuals exhibit indications of elevated body temperature. This security-grade thermal camera provides a contactless alternative to traditional screening methods. It enables high-throughput pre-screening of people to detect indications of elevated body temperature to keep facilities, and those within them, safe.

The H4 Thermal Elevated Temperature Detection camera works seamlessly with ACC video management software. Elevated temperature events can be configured in ACC, as well as end-to-end workflows for monitoring, assigning, and acknowledging elevated temperature alarms.

COMMUNICATE



A well-protected campus requires a well-directed team of teachers and officers who work together to keep kids safe. But personnel cannot always communicate easily. This requires tools that unify communications, and improve situational awareness.

MOTOTRBO™ two-way radio technology – Keep staff connected in hard-to-navigate environments.

Nitro™ - Flexible broadband data network architecture to support Newport-Mesa Unified's key applications in specific areas.

WAVE™ (Push-to-talk capability) – Personal and group communication between radios and connected phones, tablets, and other smart devices.

Dispatch applications to coordinate resources – Equips dispatchers with voice communications so they can inform personnel of an incident and direct a response to resolve it.

Mass notifications - Simultaneously communicate information to the groups that need it.

Communication – across devices and locations – is an important part of keeping you and your entire team aware and informed at all times. Our end-to-end communications solution can combine voice and data to enable a full understanding of potential incidents and, if possible, prevent them from occurring.

RESPOND



Some incidents cannot be prevented, but getting caught flat-footed makes incidents worse. School administrators and communities need a solution that mobilizes emergency responses immediately and disseminates real-time incident details to on-campus personnel. A robust suite of integrated emergency response technology and applications can get help where it's needed, coordinate onsite operations more effectively, and save lives for your community.

CommandCentral Aware Enterprise - View information in one interface, simplifying intelligence development.

ALLY incident management - Respond to fluid situations with immediate access to new developments as they happen.

Critical Connect - Cloud-based interoperability solution to unify communications with public safety partners, and enhance collaboration for a unified response.

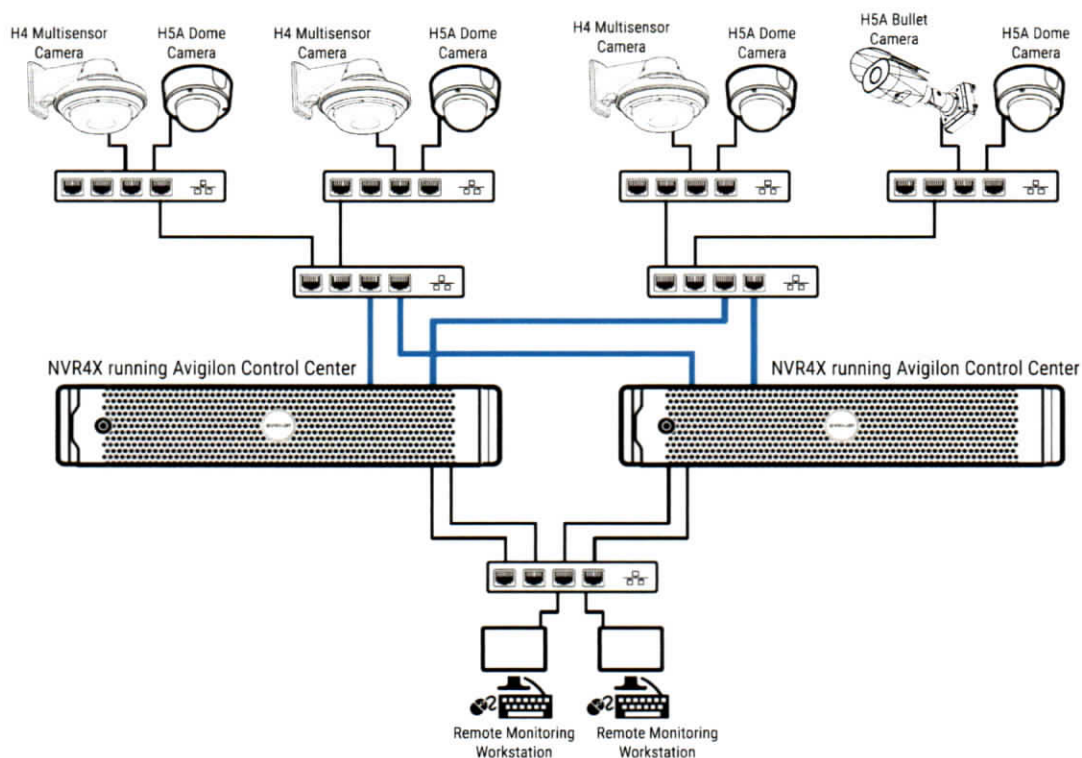
Connection to Law Enforcement – Use CommandCentral Aware to provide situational awareness for first responders by sending data to local law enforcement during an escalated incident.

Body-worn cameras - Record or stream video of emergencies and security incidents, creating a record of actions and a clearer understanding of events.

Access control to mitigate emergencies – Dynamically alter access permission to vulnerable or critical areas during emergencies, blocking access to potential threats.

These tools help make certain the right resources are sent to an event, and that those resources have the most up-to-date information necessary to remedy the situation

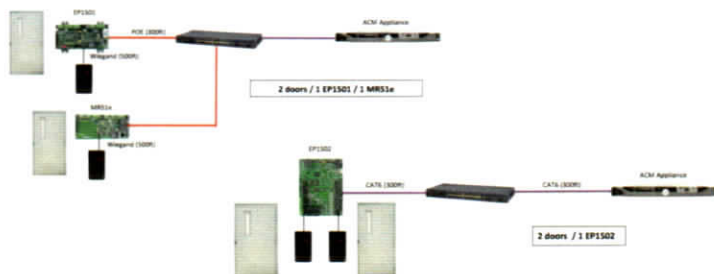
Sample Network Topology for ACC



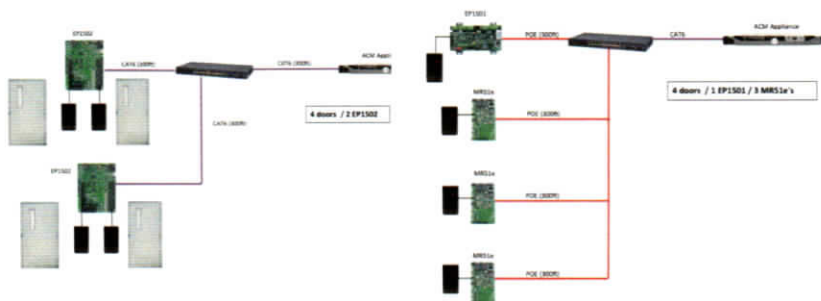
Sample Topology for ACM

2 Door Sample Designs

avigilon
a Motorola Solutions Company

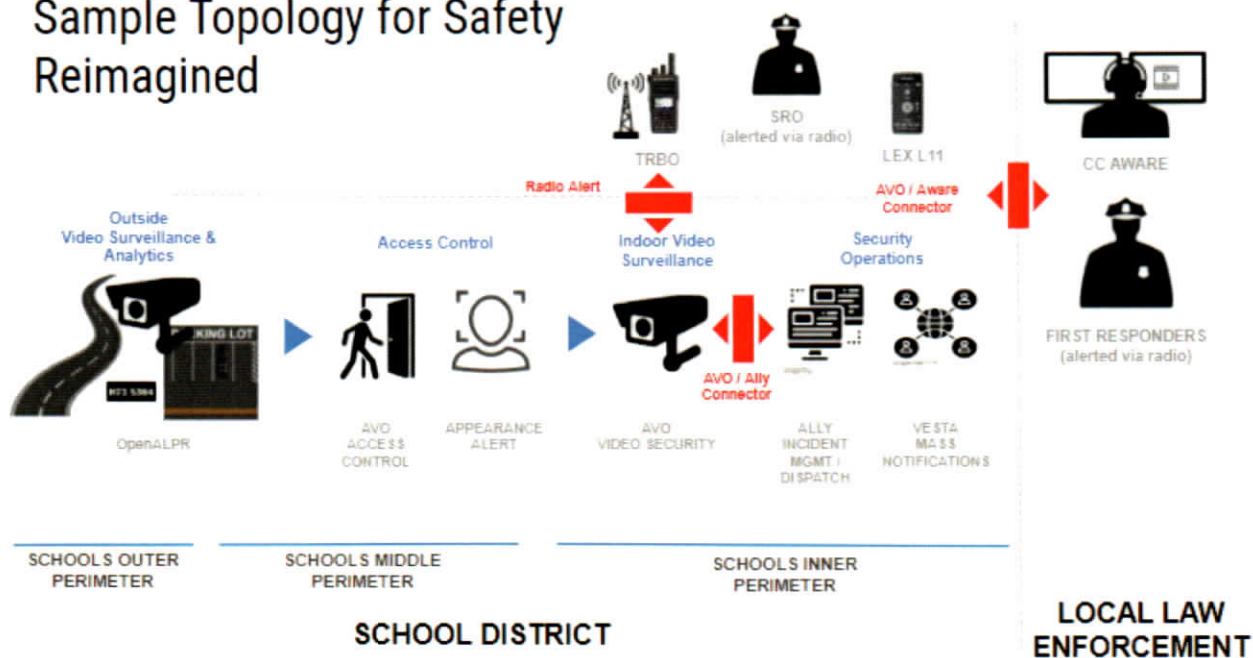


4 Door Sample Designs



© 2021 Motorola Solutions. All rights reserved. MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

Sample Topology for Safety Reimagined



Glossary

NVR4X - 4th generation Avigilon Networked Video Recorder. Provides secure, reliable and scalable platforms for high performance end-to-end security solutions. All NVRs are preloaded with Avigilon Control Center (ACC) for secure network video recording and management of multi-megapixel IP cameras and have storage capacities up to 217TB.

Remote Monitoring Workstation - Avigilon's Remote Monitoring Workstations are purpose-built to accompany Avigilon's Network Video Recorders (NVRs) or to expand and scale existing deployments with a cost-effective high-performance workstation for remote monitoring. Designed to work seamlessly with Avigilon Control Center[™] video management software, the Remote Monitoring Workstations enable users to view high definition video streams on multiple monitors or video walls.

H4 Multisensor Camera - The H4 Multisensor camera line combines Avigilon self-learning video analytics with exceptional coverage, featuring 3 or 4 individually configurable camera sensors that can be positioned to monitor 180°, 270°, or 360° fields of view. With up to 32 MP effective resolution, the H4 Multisensor can provide the image quality needed to cover larger areas with excellent detail.

H5A Dome Camera - A camera in Avigilon H5A camera line in a dome form factor which features our embedded Next-Generation Video Analytics for enhanced object detection, tracking and classification, Unusual Activity Detection (UAD), and support for Avigilon Appearance Search[™] technology to help ensure critical events do not go unnoticed. Comes in either 2MP, 4MP, 6MP, or 8MP resolutions.

H5A Bullet Camera - A camera in Avigilon H5A camera line in a bullet form factor which features our embedded Next-Generation Video Analytics for enhanced object detection, tracking and classification, Unusual Activity Detection (UAD), and support for Avigilon Appearance Search[™] technology to help ensure critical events do not go unnoticed. Also features IR ranges up to 295 ft. depending on lens type. Comes in either 2MP, 4MP, 5MP, 6MP, or 8MP resolutions and focal lengths up to 22mm.

Next-Generation Video Analytics - Avigilon's most advanced analytics technology uses neural networks to power self-learning video analytics, delivering improved accuracy in both perimeter

protection and in crowded, indoor environments. Added processing power enables the tracking and classification of over 50 objects within a field of view. More processing power enhances Avigilon Appearance Search™ technology by expanding the ability to search for a person or vehicle in both crowded and indoor environments. Avigilon video analytics not only classifies people and vehicles, but can also classify vehicles into subtypes which include car, truck, bus, motorcycle, and bicycle. Allowing a user to search for events specifically generated by people or vehicle types can increase efficiency and reduce investigation times.

Appearance Search - Avigilon Appearance Search™ video analytics technology is a sophisticated deep learning AI search engine for video. It sorts through hours of video with ease, to quickly locate a specific person or vehicle of interest by entering physical descriptions, uploading a photo, or by finding an example within recorded video. Appearance Search can improve incident response time and enhance forensic investigations by helping operators compile robust video evidence, create a powerful narrative of events, and reveal a vehicle or individual's route or last-known location.

UAD - Unusual Activity Detection (UAD) provides new edge-based intelligence that uses advanced AI technology. It is designed to enable the detection of atypical activities, such as people and vehicles travelling at faster speeds or are in unusual locations and alert operators.

ACC - Avigilon Control Center (ACC) software is an easy-to-use video management software that is designed to optimize the way security professionals manage and interact with high-definition video. It efficiently captures and stores high definition video, while intelligently managing bandwidth and storage using our patented High Definition Stream Management (HDSM) technology.

HDSM - High Definition Stream Management is a stream management technology that drastically reduces server-client bandwidth requirements and makes optimal use of client computing resources, enabling greater scalability and increased camera resolution. HDSM technology stores the video information on the server as small packets. Simultaneously, HDSM separates the video into multiple usable segments: lower resolution and smaller size streams for situational awareness, and much larger streams for full image detail. HDSM then intelligently manages these streams based on what the user is viewing

ACM - Avigilon Access Control Manager™ 6 Enterprise and Enterprise Plus Systems The Access Control Manager (ACM) system is an IT-friendly Physical Access Control System (PACS) from Avigilon for enterprise-class installations. It's a complete access solution that is designed to keep

your focus on securing your people, property and assets, and maximizing your time by helping you respond immediately to alerts wherever you are. The ACM[™] system is a browser-based solution that can integrate with existing IT/HR systems, minimizing the need for duplicate data entry. It comes with a full set of standard features that not only help to maximize your time, but will reliably safeguard your information.

ACM Virtual - Avigilon Access Control Manager[™] 6 Virtual is a physical access control system (PACS) that is VMware Ready[™] for deployment in a virtual server environment, eliminating the need to maintain a separate, stand-alone server or dedicated network appliance. Access Control Manager Virtual is purpose-built for organizations that have migrated their IT infrastructure to a secure, private cloud environment, allowing them to maintain enterprise-grade physical security without the risk of storing sensitive information on a shared server hosted in a public cloud.

LP1501 - Intelligent Controller; Linux Based with 1 door; 2 inputs and 2 outputs; PoE+ Support; expandable up to 17 doors. (Mercury Part #: LP1501)

LP1502 - Intelligent Controller; Linux Based with 2 doors; 8 inputs and 4 outputs; expandable up to 64 doors. (Mercury Part #: LP1502)

MR62e - Reader Interface Module with 2 doors; 4 inputs and 4 outputs; PoE+ Support. (Mercury Part #: MR62e)

Ally - Ally is a cloud-based incident and records management software product that collects security data in a single database. The Incidents page includes standard forms, using pre-set fields to create complete and consistent records. With customization options for certain fields, Ally Incident forms can be changed to collect specific information your staff and decision-makers need.

RFI Questionnaire

I. General Requirements	
A. Deploy systems and integration with the best value to the District	Avigilon's Access Control Manager (ACM) and Avigilon Control Center (ACC) have been deployed at many school districts across North America. ACC's total cost of ownership is lower compared to other solutions because of how our software is licensed. Our channel licenses are a one time purchase. We do not have annual recurring fees for incremental version updates (e.g. from v7.00 to v7.99) or technical support. We also offer a 5 year advance replacement warranty on our cameras and NVRs. No training fees. One time licensing rather than annual recurring fees
B. Implement proven and reliable technology	ACM supports field hardware produced by Mercury Security which has the largest installed base of any OEM Access Control panel manufacture and has been in business since 1992. The H5A camera line features our next-generation video analytics technology to help focus your attention on potentially critical events, providing a smarter and more powerful video security solution from the moment you set it up. 5 Year warranty included. https://www.avigilon.com/products/cameras-sensors/

	https://www.avigilon.com/products/video-infrastructure/nvr https://www.avigilon.com/products/ai-video-analytics/ When connected to Avigilon Control Center (ACC) software, the Avigilon AI Appliance adds patented Avigilon self-learning video analytics and Avigilon Appearance Search™ technology to almost any IP camera. Fourth-generation Avigilon Network Video Recorders (NVRs) offer our highest capacity, retention and throughput to provide secure, reliable and scalable platforms for high-performance security solutions. NVR4s come standard with optimized recording technology, a three-year Avigilon limited warranty with dedicated support and numerous additional features, including Avigilon Appearance Search technology.
C. High to medium-high system maturity level	Avigilon's products have been manufactured, sold, and deployed since 2006.
D. Scalable	ACM supports up to 2048 doors on a single server (or virtual instance). You can grow beyond this by adding additional ACM instances for limitless scalability. ACC can support >300 cameras per server, >10,000 cameras per site, and >100 servers per site. Although no limits are imposed by licensing, actual limits will depend on the hardware environment. Avigilon has tested

	up to the numbers indicated. Additionally, Avigilon's storage solutions can scale up to 1.5PB, if necessary.
E. Flexible – communication/ issues at individual schools. Some have better connections than others.	ACC can operate in low bandwidth networks because of our High Definition Stream Management (HDSM) technology, which sends you only the portion of the image that you need. That means you get incredible image quality and resolution with only a tiny amount of bandwidth and storage. HDSM is all about intelligently managing bandwidth and storage, which means that you never have to worry about adding more megapixels. HDSM keeps file sizes small, so you can add cameras while keeping bandwidth and hardware needs low. Using less data and less bandwidth means you can scale up while keeping costs down, with minimal impact on network resources.
F. Serviceable by NMUSD staff	NMUSD staff can contact Avigilon technical support directly via phone and email. Avigilon also provides free online training and an online help center for both video and access control, which can be found at help.avigilon.com
G. Simple and efficient integration	Avigilon cameras and ACC conform to ONVIF standards. ONVIF is a global and open industry forum with the goal of facilitating the development and use of a global open standard for the interface of physical IP-based security products. ONVIF creates a standard for how IP products within video surveillance and other physical security areas can communicate with each other.

H. Support for wireless solutions	Avigilon cameras can operate on wireless networks, provided there is sufficient throughput and reliable connectivity, but wired networks are preferred.
I. Compatible with District's HP servers	Avigilon recommends using Avigilon branded servers, because they are purpose built to provide secure, reliable, and scalable platforms for high-performance security solutions, but ACC can run on 3rd party servers, including HP, provided that they meet or exceed our recommendations.
J. Deployable in a virtual server environment	Avigilon ACM: ACM Virtual is a Certified VMware Ready solution designed for deployment on a virtual server, maintaining scalable design while reducing capital and operating expenditures Avigilon ACM also has upcoming support for Hyper-V. Avigilon ACC: Avigilon has not done any formal testing with virtualization. You will generally get better performance running ACC within a native host OS on a physical server, but as long as the ACC Server process is allocated sufficient resources more than the recommended system requirements, there should not be any issues. Allocate additional resources (CPU and memory) to the virtual machine for ACC Server. You need to consider the virtualization overhead when you plan for the hardware of your host server.

K. Active Directory integration	ACM supports Active Directory integration via LDAP. ACC supports Active Directory integration.
L. Multiple local integrators (single regional integrator is not acceptable)	There are multiple Avigilon partners in the Southern California Region including (but not limited to) BlueViolet Networks, Vector USA, Johnson Controls & Multicard
M. Direct manufacturer support	Avigilon offers direct support for sales and support from regional teams and direct 24/7 end user tech support via our +1 888-281-5182 number. All services are at no additional cost.
N. No sole source equipment	Avigilon products can be purchased from any of our partners in the region.
O. Strong cyber-security support – Manufacturer responses must discuss cyber-security plan in response and also explain how firmware updates are performed	When using Avigilon cameras along with Avigilon ACC software, camera firmware is automatically pushed out to connected cameras as a part of the software update process. Users can optionally choose to defer these updates, although it is not recommended. Firmware can also be updated as a batch operation using Avigilon's Camera Configuration Tool, or by logging directly into a camera's web interface. See attached flyer in supplemental documents
P. No biometrics	Facial recognition is an optional, paid (licensed) feature of ACC. It is not available by default.
Q. Audio capability	Avigilon cameras come with an audio input and output for connecting external

1. Voice communication capability desired but voice recording will be disabled per District policy	microphones and speakers. A few of our camera models come with a built in microphone. Voice recording can be turned on or off in the ACC Client software.
--	---

II. Access Control

A. Access control technology not susceptible to cloning	ACM allows the use of secure, encrypted credentials in a variety of technologies. ACM fully supports OSDP for secure and supervised reader communications.
B. Proximity technology access cards (contactless smartcards)	ACM fully supports contactless smart card technology
C. Support for wireless solutions	Wireless Lock Support for Allegion, Assa Abloy & Salto.
D. Lockdown controls	ACM provides a single button-quick emergency lockdown of all entry points in case of emergency (external threat, etc.) And also allows for handling multiple emergencies simultaneously.
E. Integration with Intrusion Detection Systems	Supported
F. Consideration for future Cloud deployment	Yes
G. Mercury Security or similar intelligent panels available to multiple manufacturers (panels supported by only one system software manufacturer are not acceptable)	Our system works with Mercury Security.

III. Video Surveillance

A. Consider integration with Police Department	We would need to know what video system the Police Department currently uses to determine what kind of integration is possible, but our system can be set up to be accessed by the Police Department through Avigilon Cloud Services (ACS), either through a web browser connection or by using our mobile application.
B. Local video recording server at each site	Video is recorded to on-premise NVRs.
C. Redundancy/backup	Avigilon NVRs are configured for either RAID 60, RAID 6, or RAID 5. Cameras can be configured to record to failover servers in the event that the primary server fails or loses connectivity.
D. Public monitor in admin waiting area	A workstation running the ACC Client or ACC Virtual Matrix can be displayed on a monitor in the admin waiting area.

E. Support for video analytic	Avigilon's H5A cameras and H4A multi-sensor cameras come with Avigilon self-learning video analytics features for object detection and classification for live or forensic events. These analytics include: • Objects in Area • Object Loitering • Objects Crossing Beam • Object Appears or Enters Area • Object Not Present in Area • Objects Enter Area • Objects Leave Area • Object Stops in Area • Direction Violated • Camera Tampering • Social Distancing (H5A Only) • Occupancy Counting When H5A cameras or H4A multi-sensor cameras are paired with the appropriate NVR, ACC can generate events/notifications when it detects a person not wearing a mask and can perform Appearance Searches, which allows a user to search for people or vehicles based on physical characteristics.
--------------------------------------	---

IV. Video Recording	
A. Standard video compression (H.264/H.265)	Avigilon H5A and H4 Multisensor cameras support both the H.264 and H.265 codecs. This can be configured on a per camera basis.
B. 45 days recorded video	The system will be designed with the appropriate server or servers to achieve the required video retention.
C. Motion sense recording	Motion detection can be used to trigger video recording. You can also configure the system to generate motion events that can be used when searching video or to trigger notifications and rules. There are two types of motion detection available: Classified Object Motion Detection analyzes the video and only reports the motion of vehicles or persons. This option is only available to Avigilon self-learning video analytics devices. Pixel Motion Detection observes the video stream as a whole and considers any change in pixel as motion in the scene. This option is available to most cameras that are connected to the system.
D. 5-10 frames per second recording rate	Avigilon's cameras are capable of recording up to 30 frames per second (fps), depending on the camera model. The recording rate can be configured on a per camera basis.

V. Video Cameras

A. Vandal resistant camera housings that conceal direction of view	Avigilon's H5A Indoor and Outdoor domes and bullets have an IK10 impact rating. The H4A surface and pendant mount multi-sensor cameras also have an IK10 impact rating. Optional dome and multi-sensor camera covers with a smoked bubble can be purchased to be used instead of covers that have a clear bubble.
B. Minimum 3 Megapixel resolution	Avigilon's H5A cameras come in resolutions up to 8MP. H4A Multi-sensor cameras come in resolutions up to 8MP per sensor.
C. Onboard storage	Avigilon's H5A cameras and H4A multi-sensor cameras come with either a microSD or SD slot depending on the camera form factor.

VI. Intrusion Detection

A. Support existing Ademco/Honeywell systems	Can be interfaced using outputs and inputs.
B. Integration with the Access Control System to provide for disarming the Intrusion Detection by presenting access credentials to record an audit trail	Supported with Intrusion Detection interfacing.

Additional RFI Response Requirements

Similar and Completed Solution Deployments in K-12 Schools with 20,000 ADA or higher

1. Irvine Unified, CA (ADA 35,000)	
Contact Name	Don Grudem
Email	dongrudem@iusd.org
Phone Number	(949) 936-5350

2. Fullerton Unified, CA (ADA 13,000)	
Contact Name	Sam Ricchio
Email	sam_ricchio@fullertonsd.org
Phone Number	(714) 447-7483

3. Tustin Unified, CA (ADA 23,000)	
Contact Name	Doug Heckathorn
Email	dheckathorn@tustin.k12.ca.us
Phone Number	(714) 730-7305

4. Oak Park Unified, CA (ADA 4,000)	
Contact Name	Enoch Kwok
Email	ekwok@oakparkusd.org
Phone Number	(818) 735-3201

5. Irvine Valley College, CA	
Contact Name	Anna Petrossian
Email	apetrossian@ivc.ed
Phone Number	(949) 541-5708

Budgetary Costs for Purchasing

At Avigilon, we work with our local integrators to meet the needs of Newport-Mesa. **In order to give accurate pricing**, there are a number of factors that will affect the overall solution (for instance: obstructed views, amount of area needed to be covered, corners, lighting, megapixels needed per area etc.). We will work closely with Newport-Mesa Unified to give you the fewest cameras with the most coverage as well as the best solution for access control. Before giving accurate pricing, a site walk would be needed to give an accurate estimate. As mentioned, there are no recurring fees with Avigilon and free online training and support are included.

Pricing should be considered when given by a partner integrator. Avigilon can negotiate pricing and special district wide discounts to all partners so Newport-Mesa Unified will receive a fair price across the board. Below is a sample setup for a high school with MSRP (not including integrator or partner discounts):

Model Name	Description	MSRP
2.0C-H5A-DO1-IR	2.0 MP (1080p) WDR, LightCatcher, Day/Night, Outdoor Dome, 3.3-9mm f/1.3 P-iris lens, Integrated IR, Next-Generation Analytics	\$1,000
2.0C-H5A-D1-IR	2.0 MP (1080p) WDR, LightCatcher, Day/Night, Indoor Dome, 3.3-9mm f/1.3 P-iris lens, Integrated IR, Next-Generation Analytics	\$850
4.0C-H5A-DO1-IR	4.0 MP WDR, LightCatcher, Day/Night, Outdoor Dome, 3.3-9mm f/1.3 P-iris lens, Integrated IR, Next-Generation Analytics	\$1,142
4.0C-H5A-D1-IR	4.0 MP WDR, LightCatcher, Day/Night, Indoor Dome, 3.3-9mm f/1.3, P-iris lens, Integrated IR, Next-Generation Analytics	\$992
4.0C-H5A-BO1-IR	4.0 MP WDR, LightCatcher, 3.3-9mm f/1.3 P-iris lens, Integrated IR, Next-Generation Analytics	\$1,142
5.0C-H5A-BO2-IR	5.0 MP WDR, LightCatcher, 9-22mm f/1.6 P-iris lens, Integrated IR, Next-Generation Analytics	\$1,245
6.0C-H5DH-D1-IR	2x 3MP H5A Dual Head Camera. Indoor camera with built-in IR,	\$1,300

	Next-Generation Analytics	
10.0C-H5DH-D1-IR	2x 5MP H5A Dual Head Camera. Indoor camera with built-in IR. Next-Generation analytics.	\$1,500
15C-H4A-3MH-180	3x 5 MP, WDR, LightCatcher, 4mm, Camera Only	\$1,800
15C-H4A-3MH-270	3x 5 MP, WDR, LightCatcher, 2.8mm, Camera Only	\$1,800
20C-H4A-4MH-360	4x 5 MP, WDR, LightCatcher, 2.8mm, Camera Only	\$2,100
ACC7-ENT	ACC 7 Enterprise Edition camera license	\$290
POE-INJ2-60W-NA	Indoor single port Gigabit PoE++ 60W	\$150
H4-MT-POLE1	Pole mount adapter for use with H4A-MT-WALL1, H4-BO-JBOX1, H4SL, H4F, H4 PTZ, H4 IR PTZ and H4 Multisensor cameras.	\$90
H4-BO-JBOX1	Junction box for the H4A HD Bullet, H4SL HD Bullet, or H4 Thermal cameras.	\$90
H4AMH-AD-IRIL1	Optional IR illuminator ring, up to 30m (100ft), for use with H4AMH-DO-COVR1.	\$330
IRPTZ-MNT-WALL1	Pendant wall mount adapter. For use with H4 IR PTZ or H4A-MH-AD-PEND1 on H4 Multisensor.	\$95
H4AMH-DO-COVR1	Dome bubble and cover, for outdoor surface mount or pendant mount, clear.	\$160
H4AMH-AD-PEND1	Outdoor pendant mount adapter.	\$160
H4-MT-CRNR1	Corner mount adapter for use with H4A-MT-Wall1, H4-BO-JBOX1, H4SL, H4F, H4 PTZ, H4 IR PTZ and H4 Multisensor cameras.	\$90
NVR4X-STD-48TB-S16-NA	NVR4X Standard 48TB 2U Rack Mnt, Windows Server 2016, NA	\$24,960

QTY	Model Name	Description	MSRP	Line Total
1	AC-APP-64R-ENT2-6	Access Control Manager Enterprise 6 – Web-Based PACS Enterprise Appliance for 64 Intelligent Controller, Linux Based with 2 doors, 8 inputs and 4 outputs, expandable up to 64	\$ 6,166.00	\$ 6,166.00
1	AC-MER-CONT-LP1502	Series 3 Two-Reader Interface Module: mag or	\$ 1,280.00	\$ 1,280.00
29	AC-MER-CON-MR52	wiegand, 8 inputs, 6 relays (Mercury Part Sixteen Door Mercury Dual Voltage Integrated	\$ 705.00	\$ 20,445.00
4	AC-LSP-16DR-MER-LCK	Power System supporting one AC-MER-CONT-	\$ 1,130.00	\$ 4,520.00
59	AC-HID-MCLASS-SE-PROX-OSDP-920PTPEK00387	R40 Standard wall switch; HID Prox, AWID and EM4102 (32 bits); ICLASS Seos, SE, SR,	\$ 315.00	\$ 18,585.00

Supplemental Data



SMART SECURITY SOLUTIONS FOR EDUCATION

Avigilon provides comprehensive video security and access control solutions that help you create a safe and secure environment and protect what is most valuable — your students, staff and faculty.

AI-POWERED VIDEO SECURITY

Avigilon Control Center (ACC) software provides an easy-to-use, AI-enabled user interface that brings the right information to you so that you can take action, helping ensure critical events do not go unnoticed.

POWERFUL SEARCH

Avigilon Appearance Search™ technology sorts through hours of video with ease to quickly locate a specific student, visitor or vehicle of interest across school grounds in near real-time.

USER-FRIENDLY DESIGN

User-friendly software is straightforward and intuitive, allowing your School Resource Officer to operate and manage the system, whether they are an IT novice or an expert.

EASY INTEGRATION AND COST SAVINGS

Our open platform security solutions allow for easy integration with your existing systems and technology, allowing you to expand your security solution with no overhaul required, and our video management system (VMS) works with both HD and analog cameras. Our cameras are compatible with a variety of VMS platforms and our access control solutions support open field hardware from other leading manufacturers.

EFFICIENT BANDWIDTH MANAGEMENT

Avigilon's High Definition Stream Management (HDSM) and HDSM SmartCodec™ technologies reduce bandwidth and storage needs while maintaining image quality, helping to keep internet connectivity costs down.



ORCHESTRATE

A simple, user-friendly and cloud-based workflow automation tool that gives you the ability to configure and automate workflows that control your integrated technology ecosystem.

AVIGILON CLOUD SERVICES

Manage multiple campuses from anywhere with convenient, centralized access to your system using a browser or our ACC Mobile app and remotely monitor the health of all your cloud-connected ACC sites to quickly assess maintenance activities.

H4 VIDEO INTERCOM

Combines a 3 MP wide dynamic range, low-light camera, with a high-performance intercom featuring noise reduction and echo-canceling technologies.

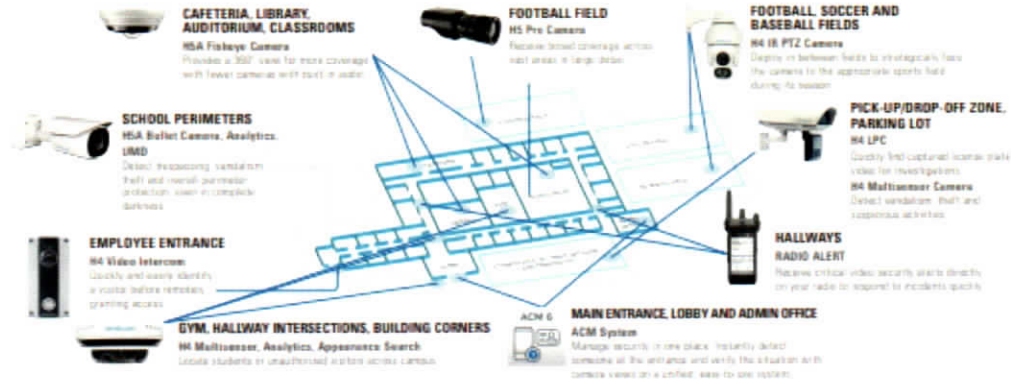
AI NVR

A purpose-built security-hardened NVR, with built-in server-side analytics that unlocks Avigilon's advanced AI capabilities for any connected video stream, including third party and non-analytic cameras.

ACCESS CONTROL MANAGER (ACM)

ACM generated door events allow you to create rule-based actions and notifications for quick on-site responses, including immediate school-wide lockdown.

NEXT GENERATION SAFETY FOR THE NEXT GENERATION



COVID-19 RESPONSE SOLUTIONS FOR EDUCATION

NO FACE MASK DETECTION

Detects individuals who are in violation of face mask policies, prompting an automated alert through ACC™ video management software for quick, corrective action.

SOCIAL DISTANCING ANALYTICS

AI-powered analytics on Avigilon video security cameras can continuously monitor social distancing efforts within your school. Run a report of when social distancing violations occur, as well as recognize high violation zones and times requiring corrective measures.

OCCUPANCY COUNTING

Know how many students and staff members are inside a room at any given time, determine peak periods, and understand high traffic entry or exit points that require further attention.

ELEVATED TEMPERATURE DETECTION

Increase the efficiency of traditional physical screening efforts with a high-throughput and contactless method of pre-screening people at access points. The H4 Thermal Elevated Temperature Detection solution detects and notifies operators if individuals exhibit indications of elevated body temperature so that further evaluation may take place.

Avigilon, a Motorola Solutions company, designs, develops and manufactures solutions in video analytics, cloud, security cameras, video management software and hardware, and access control. Avigilon is an industry leader and, together with Motorola Solutions, provides integrated solutions for video security, access control and critical communications. Avigilon is proud to offer 24/7 technical support and complimentary software training.

FOR MORE INFORMATION,
ASISALES@AVIGILON.COM

Visit info.avigilon.com/education



CORONAVIRUS RESPONSE & RELIEF ACT EDUCATION STABILIZATION FUND

\$82 BILLION

**FUNDS
AVAILABLE**

**CONSIDER COMMUNICATIONS, SOFTWARE &
VIDEO TECHNOLOGY SOLUTIONS**

FUNDING HIGHLIGHTS

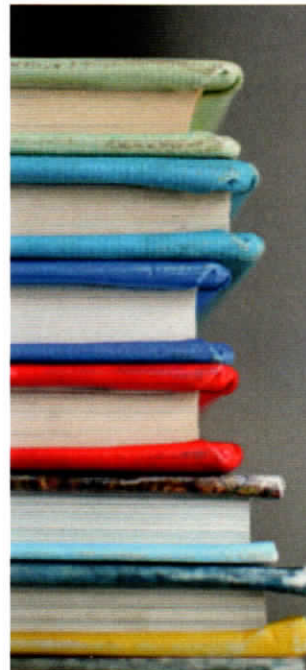
The Coronavirus Response & Relief Act provides a refresh of three CARES Act grant programs under the umbrella of the Education Stabilization Fund.

- Elementary and Secondary School Emergency Relief (ESSER II) Fund (\$54.3 billion)
- Higher Education Emergency Relief (HEER II) Fund (\$22.7 billion)
- Governor's Emergency Education Relief (GEER II) Fund (\$4.1 billion)

These grant programs are being administered through the U.S. Department of Education and are intended to support efforts by states, schools and institutions of higher learning to prevent, prepare for, and respond to coronavirus, but each has a different focus and are subject to different eligibility requirements.

WHO CAN APPLY

- ESSER Fund: State Education Agencies (SEAs) apply and must allocate at least 90% as subgrants to Local Education Agencies (LEAs), including school districts and charter schools
 - SEA allocations may be found [here](#).
- HEER Fund: Institutions of Higher Education (IHEs)
 - Public and nonprofit institution allocations may be found [here](#).
- GEER Fund: Governors apply and make subgrants to most significantly impacted LEAs and IHEs in the State
 - State allocations may be found [here](#).



GRANT EXECUTIVE SUMMARY | CARES ACT EDUCATION STABILIZATION FUND

 **MOTOROLA SOLUTIONS**

ALLOWABLE USES OF FUNDS

ESSER II FUND:

- Any activity authorized by the Elementary and Secondary Education Act, the Individuals with Disabilities Education Act, and other education statutes.
- Coordination of preparedness and response efforts of local educational agencies with state, local, tribal, and territorial public health departments, and other relevant agencies, to improve coordinated responses among such entities to prevent, prepare for, and respond to coronavirus.
- Providing principals and other school leaders with the resources necessary to address the needs of their individual schools.
- Activities to address the unique needs of low-income children or students, children with disabilities, English learners, racial and ethnic minorities, students experiencing homelessness, and foster care youth, including how outreach and service delivery will meet the needs of each population.
- Developing and implementing procedures and systems to improve the preparedness and response efforts of local educational agencies.
- Training and professional development for staff of the local educational agency on sanitation and minimizing the spread of infectious diseases.
- Purchasing supplies to sanitize and clean the facilities of a local educational agency, including buildings operated by such agency.
- Planning for and coordinating during long-term closures, including for how to provide meals to eligible students, how to provide technology for online learning to all students, how to provide guidance for carrying out requirements under IDEA and how to ensure other educational services can continue to be provided consistent with all Federal, State, and local requirements.

HEER II FUND:

- Defray expenses associated with coronavirus (including lost revenue, reimbursement for expenses already incurred, technology costs associated with a transition to distance education, faculty and staff trainings, and payroll).
- At least 50% of the funding must go toward emergency financial aid grants to students for expenses related to disruption of campus operations related to coronavirus.

GEER II FUND:

- Provide emergency support through grants to local educational agencies and institutions of higher learning that are deemed to have been most significantly impacted by coronavirus to support their ability to continue to provide educational services and to support their on-going functionality.
- Provide support to any other institution of higher education, local educational agency, or education related entity within the State that the Governor deems essential for carrying out emergency educational services to students.

- Purchasing educational technology (including hardware, software, and connectivity) for students who are served by the local educational agency that aids in regular and substantive educational interaction between students and their classroom instructors, including low-income students and students with disabilities, which may include assistive technology or adaptive equipment.
- Providing mental health services and supports.
- Planning and implementing activities related to summer learning and supplemental afterschool programs, including providing classroom instruction or online learning during the summer months and addressing the needs of low-income students, students with disabilities, English learners, migrant students, students experiencing homelessness, and children in foster care.
- School facility repairs and improvements to enable operation of schools to reduce risk of virus transmission and exposure to environmental health hazards, and to support student health needs.
- Inspection, testing, maintenance, repair replacement, and upgrade projects to improve the indoor air quality in school facilities, including mechanical and non-mechanical heating, ventilation, and air conditioning systems, filtering, purification and other air cleaning, fans, control systems, and window and door repair and replacement.
- Other activities that are necessary to maintain the operation of and continuity of services in local educational agencies and continuing to employ existing staff of the local educational agency.

DEADLINES AND ADDITIONAL PROGRAM DETAILS

Consistent with Congressional intent to provide funding quickly and with minimal administrative burden, the Department of Education is awarding funds to eligible entities without the need to submit an application, except institutions of higher education that did not receive HEER funding under the CARES Act funding must submit an application for HEER II funding by April 15, 2021.

ESSER II funding must be awarded by SEAs within one year of receipt (i.e., by January 2022) and must be obligated by SEAs and subrecipients by September 30, 2023.

HEER II funding must be expended by institutions within one year from the date of their award.

GEER II funding must be awarded by governors within one year of receipt (i.e., by January 2022) and must be obligated by governors and subrecipients by September 30, 2023.

Further details and guidance on these programs:

[ESSER I](#)
[HEER I](#)
[GEER I](#)



CONSIDER SAFETY AND SECURITY SOLUTIONS TO ENSURE A SAFE AND HEALTHY ENVIRONMENT. FROM MOTOROLA SOLUTIONS FOR YOUR EDUCATION STABILIZATION FUND DOLLARS

DISTANCE LEARNING

Ensure every student can access online learning programs from the safety of their own homes with Nitro™, the Motorola Solutions' private LTE solution. This functional and cost effective solution provides enterprise-grade private LTE as a wireless backhaul to your school's network. Combine the simplicity of an easy installation without miles of cables, and heavy maintenance work in each student's home, all with the added control of having complete ownership over your network.

SOCIAL DISTANCING TECHNOLOGY

Monitor social distancing violations automatically by measuring the distance between people so you can identify high-violation zones and times that require improvement.

OCCUPANCY COUNTING TECHNOLOGY

Monitor and manage occupancy rates by counting the number of students and staff members in a specific area of your campus, such as the library or gymnasium, to support social distancing.

NO FACE MASK DETECTION TECHNOLOGY

Automate the detection of students who are not wearing face masks with alarms to flag violations in real-time so you can take corrective measures.

CONTACT TRACING TECHNOLOGY

Physical access control helps with contact tracing to prevent contamination if an infected person is identified.

THERMAL TEMPERATURE SENSING CAMERAS

High-throughput, contactless alternative to traditional screening for elevated temperatures at entrances for preventative protection.

Learn more at www.motorolasolutions.com/education

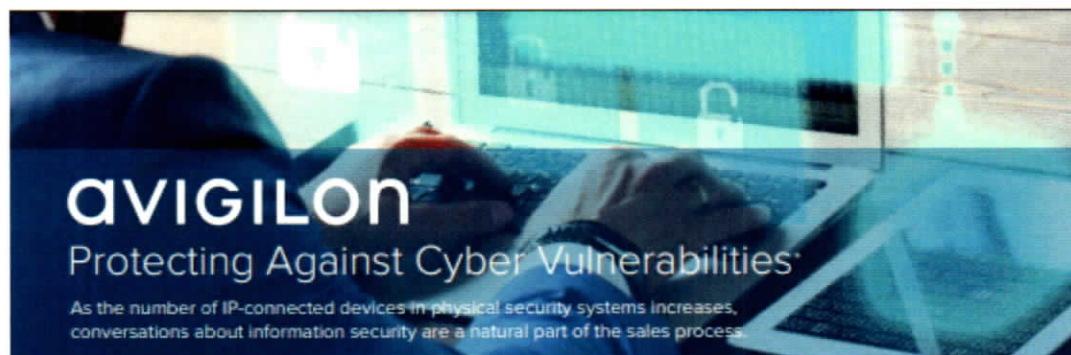
Motorola Solutions offers a variety of solutions that can be deployed to help education agencies of their cybersecurity, response and mitigation efforts. This page only offers a view into Education Stabilization Fund grants on these solutions and you should consult your SEA and/or legal department if you have questions.



MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60601 U.S.A. www.motorolasolutions.com

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2021 Motorola Solutions, Inc. All rights reserved. 09-2021



avigilon

Protecting Against Cyber Vulnerabilities

As the number of IP-connected devices in physical security systems increases, conversations about information security are a natural part of the sales process.

Organizations such as the National Institute of Standards and Technology (NIST) are actively proposing an Identify-Protect-Detect-Respond-Recover framework for cyber security. The [NIST framework](#) advocates the identification of key business risks due to cyber threats, such as the protection of data, devices, and services, continuous monitoring to enable detection of cyber security events as they happen, and the development of a clear response and recovery process.

The Three Layers of Avigilon Cyber Protection

The protection of data, devices, and services can be successful only if the network-connected software and hardware implement appropriate defensive measures to ensure integrity, confidentiality, and availability.

Integrity | Ensuring data and the function of the system are not maliciously or inadvertently manipulated

The integrity of a system is compromised when the software is maliciously modified or taken over by an attacker who has learned an administrator-level password. Software defects that permit buffer overflow, database code injection, and cross-site scripting vulnerabilities can also cause a loss of integrity.

SOLUTIONS

- No backdoor administrative or maintenance access accounts
- Signed and encrypted firmware
- Disabling access to OS
- Fully encrypted control communication
- SRP-TLS for client-server connections
- Automatic firmware updates

Confidentiality | Keeping information private and secure

A system's confidentiality is compromised when users circumvent a system's access controls to gain unauthorized access to the data it contains. Most often, a breach in confidentiality is the result of an attacker guessing or obtaining a legitimate user's password to access the system.

SOLUTIONS

- Centralized user control through Active Directory integration and/or parent/child user sharing
- Password strength enforcement
- Ability to bulk-change camera passwords from Avigilon Control Center (ACC)
- Lock-out on multiple invalid login attempts

Availability | Ensuring system uptime and continuity of function

In addition to loss of confidentiality and integrity, the availability of a system and its data can be compromised by external attacks. These usually take the form of a denial of service (DoS) attack where an attacker bombards a system with requests. Although it is difficult to protect against all forms of these attacks, the effect is usually temporary.

SOLUTIONS

- Progressive back-off on multiple invalid login attempts
- Separate limited access gateway for thin client (web and mobile) access to video
- 802.1x device authentication

*Please note that the advice and suggestions contained in this flyer are provided for informational purposes only and should not be construed or relied upon as comprehensive or exhaustive advice on how to protect your systems from cyber vulnerabilities. Avigilon does not guarantee that any of its products are immune from a potential cyber attack and adhering to the advice and suggestions contained in this flyer may still result in your system being subject to cyber vulnerabilities or a cyber attack.

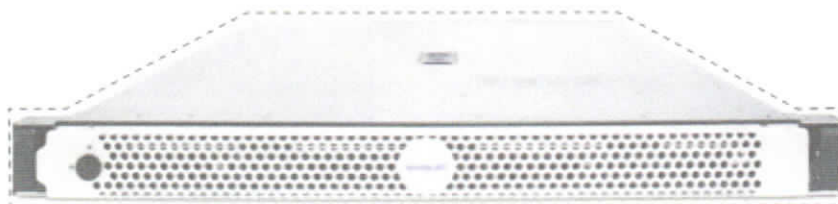
FOR MORE INFORMATION, VISIT AVIGILON.COM

avigilon

© 2017 Avigilon Corporation. All rights reserved. AVIGILON, the AVIGILON logo, AVIGILON CONTROL CENTER, and ACC are trademarks of Avigilon Corporation. Other names or logos mentioned herein may be the trademarks of their respective owners.

Avigilon Access Control Manager™ 6 Virtual

Avigilon Access Control Manager Virtual is a physical access control system (PACS) that is VMware Ready™ for deployment in a virtual server environment, eliminating the need to maintain a separate, stand-alone server or dedicated network appliance. Access Control Manager Virtual is purpose-built for organizations that have migrated their IT infrastructure to a secure, private cloud environment, allowing them to maintain enterprise-grade physical security without the risk of storing sensitive information on a shared server hosted in a public cloud.



INTEGRATED ACCESS CONTROL VIRTUAL APPLIANCE

Avigilon Access Control Manager Virtual is a web-based, access control virtual appliance that leverages open architecture, integrates identity management and video surveillance to achieve a high level of scalability with a low cost of ownership.

PHYSICAL AND LOGICAL SECURITY CONVERGENCE

Avigilon Access Control Manager Virtual allows organizations to seamlessly integrate IT and physical security systems, such as Identity and Access Governance (IAG), Security Information and Event Management (SIEM), Physical Security Information Management (PSIM) and HR systems to correlate physical and logical security event information, monitor alarms and rapidly respond to unauthorized activities.

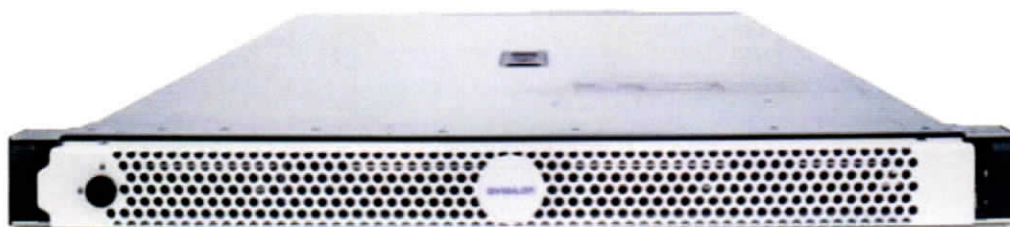
BENEFITS

- New Identity Correlation Report to track at risk identities that may have had contact with specific identities during a defined time frame.
- Video and alarm integration with the Avigilon Control Center (ACC) system
- Eliminate the cost of stand-alone servers and software
- Increase the efficiency and use of computer room resources
- Highly scalable design with decreased deployment time
- Helps reduce both capital and operational expenditures

SYSTEM RECOMMENDATIONS	VM System	VMware vSphere - v(7.0) VMware vSphere - v(6.5)
	Processor	Intel® Xeon® E3-1270 v6 3.8GHz, 8M cache, 4C/8T, Turbo
	Storage	1TB Solid State Drives
	Memory	32 GB
	Network	1 GB Ethernet Port
	Max. Controllers	512
	Card Readers	16 - 2.048
	Max. Simultaneous Operators	50
	Inputs	10120
	Outputs	10120
	Max. Identities	500,000
	Max. Stored Events	150,000,000
	Transactions (60 minutes sustained)	150,000
SUPPORTED IT PLATFORMS		Linux®
		OpenLDAP®
		VMware Ready
		SQL Server
		Oracle RDBMS
		Firefox
		Google Chrome™
		Apple Safari
		Internet Explorer
		Microsoft Edge
SUPPORTED ACCESS CONTROL SOLUTIONS		HID® VertX EVO™
		HID Global®
		HID pinCLASS®
		Mercury Security
		ASSA ABLOY
		Allegion
		Farpointe Data®
		EasyLobby® by HID
		LifeSafety Power®
		VIRDI
		Simons Voss
SUPPORTED VIDEO INTEGRATION SOLUTIONS		Autipon Control Center™
		Esacq Technologies by Tyco Security
		Milestone Systems
ORDERING INFORMATION	AC-SW-16R-VM-6-P	Access Control Virtual Appliance with 16 Readers
	AC-SW-32R-VM-6-P	Access Control Virtual Appliance with 32 Readers
	AC-SW-64R-VM-6-P	Access Control Virtual Appliance with 64 Readers
	AC-SW-128R-VM-6-P	Access Control Virtual Appliance with 128 Readers
	AC-SW-256R-VM-6-P	Access Control Virtual Appliance with 256 Readers
	AC-SW-512R-VM-6-P	Access Control Virtual Appliance with 512 Readers
	AC-SW-1024R-VM-6-P	Access Control Virtual Appliance with 1024 Readers
	AC-SW-2048R-VM-6-P	Access Control Virtual Appliance with 2048 Readers
	AC-SW-16RCU-6-P	16 Reader software add-on

Avigilon Access Control Manager™ 6 Enterprise and Enterprise Plus Systems

The Access Control Manager (ACM) system is an IT-friendly Physical Access Control System (PACS) from Avigilon for enterprise-class installations. It's a complete access solution that is designed to keep your focus on securing your people, property and assets, and maximizing your time by helping you respond immediately to alerts wherever you are. The ACM™ system is a browser-based solution that can integrate with existing IT/HR systems, minimizing the need for duplicate data entry. It comes with a full set of standard features that not only help to maximize your time, but will reliably safeguard your information.



INTEGRATED ACCESS CONTROL NETWORK APPLIANCE

Avigilon's Access Control Manager Enterprise and Enterprise Plus systems are integrated access control network appliances that leverage an open architecture, integrate identity management and video surveillance and achieve a high level of scalability with a low cost of ownership by eliminating the need to maintain a stand-alone server or install software on multiple machines.

BENEFITS

- New Identity Correlation Report to track at risk identities that may have had contact with specific identities during a defined time frame.
- Powerful 1U rack mount chassis with pre-installed software from Avigilon
- Scalable from one access door to thousands of doors per Enterprise appliance
- Automatically synchronizes security data across all Enterprise/Enterprise Plus appliances in real-time
- Auto-failover capability enables seamless redundancy to keep critical security data safe
- Leverages open field hardware investments

ENTERPRISE PLUS BENEFITS

- Provides up to 1.3 TB of effective storage capacity in a RAID 5 solid state drive configuration
- Offers 32GB of expanded memory for faster delivery of information in high demand environments
- Delivers high availability with redundant 350W power supplies
- Hot-swappable components enable uninterrupted operation of the system even if the power supply and solid state drive (SSD) need replacement.

		ENTERPRISE		ENTERPRISE PLUS			
SYSTEM	Card Readers	16 - 400		256 - 2048			
	Inputs	5,060		10,120			
	Outputs	5,060		10,120			
	Hard Disk Drive Configuration	1TB 72K RPM SATA 6Gbps 3.5in Cabled Hard Drive		4 x 480GB Solid State Drives, RAID5, 1.3TB effective storage			
	Processor	Intel® Xeon® E-2124 3.3GHz, 8M cache, 4C/4T, turbo (7W)		Intel Xeon E3-1270 v6 3.8GHz, 8M cache, 4C/8T, Turbo (72W)			
	Memory	1-8GB 2666MT/s DDR4 ECC UDIMM		32 GB (2 x 16GB), 2400MT/s DDR4 DIMMs, UDIMMs			
	Network Adapter Card	2 x 10/100/1000 Mbps Network Interface Controller (NIC) ports		2 x 10/100/1000 Mbps NIC ports			
	Remote Management	iDRAC9 Basic		iDRAC 9 Enterprise			
	Max. Controllers	512		512			
	Max. Simultaneous Operators	20		50			
Max. Identities	250,000		500,000				
Transactions (60 minutes sustained)	50,000		150,000				
Max. Stored Events	150,000,000		150,000,000				
MECHANICAL	Form Factor	1U rack-mount chassis		1U rack-mount chassis			
	Dimensions (HxWxD)	42.8 mm x 482.4 mm x 676.92 mm; 1.68" x 18.99" x 26.65"		42.8 mm x 482.4 mm x 677.3 mm; 1.68" x 18.99" x 26.66"			
	Weight	8.77 kg (19.32 lbs)		13.4 kg (29.54lb)			
	Cable Management	1U/2U Static Rails for 2-Post and 4-Post Racks		Dedicated ReadyRails Sliding Rails With Cable Management Arm			
ELECTRICAL	Power Input	90 to 264 VAC, 47-63 Hz		90 to 264 VAC, 47-63 Hz			
	Power Supply	Single non-redundant		Power supply redundancy: dual 350W Hot Plug			
	Power Consumption	250 W		350W			
ENVIRONMENTAL	Operating Temperature	10° C to 35° C (50° F to 95° F)					
	Storage Temperature	-40° C to 65° C (-40° F to 149° F)					
	Operating Humidity	10 - 80% Relative humidity (non-condensing)					
	Storage Humidity	5 - 95% Relative humidity (non-condensing)					
	Operating Vibration	0.26G _{rms} at 5-350Hz for 15 minutes					
	Storage Vibration	1.88G _{rms} at 10-500Hz for 15 minutes					
	Operating Shock	Six consecutively executed shock pulses in the positive and negative x, y, and z axis of 6 G for up to 11 ms.					
	Storage Shock	Six consecutively executed shock pulses in the positive and negative x, y, and z axis (one pulse on each side of the system) of 71 G for up to 2 ms.					
	Operating Altitude	-15.2 m (-50 ft) to 3048 m (10,000 ft)					
Storage Altitude	-15.2 m (-50 ft) to 12,000 m (39,370 ft)						
CERTIFICATIONS	ACMA/C-Tick	BELLIS	BSMI	CE	CNCA/CCC	EAC	
	FCC	ICES	IECEE CB	INSM	KCC	KEBS	
	KSA/CCP	KUCAS	KVALITET	NEMKO	NRCS	NRTL	
	NYCE/NOM	OTAN-CKT	SABS	SCC	SIR	SONCAP	
	STZ	TUV	UKRTEST/UKRSERT/COMPUTER		VCCI		
SUPPORTED IT PLATFORMS	Linux®	Google Chrome™	SUPPORTED ACCESS CONTROL SOLUTIONS	HID® VeriX EVO™	Mercury Security	SUPPORTED VIDEO INTEGRATION SOLUTIONS	Avigilon Control Center™
	OpenLDAP®	Apple Safari		HID Global®	VRDI		Esacq Technologies by Tyco Security
	VMware Ready™	Internet Explorer		HID pivCLASS®	Elmdene		Milestone Systems
	Firefox	Microsoft Edge		ASSA ABLOY	Siemens/Voxa		
				Alegion	EasyLobby® by HID		
				Fingerprint®	LifeSafety Power		
ORDERING INFORMATION	AC-APP-16R-ENT2-6		Access Control Enterprise Appliance with 16 readers (can be upgraded to 400 readers)				
	AC-APP-32R-ENT2-6		Access Control Enterprise Appliance with 32 readers (can be upgraded to 400 readers)				
	AC-APP-64R-ENT2-6		Access Control Enterprise Appliance with 64 readers (can be upgraded to 400 readers)				
	AC-APP-128R-ENT2-6		Access Control Enterprise Appliance with 128 readers (can be upgraded to 400 readers)				
	AC-APP-256R-ENT2-6		Access Control Enterprise Appliance with 256 readers (can be upgraded to 400 readers)				
	AC-APP-ENT2-WARR-EXTEND-1YR		1 Year Extended Warranty for Access Control Manager Enterprise Appliance				
	AC-APP-ENT2-WARR-EXTEND-2YR		2 Year Extended Warranty for Access Control Manager Enterprise Appliance				
	AC-APP-16R-ENT-Plus-6		Access Control Enterprise Plus Appliance with 16 readers (can be upgraded to 2048 readers)				
	AC-APP-256R-ENT-Plus-6		Access Control Enterprise Plus Appliance with 256 readers (can be upgraded to 2048 readers)				
	AC-APP-512R-ENT-Plus-6		Access Control Enterprise Plus Appliance with 512 readers (can be upgraded to 2048 readers)				
	AC-APP-1024R-ENT-Plus-6		Access Control Enterprise Plus Appliance with 1024 readers (can be upgraded to 2048 readers)				
	AC-APP-2048R-ENT-Plus-6		Access Control Enterprise Plus Appliance with 2048 readers				
	AC-APP-ENT-PLUS-WARR-EXTEND-1YR		1 Year Extended Warranty for Access Control Manager Enterprise Plus Appliance				
	AC-APP-ENT-PLUS-WARR-EXTEND-2YR		2 Year Extended Warranty for Access Control Manager Enterprise Plus Appliance				