PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0034 April 2023

Optimization of Airport Security Camera Systems

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Ryan Hagan, PSP
René Rieder Jr, PSP, CPP, ASC
Burns Engineering
Philadelphia, PA

NOTICE

The project that is the subject of this report was a part of the Program for Applied Research in Airport Security (PARAS), managed by Safe Skies and funded by the FAA.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by Safe Skies.

The opinions and conclusions expressed or implied in this report are those of the individuals or organizations who performed the research and are not necessarily those of Safe Skies or the FAA.

Safe Skies and the FAA do not endorse products or manufacturers.

NATIONAL SAFE SKIES ALLIANCE, INC.

National Safe Skies Alliance (Safe Skies) is a non-profit organization that works with airports, government, and industry to maintain a safe and effective aviation security system. Safe Skies' core services focus on helping airport operators make informed decisions about their perimeter and access control security.

Through the ASSIST (Airport Security Systems Integrated Support Testing) Program, Safe Skies conducts independent, impartial evaluations of security equipment, systems, and processes at airports throughout the nation. Individual airports use the results to make informed decisions when deploying security technologies and procedures.

Through the POST (Performance and Operational System Testing) Program, Safe Skies conducts long-term evaluations of airport-owned equipment to track and document a device or system's performance continuously over its life cycle.

Through PARAS (Program for Applied Research in Airport Security), Safe Skies provides a forum for addressing security problems identified by the aviation industry.

A Board of Directors and an Oversight Committee oversee Safe Skies' policies and activities. The Board of Directors focuses on organizational structure and corporate development; the Oversight Committee approves PARAS projects and sets ASSIST Program priorities.

Funding for our programs is provided by the Federal Aviation Administration.

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

The Program for Applied Research in Airport Security (PARAS) is an industry-driven program that develops near-term practical solutions to security problems faced by airport operators. PARAS is managed by Safe Skies, funded by the Federal Aviation Administration, and modeled after the Airport Cooperative Research Program of the Transportation Research Board.

Problem Statements, which are descriptions of security problems or questions for which airports need guidance, form the basis of PARAS projects. Submitted Problem Statements are reviewed once yearly by the Safe Skies Oversight Committee but can be submitted at any time.

A project panel is formed for each funded problem statement. Project panel members are selected by Safe Skies, and generally consist of airport professionals, industry consultants, technology providers, and members of academia—all with knowledge and experience specific to the project topic. The project panel develops a request of proposals based on the Problem Statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables.

The results of PARAS projects are available to the industry at no charge. All deliverables are electronic, and most can be accessed directly at www.sskies.org/paras.

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies PARAS Program Manager*

PARAS 0034 PROJECT PANEL

Christopher Campbell *National Safe Skies Alliance*

Stephanie Lane *Dallas Fort Worth International Airport*

Sean Florio *Lee County Port Authority*

Michael Pilgrim *International Security Concepts*

Christian Samlaska *Convergint*

Sheeba Varughese *Los Angeles World Airports*

AUTHOR ACKNOWLEDGMENTS

BURNS ENGINEERING

- Ryan Hagan, PSP, Principal Security Specialist
- René Rieder Jr, PSP, CPP, ASC, Aviation Security Lead
- Reiko Nunley, PSP, CPP Senior Engineering Specialist
- Suzanne Guzik, Senior Systems Engineering Specialist
- Joseph Keith, Principal Security Specialist
- Danielle Tabachnick, AIA, PMP, LEED AP, Senior Security Specialist

CONTENTS

TABLES & FIGURES

PARAS ACRONYMS

ACRP	Airport Cooperative Research Program
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue & Firefighting
CCTV	Closed Circuit Television
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
IED	Improvised Explosive Device
IT	Information Technology
MOU	Memorandum of Understanding
RFP	Request for Proposals
ROI	Return on Investment
SIDA	Security Identification Display Area
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

AI	Artificial Intelligence
ASP	Airport Security Program
BSI	British Standards Institute
CBP	Customs and Border Protection
DVR	Digital Video Recorder
IP	Internet Protocol
LAN	Local Area Network
NAS	Network Array Storage
NDAA	National Defense Authorization Act
NVR	Network Video Recorder
POE	Power Over Ethernet
PTZ	Pan-Tilt-Zoom
PVC	Polyvinyl Chloride
SVA	Security Vulnerability Assessment
UPS	Uninterruptible Power Supply
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VMS	Video Management System
VSS	Video Surveillance System

SECTION 1: INTRODUCTION

Security system requirements and recommendations for airports are constantly evolving due to dynamic threats to facilities, staff, passengers, and operations, as well as improvements in technology. Camera systems are powerful tools in a security operations program. They provide the capability to visually monitor areas of an airport remotely in real time, record events for forensic purposes, detect and deter unauthorized activity, and minimize resources needed for incident response.

Due in part to Moore's Law,[1] video camera system manufacturers have been able to double the processing power of cameras roughly every two years, providing new models and features with each iteration. As technologies advance and industry security protocols change, it is important that airports periodically review their camera and video systems for opportunities to enhance system performance and operating costs. The purpose of this document is to provide guidance to help airports refine and/or develop their video camera program and program goals; review the use of their existing camera and recording technology; make well-informed decisions when optimizing, expanding, upgrading, or replacing their video camera system; and ensure continued effectiveness and efficiency of these systems.

As every airport and camera system is unique, there is no single right way for decision making, nor is there a single best system approach. Each airport operator must make their own assessment, determine what their camera program needs to accomplish, and find their optimum individual solution. This document serves to guide the user through key considerations in the process and provides a roadmap for optimizing the current camera system or moving towards future expansion, upgrade, or replacement. PARAS 0028 – *Recommended Security Guidelines for Airport Planning, Design, and Construction*[2] provides guidance on the design of new camera systems and should be reviewed in tandem with this document, along with any available current security programs, design criteria and planning documents.

For clarity and to mitigate misinterpretation, the term *camera system* is inclusive of cameras and all components used to monitor, transmit, record, store, retrieve, and manage video footage from cameras that are deployed throughout an airport campus. Components typically include the cameras, digital video recorders (DVR) or network video recorders (NVR), cloud-based storage, network infrastructure, and video management systems (VMS).

The term *surveillance* will be used to describe the purpose of the camera system as opposed to the camera system being used to surveil. This document will not address the policies or regulatory restrictions as to what, who, and where cameras can be positioned within the airport environment.

While this document focuses on facilities' existing camera systems, many topics and concepts herein may also be applicable to airports that are planning a new camera system.

1.1 Document Organization

A brief description of the document structure and what is contained within each section is provided below. The target audience for each section has not been specifically identified, as this document is

[1] "Moore's Law is the observation that the number of transistors in an integrated circuit doubles about every two years." (https://en.wikipedia.org/wiki/Moore%27s_law)

[2] **PARAS 0028:** https://www.sskies.org/images/uploads/subpage/PARAS_0028.Recommended_Security_Guidelines_.FinalReport_.pdf

intended to provide an overarching guide and approach to video system optimization for owners, architects, engineers, and contractors.

Section 1 introduces the document and discusses applicability, intent, and changing industry security concerns and their impacts on video camera systems.

Section 2 focuses on the planning and video camera program development and review process. It includes discussion on stakeholder collaboration, needs assessments, regulatory considerations, and benefit-cost analysis.

Section 3 addresses the considerations involved in deciding whether to upgrade, optimize, or replace the current system. It also discusses the recommended project phases and methodology to ensure a successful project outcome.

Section 4 addresses the system design process, including the technology, infrastructure, and supporting systems that should be considered.

Section 5 focuses on implementation, including project design, vendor selection, system installation, testing, training, owner acceptance, operation, and life cycle management.

1.2 Changing Security Concerns and Contingency Measures

Security threats constantly evolve based on the criticality of an asset, its value, and the perceived impact in stealing, damaging, or destroying the asset at any given time. As such, monitoring of assets also needs to change over time to meet requirements that may not have been in place previously and due to improvements in detection technologies since the monitoring system was deployed. Review of the existing security program or provisions is paramount in determining the level of upgrade needed to effectively monitor assets based on the current degree of security threat and possible future threats.

An inoperable video camera system can result in contingency measures such as safeguards. However, these measures can be unnecessary if the protected asset’s liability, value, or criticality has diminished or been eliminated over time. The security program should also outline contingency measures to ensure proper coverage of assets that have been identified for increase in their current security level.

SECTION 2: PLANNING

The key to an effective and efficient camera system is maintaining a program to routinely review the system's functionality, operating costs, maintenance, and performance in meeting the security program requirements. Planning is always the first stage in developing and maintaining an adequate video camera system. Key phases in camera system planning include:

- Video Camera System Program Review
- Needs Assessment / Security Vulnerability Assessment (SVA)
- Airport Stakeholder Collaboration and Communication
- Regulatory Review
- Benefit-Cost Analysis

2.1 Video Camera System Program

Video camera systems can be complex, but are fairly easy to operate once they are installed and staff are trained on how to utilize the system. However without a defined program, the system's use can be inefficient or may not meet the airport's security objectives.

2.1.1 Program Development

A video surveillance program should document the methodologies utilized to define the needs and requirements of the surveillance system and how it aligns with the airport objectives. Development of the video surveillance program should be led by an empowered and experienced member of airport leadership, typically a Director of Security.

The following sections outline the recommended steps to be completed in order to develop the video surveillance program.

STEP 1: DEFINE THE METHODOLOGY

A video surveillance system is a powerful tool in the overall airport security program, but it also presents a potential risk to the privacy of individuals whose personal information may be collected, used, and disclosed as a result of the surveillance system. While there is no expectation of privacy in public locations, this could be raised as a concern if there is not a defined program to identify the needs for each surveillance coverage zone.

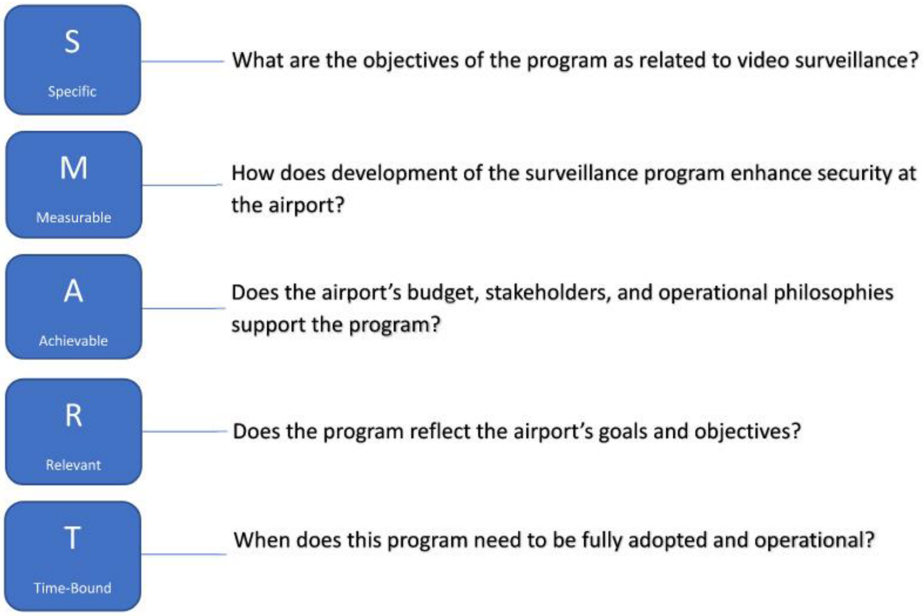
A defined methodology should be utilized to establish the camera requirements. The goal of the methodology is to ensure a consistent level of surveillance aligned with a specific intent and/or risk mitigation requirement. Potential resources and methodologies to define the video surveillance requirements may include:

- Security Vulnerability Assessment
- Airport Risk Management Department Standards
- SMART Airport program[3]
- Regulatory compliance

[3] The SMART Airport program is the utilization of digital technologies to improve the operations of the airport, passenger experience, and/or existing system operations based on collected data. For the purposes of this document, the SMART program is the utilization of surveillance cameras to provide data points for the automation of processes.

Based on the outcome and analysis of these tasks and resources, the foundation of the video surveillance program can be developed. The foundation should have clear, defined, and accessible results. Using SMART (Specific, Measurable, Achievable, Relevant, and Time-Bound) criteria, as shown in Figure 2-1, is a realistic approach to defining and developing a surveillance program.

Figure 2-1. SMART Criteria Model



S Specific — What are the objectives of the program as related to video surveillance?

M Measurable — How does development of the surveillance program enhance security at the airport?

A Achievable — Does the airport's budget, stakeholders, and operational philosophies support the program?

R Relevant — Does the program reflect the airport's goals and objectives?

T Time-Bound — When does this program need to be fully adopted and operational?

When establishing the foundation, the following questions should be considered:

1. Is there an alternative solution to meet the video surveillance requirements (i.e., additional security staffing, different security technology, etc.)?
2. Is there a business reason for utilizing video surveillance?
3. Is there a policy on the use of video surveillance, including users of the system?
4. Is there a requirement, law, or local mandate that requires the airport to inform the public that video surveillance is taking place?
5. Are recorded images stored in a secure location, with limited access, and destroyed when no longer required for business purposes?
6. Can the airport define who will view and have access to the live and stored video and why, what information is being captured, and how the recorded images will be used?

While this establishes the foundation of the video surveillance program, it does not define the technical specifications of the video surveillance program.

STEP 2: TRANSLATE INTO A DESIGN

In Step 2, the foundation that documents the intent of the surveillance program is converted into technical criteria/specifications that can be utilized for the procurement of the video surveillance equipment. For existing system expansions, this may be limited to selecting cameras to meet the requirements of the surveillance program. This is also an opportunity to look at newer technologies that can enhance the security posture of the airport. For new systems, the selection of the VMS should be considered first to ensure that it will meet all the performance requirements identified in the program. This may be accomplished through visiting airports where the solution is installed, inviting manufacturers to a Technology Day at the airport to present their platforms, or researching solutions with an independent consultant. Once the VMS is selected, camera technologies that are supported by the VMS platform should then be selected.

The selected solutions can then be procured through the airport's approved purchasing methods.

Security departments without an established Security Design Criteria/Performance Requirements Document have greater struggles justifying replacing, adding, and upgrading cameras. A Security Design Criteria document establishes the minimum needs of the airport security department and therefore justifications to replace cameras that are not performing or providing the required views or quality of view.

STEP 3: VERIFY AND VALIDATE

Upon completion of installation, testing, and acceptance of the video surveillance equipment, the final step is to compare the installed system with the original foundation developed in the first step to verify that the system is meeting the goals and intent of the program.

This step is intended to be a living process, meaning that when there are changes in the airport environment (e.g., construction, new threats, change in airline tenants), the video surveillance system should be reviewed and actions implemented as necessary to modify the existing system to ensure compliance with the original surveillance program.

2.1.2 Program Review

When developing a Video Camera System Program Review, there are three primary factors to consider: frequency, criteria, and team.

FREQUENCY

The frequency that the system is reviewed for optimization or improvement needs is an important consideration. Reviewing a system too frequently taxes resources and funding. Reviewing a system too infrequently can result in inefficiency in operation and costs, or may allow a system to age too far for cost-effective changes. The industry standard frequency for reviewing video systems is two to four years, unless there are special circumstances such as changes in regulatory requirements, failure of the current system components, or renovation or construction projects that impact the system's function.

CRITERIA

The system review should cover several areas to ensure all aspects are thoroughly accounted for and evaluated for effectiveness, efficiency, and operational requirements. Below are some key examples of a review:

Operations

- Issues of Concern: Discuss and annotate any issues that have been or are currently adversely affecting security monitoring operations. Examples include cameras being intermittently inoperable, or an event such as a virus in the VMS that has diminished the system's effectiveness.
- Need for Monitoring: Discuss whether the cameras meets the requirements for surveillance of their respective areas. A resource that is temporarily located would not typically meet prerequisites for 24/7 video camera monitoring, and alternate options for monitoring should be considered.

- Budgetary Constraints: Discuss whether the budget accommodates changes to the video camera system or if critical system requirements may necessitate changes to the budget.
- Operational Change: Discuss where there has been an operational change in the need for monitoring a location or asset that will require changes to the system.
- Construction: Airports are typically in a constant state of construction, whether a major capital program like a terminal modernization program or a relatively minor project like upgrading signage. Construction projects may impact operational camera views, either temporarily during construction or permanently because of the end result of construction. In either case, the camera system should be reviewed for impacts.

Technology

- Camera Quality: When an airport relies on cameras for security, a camera that cannot provide the expected level of surveillance due to poor resolution, frame rate, lighting sensitivities, etc. can be a liability.
- Environmental Factors: This is particularly important for exterior cameras, since a camera may need to be cooled or heated depending on the installation conditions. Issues such as water droplets appearing on a camera view may be the result of condensation within a camera dome or a failed gasket.
- IT Infrastructure: A security camera system is only as good as the supporting network infrastructure. Therefore, any changes to the IT topology can have broad effects on network systems, including the VMS. Changes in network equipment (switches, patch panels, fiber type, etc.) that can affect the camera system are often overlooked in system reviews.
- Data Planning: As camera resolutions increase, the cameras require more bandwidth to operate. It may be necessary to migrate from the Local Area Network (LAN) to a dedicated security Virtual Local Area Network (VLAN). A VLAN provides better control and network throughput to support the intensive needs of a camera system.

Crime Prevention Through Environmental Design Considerations

- A key consideration for a camera system revision is natural surveillance of the area being considered for additional monitoring. An area may be less susceptible to crime when there is suspected camera surveillance of the area.
- Passengers, airport workers, and passers-by should feel a sense of being monitored in and around the airport. Terminals and support facilities will often have visibly apparent cameras to support the appearance of monitoring. However, airports also deploy cameras in obscure locations (i.e., vaulted ceilings or in rafters) for aesthetics of the airport environment. Architectural conditions will also influence the location of security cameras, as mounting may be limited to specific locations feasible for installation.

TEAM

The team reviewing the video camera system should include individuals who are likely to understand the needs of the system and provide appropriate feedback on security program requirements. Typical participants include the Airport Manager, Security Manager, IT Manager, select user group and stakeholder members, and a risk management officer.

2.2 Airport Stakeholder Communication and Collaboration

The inclusion of key stakeholders is integral to the success of a video camera review, upgrade, or replacement project. Continuous communication with stakeholders helps identify and understand their needs, address issues as they arise, and manage possible conflicting interests.

Camera projects should include input from all potential stakeholders to optimize camera placement and technology selection for the greatest number of applications. Cameras can be used to monitor quality of service (queue monitoring), perform remote system diagnostics such as to address faults/error messages (baggage handling systems), manage ramp operations (aircraft movements, baggage handlers, aircraft service vehicles), and, recently, to detect compliance with COVID masking requirements.

Camera sharing involves communication and collaboration between different stakeholders and airport entities on a regular basis. The process for requesting and sharing views between different stakeholders should be mutually agreed upon and documented. If different networks and systems are involved, cybersecurity concerns will also need to be addressed.

A list of key stakeholders should be maintained as a part of any project or system evaluation. Because management, personnel, or tenant groups may change over the course of a security camera system review and subsequent projects, identifying stakeholders is not a one-time process—it should be considered throughout the project life cycle.

Potential stakeholders include, but are not limited to:

- Security
- Operations
- Customs and Border Protection (CBP; where applicable)
- IT
- Tenant Relations
- Current Security Contractor
- Risk Management
- TSA
- First Responder(s)

A Stakeholder Review Board should be developed to include key stakeholders such as Directors of Security, Risk Management, and IT, among others. The Board should be empowered to make security decisions on behalf of the airport, including the approval of system changes, system expansions, and capital investments.

Engaging and re-engaging stakeholders throughout the project obtains and confirms stakeholder commitment. Stakeholders must understand that their input, or lack thereof, shapes a project or evaluation. Contributing to the discussion of security camera system evaluation allows stakeholders to address concerns and provide criteria they want addressed. By not actively participating in this process, stakeholders forfeit their input in a project.

2.2.1 Memoranda of Agreement

Existing Memoranda of Agreement between the airport and respective agencies (TSA, CBP, tenants, etc) should be evaluated in advance of any modifications to the camera system to ensure the existing agreements are maintained both during upgrades and in final conditions.

2.3 Needs Assessment

Camera systems, once installed and functional, should not be viewed as a static system. Planning for a camera system's periodic review, upgrade, or end-of-life replacement should be part of any facility's overall security program to monitor and maintain the effectiveness of a camera system's contribution to airport security. A needs assessment of an existing video camera system is necessary to determine where there are gaps and vulnerabilities associated with the current technology, and what is needed to enhance security monitoring and detection. This assessment should also consider future growth and expansion of the video camera system. The assessment should focus on meeting operational needs as opposed to upgrading a system for the sake of newer technology. It is not advisable to chase technology unless the result is increased security and immediate return on investment.

A needs assessment for a video camera system should address the following factors:

- Existing system/equipment, including cameras, servers, workstations, etc.
- Capacity and type of the existing infrastructure (e.g., coaxial cable, fiber optic cable, network cable, wireless)
- Quality of the existing equipment and infrastructure (e.g., Are devices failing? Is the cabling protected? Are the connectors at the camera or telecommunication closet secure?)
- How the system is being used (e.g., the system's functional requirements)
- How the system could be used in the future (e.g., people counting, direction of travel detection, object detection/removal)
- Whether optimization changes are required or if the system is acceptable as-is
- Whether other stakeholders can take advantage of a camera field of view

A needs assessment should also consider existing camera program documentation, master planning requirements, system design standards, and other planned projects.

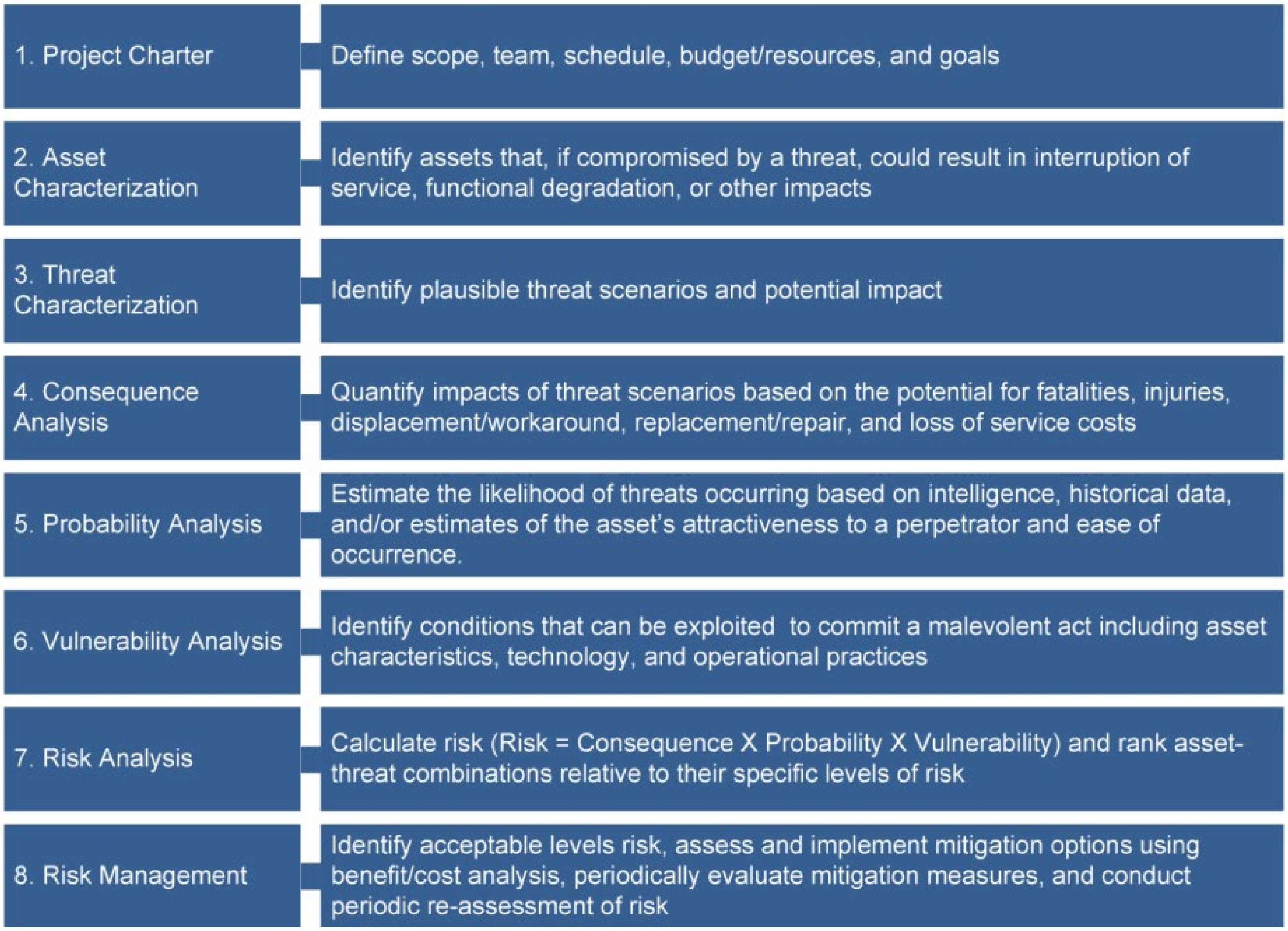
It is also imperative to understand the layout and capabilities of the existing security camera system to verify if existing resource locations still need monitoring (e.g., resource being relocated, change in traffic flow patterns, change in risk factors of the resource). As renovations and improvements within the airport take place, assets should be re-evaluated for their coverage needs and requirements.

2.3.1 Security Vulnerability Assessment

In conjunction with a needs assessment, the execution of an SVA can help assess the camera system's value at key locations. The scope of the needs assessment will determine the depth and extent of an SVA. The results of this, in concert with the Stakeholder Review Board recommendations, will establish whether to upgrade, optimize, expand or replace an existing camera system.

Figure 2-1 details the eight steps recommended for performing an airport SVA. In understanding the risk of not upgrading, a risk evaluation must be performed so that it can be managed at an acceptable level.

Figure 2-2. 8-Step Process for Completing an Airport SVA



1. Project Charter	Define scope, team, schedule, budget/resources, and goals
2. Asset Characterization	Identify assets that, if compromised by a threat, could result in interruption of service, functional degradation, or other impacts
3. Threat Characterization	Identify plausible threat scenarios and potential impact
4. Consequence Analysis	Quantify impacts of threat scenarios based on the potential for fatalities, injuries, displacement/workaround, replacement/repair, and loss of service costs
5. Probability Analysis	Estimate the likelihood of threats occurring based on intelligence, historical data, and/or estimates of the asset's attractiveness to a perpetrator and ease of occurrence.
6. Vulnerability Analysis	Identify conditions that can be exploited to commit a malevolent act including asset characteristics, technology, and operational practices
7. Risk Analysis	Calculate risk (Risk = Consequence X Probability X Vulnerability) and rank asset-threat combinations relative to their specific levels of risk
8. Risk Management	Identify acceptable levels risk, assess and implement mitigation options using benefit/cost analysis, periodically evaluate mitigation measures, and conduct periodic re-assessment of risk

Source: PARAS 0016

A large part of the SVA focuses on vulnerability and risk. These need to be understood when considering not upgrading a system, as this could lead to the loss of forensic data that is essential in the review of airport operations, events in the terminal, or injury that would require stakeholder or emergency services involvement. Stakeholders will need to evaluate risk factors to ensure that the threshold of acceptable risk is not surpassed by not upgrading or replacing a system.

2.3.2 Existing Cameras

Cameras can malfunction or perform poorly for various reasons. During review of the video surveillance system, any inoperable cameras should go through a troubleshooting process to determine if the issue is with the camera, the infrastructure to/from the camera, peripheral component malfunction, software incompatibility, or end of serviceability. Troubleshooting possibilities may include:

- **Ensuring the camera license is still valid –** Camera licensing is often overlooked when troubleshooting image problems. Although the manufacturer or installer should notify the owner that a license is about to expire or has expired, sometimes camera license renewal sometimes falls through the cracks. The installer should be responsible for maintaining licensing if there is a warranty or service-level agreement in place.
- **Ensuring the VMS and/or camera firmware is up to date –** VMS firmware updates typically come from the manufacturer and can be automatically downloaded and updated to the server.

However, this is not the case with all VMS manufacturers, and in some cases, the license status may affect firmware updates.

- **Ensuring the integrity of the connecting cable has not been compromised** – Some types of cable connections on a camera can become loose. A loose connection could cause inconsistency in the data transmission, resulting in image loss.

2.3.3 Existing Infrastructure

The current infrastructure for the existing system should be assessed to determine its further usability. Supporting components and infrastructure often have a shelf life that is dependent on their date of installation and age. At a minimum, the review should include the following:

Coaxial cables – Because these cables are often thicker and stronger than Ethernet cables, they will typically surpass the usefulness of Ethernet cables. However, coaxial cable is not as efficient because of its relatively low digital resolution capabilities. Internet Protocol (IP) data and power can be transmitted over coaxial cable by using encoders, but this is not recommended as it presents more points of failure. Existing coaxial cable is often degraded and has splice points that attenuate or completely disrupt the signal, making it useless.

Ethernet cables and connectors – Ethernet cable coating can become rigid and brittle with age, and can be the source of distorted images. Although the wiring inside will long outlast the coating, exposed wire due to frayed or cut coating will eventually diminish its manufacturer-specified capabilities. In addition, the material composition of the plastic connectors (RJ-45) makes them susceptible to deterioration over time. Ethernet cables can be tested to ensure compliance with industry-recognized standards established by ANSI/TIA.[4]

Fiber optic cables and connectors – Fiber is typically used as backbone cable (cable used as the primary network pathway), but it can also be used to transmit video data from camera locations at extended distances. When used in this application, the cables are susceptible to being nicked or broken if not protected. Small nicks in the sheathing can create distortion issues and, in extreme cases, total loss of signal. If proposing to reuse fiber optic cable, the cables should be tested by a specialist.

Media converters – While it is a required component for a multimedia pathway, a media converter can pose a single point of failure and present challenges to camera signals when it is not properly installed or maintained, such as by providing inadequate environmental protections or providing improper power to the converter. Media converters are not smart devices, so they do not report to a central headend when they malfunction or fail, and as such they are often overlooked during troubleshooting of video signal problems.

Power over Ethernet (POE) switches – The POE distribution switch is an essential device in providing power and data to video cameras. Although it is long lasting and reliable, a POE switch is not invulnerable to failure over time and does not die suddenly. Small glitches in video transmission or power supplied to the cameras should be investigated starting with the switch. A switch that is installed in harsh conditions (e.g., overheated telecom room, dusty environment, no ventilation) can cause the slow death of a switch, which will eventually lead to loss in camera coverage or even a partial or entire network system.

[4] **ANSI/TIA-568** (for purchase): https://global.ihs.com/doc_detail.cfm?&csf=TIA&item_s_key=00378460&item_key_date=790906&input_doc_number=568&input_doc_title=&org_code=TIA

Cable trays/J-hooks – Cable tray/J-hook cable management systems can be composed of various materials ranging from plastic to metal. Over time, these cable management devices can be weakened by age and the weight of system cables, making them susceptible to sagging, disfigurement, or breakage.

Conduit – Existing conduit is seldom replaced when reusing its pathway. Fill ratios calculated at planning and construction phases determine the future usability of the conduit when additional network devices may need to use the same conduit. Rigid steel conduit is essentially impervious to damage, failure, or vandalism, so the same conduit can be used for many years before another cable conveyance is necessary.

However, conduit can pose its own challenges when attempting to evaluate for future use or to troubleshoot a camera issue. Cable issues within the conduit are hidden as the cable ages within the conduit, and are invisible until the cable is otherwise replaced. It can be a frustrating and time-consuming process to find the source of a camera issue if there are multiple cables within the conduit and the cables pass testing. Evaluating the current fill ratio of the conduit will determine its usefulness to the project and if it is worth replacement, reuse, or repulling cable, which can affect the project budget.

2.3.4 Existing Video Management System

The functionality of an existing VMS is contingent on whether the system is meeting the needs of the airport and has the capacity to continue to meet those needs in the future.

This system is indirectly evaluated daily by the end users. However, formal evaluation of the VMS should also be part of the needs assessment. How the system is used currently will determine if either the full capabilities of the existing VMS are being used or if the system is unable to meet current requirements.

If the VMS cannot be updated to support new technology, replacement of the VMS may be required. However, replacement may introduce additional costs beyond just software replacement. For example, camera technology may require updated firmware to be integrated with the new VMS.

2.3.5 Existing Lighting

Lighting is essential to any security camera system. The existing lighting conditions during both daytime and nighttime should be assessed at each camera location. Lighting includes artificial sources as well as natural lighting.

Lighting deficiencies can surface when new cameras or camera types are introduced. Knowing the existing camera capabilities will help determine if the potential new cameras will meet the operational viewing requirements under the existing lighting conditions.

2.3.6 Regulatory Review

The framework for any airport video program or project should include review of federal regulations, airport security standards, and local codes regarding use of video camera technology within an airport environment. This review should encompass, at a minimum, DHS, FAA, and CBP standards to ensure that the video camera system upgrade or expansion does not interfere with other operational entities' ability to interface with the system.

Project teams managing system upgrades, optimization, expansions, or replacement should consider and be familiar with the requirements of 49 CFR §§ 1540 and 1542 regarding airport security operations. As revisions to an existing security system may have residual effects on other related airport systems, it is also essential to coordinate with other contiguous agencies or departments.

The following documents also identify requirements and guidelines for cameras in specific areas of the airport:[5]

- CBP Airport Technical Design Standards
- TSA Checkpoint Requirements and Planning Guide
- TSA Planned Guidelines and Design Standards for Checked Baggage Inspection System

2.3.6.1 National Defense Authorization Act

The John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA)[6] prohibits the use of federal funds to procure or use certain "covered" telecommunications and video surveillance equipment and services. This includes telecommunications equipment from Huawei Technologies Company or ZTE Corporation (or their subsidiaries or affiliates), and video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Company, or Dahua Technology Company (or their subsidiaries or affiliates). This act also provides for a phase-out of currently installed "covered" components when camera system projects are being planned.

To comply with the act, government-funded agencies, such as airports, should ensure that no components being used in a current project are procured from the restricted/banned countries or manufacturers. This pertains to cameras and components within a camera, NVRs/DVRs, or any security devices connected to a network. It is ultimately the airport operator's responsibility to make sure these components are not included in the implementation of any upgrades or new systems.

Consultants, designers, and engineers working for any government-funded entity should be aware of this act to ensure banned products do not make it into a design.

2.4 Benefit-Cost Analysis

In addition to simply *what* can help a video camera system improve, it is critical to understand what can be afforded for the maximum benefit. Options can be developed to compare good, better, and best plans of action to calculate the best benefit/cost for the work to be done. This evaluation must be completed with broad airport input to ensure work is not planned without the consideration of other airport projects that may pose different requirements for the airport's security camera system in the near future. Section 6 of PARAS 0016 – *Airport Security Vulnerability Assessments*[7] provides detailed guidance for conducting a benefit/cost analysis.

When the results of a security camera review support upgrading or replacing a system, it is always an option to not proceed with the project. However, choosing this option will result in zero positive gain, and may result in the evaluation being revisited again in the near future. Furthermore, not upgrading a security camera system can leave an airport exposed to risks identified in the SVA. The cost of

[5] Designers should request the specific version of the guidance document that is applicable to the airport and/or project.
[6] **NDAA:** https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf
[7] **PARAS 0016:** https://www.sskies.org/images/uploads/subpage/PARAS_0016.SVAGuidebook__.Final__.pdf

upgrading the system should be compared to risk of not upgrading the system by using the benefit-cost formulas and completing an airport SVA.

Budgeting for camera system improvements should be in the Airport Master Plan and updated every two to three years to ensure the budget is in line with current costs. Whether budgeted in the fiscal year plan, as a capital improvement project, or as a small tenant improvement project, the budget should be considered one of the most important and integral aspects of the project.

2.4.1 Existing System Maintenance Costs

Line items such as maintenance of the security camera system should always be included in the benefit-cost analysis. In addition to typical repairs and operational maintenance, costs for maintenance contracts, extended warranty contracts, software and licensing fees, and periodic training should also be considered. When considering upgrading an existing system, the increased cost and availability of parts as a system ages should also be considered. It should also be noted that as a system ages it often needs more servicing and maintenance for components.

SECTION 3: SYSTEM UPGRADE, OPTIMIZATION, EXPANSION, OR REPLACEMENT

After thorough review of the existing system, if the airport decides that the system should not be left in its current state, the next step is to determine whether to upgrade, expand, or replace the system. A decision matrix can be developed to streamline this decision process for various change criteria, such as camera end-of-life and firmware updates. See Appendix A for an example Camera System Decision Matrix.

3.1 System Upgrade

An upgrade to an existing system is typically performed if the system's inadequacies can be resolved by adding or replacing system components. These inadequacies may occur when new requirements are added or if the existing requirements have evolved to require more monitoring capability. They can also be derived from the results of a needs assessment or SVA.

The upgrade process can involve replacing old cameras or recording devices, or installing new software that complements the existing VMS. These components should be tested before their integration into an existing system. After the upgrades have been completed, existing integrations should be reviewed to make sure they are supported by the upgrade and that all replacement components work within the system.

It should be noted that replacing cameras within an existing system may upgrade the viewing capabilities, but the system may still be limited by the manufacturer's software that manages the cameras. It is important to understand that upgrading single portions of the camera system may not provide the desired results. An existing system can only be upgraded so far before the limits of the system capabilities have been exhausted. It is also important to make sure the goal or intention for upgrading the system is clear prior to implementation.

3.2 System Optimization

Optimization of a video camera system is a process of mitigating issues or enhancing the system based on its existing capabilities.

SOFTWARE

A manufacturer may routinely and systematically optimize their system's software. Software patches or firmware upgrades, often available for download from the manufacturer's website, can update existing system features or provide additional or enhanced features that were not previously available. This is not necessarily an upgrade to the existing system, as this process is typically to ensure the operating system remains fully relevant and efficient based on the latest software developments.

Software optimization can be regulated and managed by the IT department to be automatically downloaded, executed, and configured, or the updates can be retrieved from the vendor's portal. In some cases, the updates can be partially installed to apply only the specific features required by the user. Communication between the end user, IT department, and the vendor is critical to ensure the optimization has been fully executed and has not diminished the system's operation.

A backup of the current system configuration should be performed before any work begins.

HARDWARE

Optimization of a video camera system can also involve utilizing the existing physical infrastructure (e.g., cables) to change a camera type from, for example, a fixed camera to a multi-imager camera to increase the coverage area.

3.3 System Expansion

Expansion of a video camera system involves adding components or devices, or changing security procedures to fill gaps in security, provide additional monitoring, and mitigate potential threats and vulnerabilities.

An example of where this option might be considered is an airport with a working camera system that is fulfilling the requirements of the security program. The airport then adds assets where no cameras were previously installed, so the airport will need to increase their camera coverage. Depending on the limits of the system (e.g., camera license availability, networking constraints), expansion may be a viable option.

Budgetary constraints will be a major consideration in the decision to expand an existing system. The cost of additional cameras, storage devices (e.g., NAS, storage bays), integrated software, and infrastructure can influence a project's budget. NDAA compliance will also be a consideration, as components installed prior to the NDAA may not be in compliance, which would make them ineligible for further purchase.

Expanding an existing security camera system also requires consideration for space requirements for cabling, new equipment, cameras, etc. Also, a backup of the current system configuration should be performed before any work that could jeopardize the system begins.

3.4 System Replacement

Replacement of an existing video camera system is considered a last resort, as this option has the most impact on operations, budget, training, and system capabilities, and may have overarching effects on the security of the airport.

An airport typically replaces a camera system when it determines that the existing system cannot be upgraded, optimized, or expanded any further, and the full capabilities of the system do not meet the airport's requirements any longer. There are numerous reasons why an airport may want or need to replace a video camera system, but the most crucial and time-sensitive reason is that the system is deemed end-of-life. It is generally understood that system components can be deemed end-of-life when they are no longer supported and the model has been replaced in the manufacturer's product lineup. Entire systems can be deemed end-of-life when a manufacturer has gone out of business or otherwise ceased operating, and there is no further support for the system. A legacy analog camera system should be replaced as soon as possible to mitigate potential loss of coverage and to meet current video standards and technologies as funding and program approvals allow.

Replacement of video system components, such as cameras, should not be the determining factor in replacing an entire system. However, replacement of technology may be a catalyst for full replacement or upgrade. For example, replacing an analog camera with a high-definition IP camera on an analog infrastructure may not require system replacement since the more advanced camera can operate on the analog infrastructure through the use of converters and network integration components. On the other hand, if the headend system cannot support the the new camera, and this camera is included in the security design criteria or project scope, then replacement of the system may be warranted.

Replacement might require the most planning. Phasing will need to be considered so that the existing system is not impacted by the replacement work being performed until the new system is deployed.

3.5 Project Phasing and Methodology

Project phasing includes project management and should be applied when making any changes to a camera system, whether upgrading, expanding, or replacing. The scope of the project will determine the complexity and length of each phase, but all phases should be implemented to provide the best possible outcome. Proper planning will assist in keeping the project within budget.

INITIATION

The stakeholders determine the security requirements based on the airport needs and how those needs are currently lacking with the existing camera system. Based on that assessment, a decision is made to optimize, upgrade, expand, or replace the current camera system. A scope of work is developed that outlines project goals and dates for project start and completion. If the project is small (e.g., adding a camera) the work may be performed by in-house technicians or with the integrator currently maintaining the camera system. If the project is larger (e.g., replacing all cameras and infrastructure or upgrading the full system) the project may go out for bid or be a sole-source award. In either case, the initiation phase is when the integrator will provide a proposal to complete the work, and a contract will be executed.

PLANNING

A project team will develop a schedule for the installation and share it with the stakeholders. The schedule will be a detailed plan for each task to be completed from kickoff to turnover. The project manager is responsible for maintaining the schedule and updating the stakeholders on progress.

EXECUTION

When the schedule is agreed upon, the contractor will begin to complete the defined milestones in the schedule. Project monitoring and control occurs during the Execution phase to ensure the schedule is on time and within budget.

However, it is not unusual to discover inconsistencies in the existing installation that may require changes to the scope of work or schedule. Daily or weekly meetings should be held to keep the stakeholders informed of progress and to address any variances to the project. Any changes to the project and schedule will be tracked and agreed upon by both parties.

When working on a live system, it is imperative to ensure that the camera system is not degraded in any way, and to test each new camera for full functionality prior to deactivating the existing camera. If necessary, the existing camera may need to be reinstalled if there are issues with the new product.

CLOSURE

At completion of the installation, a final system test and inspection will be performed by members of the installation team and stakeholders. A successful completion will require a documented test procedure that is agreed upon and signed off by all parties. There may be a punch list for unfinished items that the contractor will need to address if any discrepancies are found during the final test and inspection.

SECTION 4: SYSTEM DESIGN AND COMPONENTS

Video camera system design includes consideration of camera technology, IT infrastructure, and supporting systems. All of these are factors are critical to the design of a functional security camera system. The recommendations for components within a video camera system can be determined by the scope of work for the upgrade or implementation. PARAS 0028 (Appendix G: Security Systems)[8] succinctly illustrates how each camera and function can contribute to a video camera system.

4.1 Camera Technology

The camera technology needed to monitor an asset is determined by the design criteria or functional requirement of the project, the security program, and the established scope of work. The monitoring requirements can have an impact on the type of technology selected.

Types of cameras vary in their availability, capabilities, mounting, and feasibility of use. In addition, the installation environment can determine a camera's type, use, and recording requirements. The most versatile and widely used camera in facilities is the fixed dome camera, which can accommodate many different mounting applications and can be used with varying lenses and environmental protection. Below are some additional camera types that are typically installed with video camera systems:

- **Fixed cameras** require the lens of the camera to match the field of view requirements. Varifocal lenses are typically used in these types of cameras to adjust the field of view without changing the lens, but varifocal lenses are limited to specific ranges, typically 2mm to 25mm.

  If considering adjusting the camera location to maintain view of an asset that has been moved, and the varifocal lens has been zoomed in or out as far as possible, changing the lens may be more cost effective than moving the camera and its supporting infrastructure.
- **Single-Sensor Panoramic cameras** can replace several cameras with one camera, and can be installed either horizontally or vertically. Horizontally mounted, the camera displays either a single 360-degree birds-eye view or can be configured into two separate 180-degree views. Mounted vertically, the same camera can provide a single 180-degree panoramic view.

  Single-sensor panoramic cameras depend on the VMS to dewarp the image from a fisheye view, so they need to be compatible with the VMS with which they are being managed. It should be noted that, if the camera is not supported by the VMS, upgrading the VMS software may invalidate use of the camera's image for prosecution purposes as, technically, the dewarping alters the original image. When the VMS supports the camera, however, digital evidence can show that the image was not edited.
- **Multi-Sensor Panoramic cameras** can provide up to five different camera views within a single camera housing, saving both infrastructure costs and costs of purchasing and deploying other cameras to provide the same views.
- **Pan-Tilt-Zoom (PTZ) cameras** provide maneuverability of the field of view and the ability to zoom in on a specific target both optically and digitally. PTZ cameras are particularly useful for target tracking where fixed cameras provide a limited field of view.
- **Bullet cameras** are small, high-resolution, low-cost cameras that can be installed in rugged and tight areas.

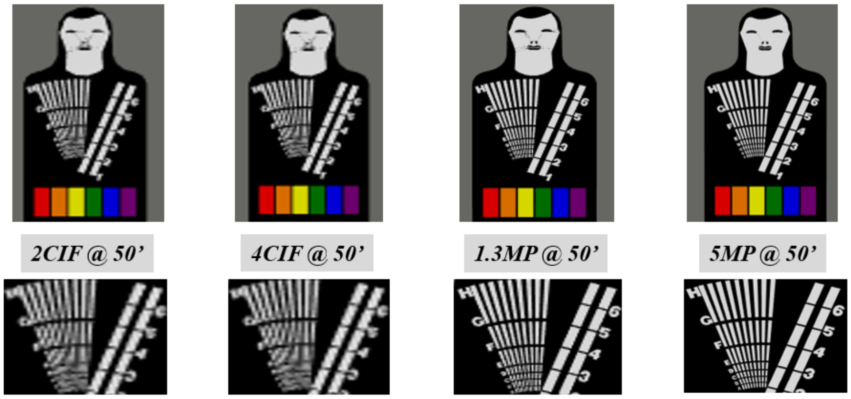
[8] **PARAS 0028 –** Recommended Security Guidelines for Airport Planning, Design, and Construction: https://www.sskies.org/images/uploads/subpage/PARAS_0028.Recommended_Security_Guidelines_.FinalReport_.pdf

- **Thermal Imaging cameras** create images using heat signatures of objects in their field of view. This enables the camera to provide surveillance in total darkness, which can be useful in areas where lighting is unavailable or not conducive to video surveillance.
- **Night Vision cameras** enable monitoring in lowlight environments by gathering light from sources such as stars, ambient light, or distant lights to provide an image. This technology is sometimes coupled with an active infrared illuminator, either incorporated into the camera or as a separate device, that enhances images in low- to zero-light conditions.
- **Multifocal Sensor cameras** provide an array of up to eight high-definition cameras within a single enclosure. Each camera within the enclosure converges into a single image but provides optimal clarity, resolution, and situational awareness.

4.1.1 Resolution Requirements

Several factors contribute to the quality of the camera images displayed on the system's monitors. One of these is the camera's resolution, which is the total number of pixels that make up the camera image. This in turn influences the number of pixels on target, which determines how clear a particular object is in the camera scene. The pixel requirement is a critical component to determine if a camera meets the functional requirements for the specific monitoring location or if it needs to be replaced with a higher resolution imager.

Figure 4-1. Examples of Different Resolutions at the Same Distance



2CIF @ 50' *4CIF @ 50'* *1.3MP @ 50'* *5MP @ 50'*

Source: PARAS 0028

There are several different calculations used to determine the specific number of pixels on target required to see a clear image. PARAS 0028, Section 3.2.3 Video Surveillance Systems identifies the Detection, Observation, Recognition, and Identification ranges for a camera's field of view to provide optimal resolution per the environment.

4.1.2 Video Analytics and Artificial Intelligence

Video analytics work by monitoring and detecting changes in pixels on the camera imager and using algorithms to process those changes. Alerts can be set up to automatically notify monitoring staff of a specific event that is occurring or has occurred based on the degree and pattern of the changes.

Video analytics can be used to detect many different events such as an object left behind, object removed, people counting, frequency of use, breaches, vehicle detection, pattern recognition, etc. Video analytics should not replace human monitoring and assessment, but are a useful tool in enhancing detection in an existing monitoring program.

Artificial Intelligence (AI) is a form of video analytics. While AI processors use some form of video analytics to track objects, AI identifies those objects using specialized algorithms, predictions, and constant learning. For example, with analytics it is possible to identify a person as an object, but AI can further identify the person as a white male wearing a red shirt, brown pants, and a mask, which can be beneficial when tracking an individual or searching video after the event.

4.2 IT Infrastructure

Telecommunications support provides the pathway between the cameras, the switch, and the monitoring workstations in an IP camera system. During an upgrade project, the existing infrastructure should be evaluated to determine if it supports new devices or if additional cabling may be needed. Depending on the age of the infrastructure, cabling standards may have changed and new technology may have emerged, making the existing infrastructure obsolete. This may influence the feasibility of adding to an existing system.

Early discussions with the IT department are critical to the success of camera deployment projects. It is important to understand if the video surveillance system will have a VLAN to support better data traffic management. It is also critical to understand whether a network camera needs to provide multiple streams (unicast network configuration) or if the network will replicate the data streams (multicast network configuration).

4.2.1 Network Cables

There are several options available for network cabling. Each has pros and cons, as described below.

UNSHIELDED TWISTED PAIR (UTP)

UTP cable consists of twisted pairs of copper wire inside an outer jacket. This type of cable has no metallic shield, which makes it susceptible to electrical interference. A UTP cable's rating determines its application. Category (5/5e/6/6a) rated cabling provides the pathway for data between the camera and the patch panel and switch in the IT room. The category rating of the cable usually depicts the speed and efficiency at which data is transferred between the camera and the switch, but is predominately limited by distance (typically 328 feet [100 meters]).

During review of an existing video surveillance system, cable integrity should be taken into consideration, as the age and condition of existing cabling can affect performance and operation of cameras and other edge devices. Age, vermin, friction from adjacent objects, and excessive heat are some factors that can deteriorate existing cabling. Because these cables are normally installed above the ceiling and out of sight, these threats are often unrevealed until the cable integrity is tested or a camera or edge device fails.

Be conservative on cable lengths and check the power out of the network switch. When designing cable routes, use a 290-foot maximum (including bends). If the cable length exceeds the maximum distance, an Ethernet Extender can be utilized, though it should be understood that it will require power. In addition, older network switches may not be able to adequately power the IP camera if the 328-foot camera distance is exceeded.

FIBER OPTIC CABLE

Fiber optic cable is usually installed when the distance from the IT room to the camera location is further than the maximum distance of copper cable (approximately 300 feet), and when a bandwidth transmission rate of at least 10 GB is needed. Remote areas of an airport often rely on fiber.

Fiber is very fragile, but the cables themselves do not typically fail regardless of age. Because fiber is glass, fiber failure usually means the cable has been broken at some point between the edge device and the source. There are tests that can be performed to detect these breaks, and depending on the length of the run, the fiber can be restored quickly. Fiber does not carry power, so local power must still be provided at any new camera location. The following types of fiber optic cables are used with surveillance systems:

- **Single-mode fiber** is the most common fiber for surveillance cameras. It can transmit to distances of up to about 60 miles from the source. Because of this extended data capability and speed, surveillance cameras benefit from the fast and efficient data transmission rate of images to the VMS in lieu of other transmission processes, such as wireless.
- **Multi-mode fiber** is typically used for shorter distances (about 1,800 feet) and has a slightly higher attenuation rate than single-mode fiber, but it is cheaper to install. Multi-mode fiber is typically not used for surveillance camera pathways. For most camera installations within distance, multi-mode fiber will be sufficient. For installations of high megapixel cameras (12 MP and above), it would be recommended to only transmit on single-mode fiber to support the increased data traffic.

COAXIAL CABLE

Depending on the age of the existing video surveillance system infrastructure, coaxial cable may be the pathway used for transmission of camera data to the IT room. Coaxial cables cannot support IP camera transmissions without a media converter on both the transmitter and receiver sides. While this solution can support utilizing the existing infrastructure, the media converters introduce additional potential points of failure within the camera system. When migrating from analog cameras to IP cameras, consideration should also be given to replacing the coaxial cable with UTP data cable (Category 5, 5e, 6, 6a).

4.2.2 Bandwidth

To effectively transmit image data over an established network, bandwidth should be robust enough to accommodate the minimum requirements of the camera system and any other devices that rely on the network. With the introduction of H.264 and H.265 compression rates, as well as MPEG4 and MP4 file formats, video camera systems have become less taxing on a network, but can still have major impacts if the network is already overwhelmed.

Early discussions with the IT department should be held to determine if the current network can handle additional video camera system data, as the existing network may comfortably accommodate the current system but may struggle to support a new or expanded video system. Likewise, if planning to install new networking infrastructure, be forward thinking when designing the system backbone. Camera technology is continually providing higher resolution cameras that generate larger amounts of data requiring more bandwidth. Having too much network is not a problem, but needing more and not having the ability to expand is.

4.2.3 Physical Space

The availability of space within a network cabinet should be considered when planning camera additions or upgrades that may introduce new network equipment, such as switches, patch panels, servers, or other equipment needed to accommodate the project. Network cabinet space is limited, so advance planning will be needed to install additional components. Adding another cabinet or expanding the telecommunications room may be required.

In a typical networking environment, a telecommunications room or IT closet is the primary location for network equipment cabinets that house the network components not necessarily associated with security. However, in an open network where there may be multiple system-networked components, these components may be provided with their own equipment cabinet instead of being installed in a common cabinet. Switches, patch panels, servers, and routers are some of the typical networking equipment located in a dedicated network cabinet. Depending on the amount and type of other network-dependent systems, the cabinet can be crowded with many other systems' components.

For camera systems, camera cable terminations can take up a substantial amount of space in a patch panel. And in some networking topographies and standards, the camera system may require a separate patch panel or even a designated cabinet. Therefore, the availability of cabinet space can depend on the use of a common patch panel versus a dedicated patch panel for cameras. The internal space of the telecommunications room will determine the feasibility of a dedicated security cabinet for separation of system components.

Expansion projects can present their own challenges if not properly coordinated. Storage retention calculations should be thoroughly allotted to determine the additional storage components that are needed in the equipment rack. Storage bays typically take up at least one Rack Unit of cabinet space.[9] If space for these additional components is not regulated by standards (i.e., requiring scalability), issues can be compounded if there is no available space, as the telecommunications room may not be able to support additional equipment cabinets.

4.2.4 Network Equipment Features

Network equipment must be considered when optimizing, replacing, upgrading or installing cameras. Considerations include POE requirements, VLANs, and dedicated security networks:

- **POE** – While a common feature on networking equipment, older switches may not have this feature or it may only output the standard 13.3W. This is sufficient for the majority of fixed IP cameras, but PTZ cameras utilizing POE require a minimum of 15W.
- **VLAN** – A VLAN offers a way to provide a separate LAN without installing new equipment. It segments the network, separating it from the general LAN, providing a measure of security and decreasing latency that would come from the new video data.
- **Dedicated Security Network** – As the name implies, this is a completely separate network with its own networking infrastructure and equipment. It is the best way to secure the data from the general LAN, but comes at a high cost. Dedicated Networks are normally used in very high secure environments where they are required due to regulation.

[9] A Rack Unit is a standard term for the vertical size (1 ¾") of a piece of equipment mounted in a rack.

4.2.5 Network Hardening

Securing the airport network is just as important as securing the physical assets on the airport. Hardening a network can minimize the effects of potential threats and enable critical operations to continue after a threat has been detected.

Steps that should be taken to provide a level of continued or advanced protection when revising an existing IP camera system include:

- Reset the manufacturer’s password on the camera when installed.
- Manage contractor access to the server by providing a new password on the server that is instantly removed when contractor access is no longer needed.
- Provide only the network access required to fulfill the scope of the contractor.
- Limit network access through contractor-owned laptops and mobile devices when configuring and managing the system. Utilize owner network–approved devices for configuring and managing the system.
- Continually monitor network traffic during the camera configuration.
- Work with the IT administrator and the manufacturer to ensure all updates are installed.
- Ensure strong passwords are used for all system logins.

4.3 Supporting Systems

Ensuring the reliability of network support systems is crucial because failure of the supporting systems can impact the operation of the camera system or the network itself.

4.3.1 Video Management System

The VMS manages all cameras connected to the system, both IP and analog. A VMS upgrade can be as simple as upgrading the manufacturer firmware or replacing the manufactured solution altogether.

Each camera has its own IP address, firmware profile, and embedded features, but the VMS provides access to those functions. It should be noted that cameras do not necessarily have to be of the same manufacturer as the VMS to function, but some functions of those cameras may or may not be available within the VMS if the manufacturers are different.

Over-specify servers when upgrading the VMS, as the VMS software will have updates over its lifetime. Like budgeting for bandwidth, it is better to have too much than not enough as the system matures and grows.

Integrate the VMS with access control systems (ACS) when possible. Many incidents at an airport trigger an alert (forced door, badge entry, emergency telephone, motion sensor, etc.) that is annunciated on its respective system. If the systems are integrated with the VMS, a camera can be programmed to immediately call up a view of the alert location for review. If there is an investigation, the video will be tagged to that event for easy retrieval. If the systems are not integrated, the operator will need to manually match the time from the event to the time on the VMS and find the specific camera in the area.

4.3.2 Monitoring Workstations

Cameras can be monitored in a variety of ways, including:

- **Desktop Computer:** A desktop workstation provides a local platform to install client software for cameras to be monitored, configured, added, or deleted. This is usually located at a staff desk location and can be used with other non-camera system software.
- **Rack-Mounted Laptop:** Usually mounted in an equipment cabinet, this laptop can provide remote management of cameras within a telecommunications/IT room, as well as provide troubleshooting of the system outside of the operations area.
- **VPN access:** This allows remote access to cameras, per airport security and IT department guidelines. Specific or all cameras may be accessed via a remote client application or workstation outside the airport environment.

Do not underestimate the workstation and graphics processing power required to view cameras. To minimize bandwidth, video streams are highly compressed at the point of transmission and need to be decompressed to be viewed on the workstation. This decompression task is processor intensive. Working closely with solution providers will ensure the workstation is sized appropriately.

4.3.3 Cooling Systems

Heat dissipation systems are among the most critical components of a network support system. Depending on the location or environment where the network equipment is located, failure of an air conditioner, fan, or cooler can have devastating effects.

As network equipment creates heat, a telecommunications room can quickly become too hot for the system to function any longer. POE switches, NVRs, and servers may shut down once the temperature reaches a certain threshold (typically around 150°F). As such, a high-availability cooling system should be installed and maintained in each room that houses security camera system network equipment. This cooling system could include a dedicated and supervised thermostat, a computer room air conditioner unit connected to Uninterruptible Power Supply (UPS), an over-cabinet fan, or inductive floor cooling.

4.3.4 Camera Power Supplies

All cameras require power to operate, whether it be from remote power, local power, or solar power. Any project requiring camera changes or provision of power to new cameras should consider the power required for that camera type. Power requirements for cameras can vary between camera types, so a one-for-one camera switchout may or may not be feasible using the existing power supply. Each camera should be evaluated for compatibility with existing infrastructure and available power both at the network rack and at the camera location.

- **POE Switch:** The POE switch is an integral part of an IP surveillance system upgrade in that it manages the network data transmission to and from the camera, and it also provides up to 12.95 watts of power to each camera. Video system upgrades where new IP cameras are introduced should take into consideration the POE requirements for new technology. Some cameras, such as IP PTZ cameras, may require POE+ power, which provides up to 25.5 watts.
- **Power Injector:** Where a new camera has been added to an existing system that may not have been part of POE infrastructure (non-POE switch), a power injector may be required to provide power to the new location. Because power injectors require 120V AC power at the device, they should be powered by the same power supply as the switch in the network equipment rack.

4.3.5 Backup Power Systems

The UPS is another important component supporting the security video camera system. This apparatus provides temporary power for telecommunications rooms and/or network cabinets during a power failure, or interim power until a generator, if provided, becomes fully operational.

The UPS is considered emergency power and should be maintained to ensure availability when needed. It should be stressed that UPS power is not permanent power and has a time-limited range of availability based on the battery amperage, rating, and manufacturer. If UPS is the only emergency power available during a power failure, calculations should be performed for each UPS to determine the amount of time available.

Generators supply power on a much larger scale than UPS. They are capable of powering not only supporting systems but the entire facility during a main power failure. The generator should be maintained to be available immediately upon power failure. The system's fuel should be maintained at full level before an outage and should also be available for replenishment during a lengthy outage.

4.3.6 Patch Panels

A patch panel is a unit that contains multiple ports to connect, route, and organize cables. Patch panels are utilized to connect incoming camera data cables to new patch cables that attach to the network switch. Due to the distance limitations of IP data and power, cameras will typically connect to the nearest usable IT room, and the IT administrator will designate ports on the patch panel and switch.

Although not ideal, it is not uncommon for security and other systems' cables to co-exist within the same patch panel. This is acceptable as long as allocation of ports and availability of additional rack space are accounted for, and cohabitation of systems' cables is permitted in the airport security standards. As rack space in a network cabinet is sometimes limited, it is usually more feasible to reallocate or reorganize ports on an existing patch panel to accommodate additional camera terminations than it is to install a new panel in an existing cabinet.

To easily identify what ports are used for the security camera system, the airport's cabling scheme should specify a unique color for each system's cables. This will facilitate identification for IT personnel when maintaining or troubleshooting the system.

4.3.7 Cable Pathways

Cables from a camera to the headend can be routed through a dedicated pathway or a shared pathway with other cables from other IP systems. Planning for upgrading or replacing cameras or other components in the system can also include reusing, replacing, adding to, or removing old pathways to accommodate the design requirements. As many cable types have distance limitations for effective performance, and pathways for cameras can comprise a major portion of the budget, conduit routes should be kept to the shortest path possible to accommodate the device locations.

Conduit requires a dedicated pathway that may traverse a facility from device to termination point. This path can be composed of metal conduit or polyvinyl chloride (PVC), which varies by installation locations and local code. Metal conduit provides the most protection because of its composition and its impenetrable structure, which enables cables to be run in harsh environments. However, metal conduit is often expensive. PVC conduit is not expensive, but it does not afford the protection capabilities of metal conduit and is also limited in its deployment.

Conduit fill ratios determined during a previous installation may not accommodate system growth. When planning to use existing conduit pathways, this oversight can limit the use of the conduit or require the installation of new conduit, or the new cable can be installed without conduit (where local codes permit). Either way, the new installation will ultimately affect the project budget.

Cable tray systems provide open pathways for deployment of new cameras or upgrading or replacing cameras. Like conduit, they can be composed of metal or plastic. Unlike conduit, however, new cables can be added to open cable trays up to the weight limit of the supporting infrastructure or as determined by the airport's telecommunications standards. Also, a cable tray can be reused repeatedly without requiring much reconfiguration or calculation of its fill capacity. Upgrading, expanding, or relocating cameras can be accommodated with cable trays easier than with conduit. However, assessing the condition of the existing cable tray system to determine scalability should be a precursor to planning for any new cameras to be added to the video camera system.

4.3.8 Media Converters

Media converters enable conversion of cabling from one type to another. This can include coaxial to/from copper, fiber to/from copper, and fiber to/from coaxial, depending on the existing or new camera infrastructure.

Media converters are an excellent method of extending a video signal from a camera location to the patch panel without diminishing the signal strength. The typical conversion in a camera system topology is fiber-to-copper, though other media types also require conversion and would need to be assessed in the planning stage of an expansion or replacement project.

The disadvantage of a media converter is that it adds another component that can be a single point of failure, as it requires power to operate.

4.3.9 Other IT Equipment

An airport's layout, infrastructure, and environment all factor into the design of a camera security system, and can necessitate specific equipment. For example, a network run may be longer than 100 meters, or the existing analog cameras or cabling may need to stay in place while the VMS system is upgraded. The following equipment can be used to address various types of installation challenges:

- **Video Encoder** – This device converts an analog signal to IP, allowing existing CCTV analog cameras to remain in place and communicate with an updated VMS.
- **IP Converters –** These devices are used in pairs to transmit IP data and POE over existing coaxial cable. This solution is useful if a high-resolution camera is required but replacing the coaxial cable is not feasible at the time of the system upgrade. IP converters are not recommended as a long-term solution. They also have distance limitations, and require the coaxial cable to be in excellent condition.
- **Ethernet Extenders –** The maximum cable distance for a POE ethernet signal is 328 feet (100 meters) to be in compliance with ANSI/EIA 568 design standards. This distance can be doubled with the use of an Ethernet Extender, but there are limitations that should be considered. These devices will consume 4–5W of power and should not be daisy chained. They are also a potential failure point in the system.
- **Wireless –** If there is a need to view an area where there is no IT infrastructure available, there are wireless solutions that can address this, including wireless mesh networks and high

bandwidth line-of-sight solutions. Consult an expert in this area to design the best solution in concert with the airport guidelines.

- **Paige GameChanger Cable –** This guidance document is manufacturer agnostic in all except for this specific item. This cable, from Paige Datacom Solutions,[10] has a patented design to support the transmission of IP power and data over 200 meters, which is double the distance of standard networking cable. This added distance does have a greater cost and cable diameter that need to be considered. But in instances where the nearest IT closet is at capacity, this cable could support a run to an alternate IT closet at a greater distance.

4.3.10 Lighting Requirements

The correct type of lighting is crucial to video camera system operation. Certain lighting types compliment video imagery while others hinder it. In certain situations, no lighting can be better than too much lighting. Lighting, color, shadows and weather conditions can all affect the image quality and analytic capabilities of a camera.

Typically, airport facilities and assets would always be lighted. However, where lighting conditions are not optimal, there are a number of possible mitigating strategies, such as:

- Adding lighting stanchions for temporary locations
- Installing cameras with embedded infrared illumination
- Installing standalone infrared illuminators
- Installing additional permanent lighting
- Relocating the asset to a lighted area

Video analytics also have specific lighting considerations that are critical to accurate and reliable detection. The varying types of analytics will be affected differently by lighting. Subject matter experts should review the lighting in each camera's location to ensure it meets the minimum requirements of the ASP.

4.3.11 Data Storage

Data storage requirements vary from airport to airport. At a minimum, all video data should be stored for 30 days. Each airport may have a different recording standard based on their ASP. Existing storage capacity should be evaluated for any additional video data requirements before planning for replacement or upgrade of the VMS. Data must be safeguarded from deletion or corruption until the last day before cutover to a new system, if being replaced.

Storage procedures should be in place for additional retention beyond the prescribed date. These procedures should be a part of the security design standards. Examples of procedures could include storage on DVD, portable hard drive, or DVR network area storage (NAS).

Frame rate, resolution, compression, and the number of cameras will determine the size of the storage required. Data storage also correlates to the system infrastructure and other building system needs (e.g., power requirements, rack space, cooling systems), and should be considered when reviewing the Needs Assessment. Camera system upgrades or replacement can affect the storage requirements as key factors change.

[10] **Paige Datacom Solutions:** https://paigedatacom.com/gamechanger

SECTION 5: IMPLEMENTATION

Whether optimizing, upgrading, expanding, or replacing a video camera system, implementation will account for most of the planned budget. Selecting the right vendor, planning the installation, testing, follow-on maintenance, and support is essential for maximizing the use and longevity of the system. The project delivery method, type of contract, and selection criteria all must be determined prior to issuing the RFP.

Changes to the project design or installation parameters typically occur during stakeholder collaboration and communication. However, during the installation/implementation phase of the project, aspects of the project may require revisions, which may affect the project constraints (scope, budget, timeline).

On larger scale projects, a Change Control Board should be established to ensure that any changes in the scope have been carefully and diligently planned, discussed, resolved, and distributed to the team for implementation. Authorization of project changes from the board should be well documented and recorded in the project files, since the outcome may affect currently established baseline contracts and specifications.

5.1 Project Design

When the project is ready to be implemented, the next steps are to define what the final solution will be and how it will be built. Most airports do not have the in-house expertise to complete the project design, so a consultant would typically be retained to perform this service, which consists of the following tasks:

- **Schematic Design:** This is the first stage of the project, focused on defining the project scope. It is written in narrative format, and often describes the camera system components recommended to be implemented at the airport. This report will not relay costs or budgetary constraints but will be used as a pathway to budgetary discussions as the project progresses into design. The focus of the Schematic Design phase is to lay out the foundation of design for the system, and its intent and use. In some cases, this is done in conjunction with a narrative of the existing system or requirements that may be carried forward into the project.
- **Design Development:** This is the phase of design where cameras will be displayed on a design drawing to allow the owner and end users to visualize where cameras and security camera-related components will be located. Feedback regarding specific requests and feasibility during this stage is critical to the development of the design. During the Design Development stage, an estimate for the camera system is discussed and realized based on the design thus far. The design can be scaled back or embellished based on this estimate. In this stage of design, cameras and their associated components can be evaluated for cost, features, and best fit for the project. The Design Development stage is where the system can be developed, edited, changed, and adapted before it is solidified in the next design phase.
- **Construction Documents:** During this stage, design drawings and specifications are fully developed. The surveillance system is well underway, and coordination with other disciplines can occur to ensure that the intended camera views and system operation will function as desired. Through several iterations of design deliverables, the design package is finalized. The drawings and specifications are sent out for bid by contractors/integrators at Issue for Permit, Issue for Bid, or Issue for Construction. At this point, all changes and owner requests should have been reconciled within the design package. Any further changes directed by the owner after the drawings are issued will be considered a design revision. The changes are documented in the

Construction Administration process so that cost considerations can be documented along with the change.

- **Construction Administration:** This pertains to how the installation, implementation, programming, interfacing, integration, and commissioning is monitored and enforced throughout the construction phase. There is a lot of movement and responsibility within the Construction Administration phase that can result in an unsuccessful project if not thoroughly managed. The Construction Administration phase allows monitoring of any deficiencies in the installation process through product submittals, shop drawings, and site visits. All these steps are documented pieces of the Construction Administration phase that work together to ensure that the final camera system aligns with the design drawings and specified products.

5.2 Vendor Selection and System Procurement

The approach used to select a vendor should follow project specifications and timelines. The stakeholders will evaluate competitive proposals and rank them based on predetermined evaluation criteria.

Prior to releasing the RFP, the stakeholders will establish the type of project delivery method and contract vehicle that best fits the project needs. The project delivery method is how the project will be delivered (designed and installed). For airport construction and system installation, there are three primary models: Design-Bid-Build, Construction Management at Risk, and Design-Build. The contract vehicle is how the parties (designer and contractor) will be compensated. The three most common contract types are Firm Fixed Price, Cost Plus, and Guaranteed Maximum Price.

5.2.1 Preferred/Required Manufacturers

Preferred manufacturers, or sole sourcing, either as required or requested by project stakeholders, can affect the project scope and budget, especially when the preferred manufacturer is “embedded” in the airport and feels assured that they do not need to compete on price. For example, if an airport has an existing VMS platform that works only with specific cameras, the proposal costs for the camera replacement may be higher since the manufactuere knows that the airport is more likely to pay a premium for the cameras than replace their entire VMS and camera system.

If the existing system is already from the preferred manufacturer, its capabilities should be thoroughly researched and evaluated when determining if the manufacturer should be retained or replaced. Throughout this process, meetings and discussions with the current vendor should occur to ensure the feasibility of the project scope, without divulging any possible project direction to replace the vendor. This can ensure the discussion is unbiased and based on the capabilities of the current system to accommodate new technologies and upgrades versus “checking the boxes” on technologies that may or may not have been fully developed.

For replacement projects, sole-sourcing cameras or camera manufacturers is only recommended when those cameras provide better integration or data management with the existing VMS.

Where a preferred/required manufacter must be defined, consideration should be given to soliciting multiple bids from authorized installing contractors. So while the cost of the products may not be competitively bid, the labor for the installation, programming, testing, and commissioning can be competitive.

5.2.2 System Selection

Once the determination has been made to replace or upgrade the video camera system with agreed-upon specifications and a budget, a new platform should be researched and selected based on the agreed functional requirements. A review board should be assembled consisting of the Security Director, IT Adminstrator, TSA, stakeholders, and other individuals deemed necessary to ensure support for the new system. The review board will determine how the existing system is being used, what the shortcomings are, and how a new system can expand with the needs of the airport. Items to be considered include:

- How long has the manufacturer been in business? Are they a top-tier value-added reseller for the camera solution?
- Request a product roadmap from each candidate vendor. How is the solution positioned on the roadmap? If the solution is scheduled for a version upgrade, consider delaying the migration until the new software version is available, or ensure the software upgrade is included at no additional cost.
- Do other airports use the platform? Reach out to that airport's Security Director for feedback.
- What integrations are existing or desired? (e.g., ACS, Building Management System, Gunshot Detection, Perimeter Intrusion Detection, Emergency Telephone, Physical Security Information Management)
- How user friendly is the interface? Have a current operator review a sample version of the software.
- What features are offered or planned for? (e.g., video analytics, facial recognition)
- Does the system provide alerts via text or email? Is there a mobile interface?
- What is the warranty?
- What software license agreements are offered? Is the licensing agreement based on the number of cameras, number of users, number of video recorders, number of interfaces, etc.?

Selecting a new manufacturer involves research, a dedicated project team, and a clear definition of the system's requirements. Before making a final decision, request a demonstration version of the software or hardware and test it for features and operator experience.

5.2.3 Proposal Reviews and Selection Criteria

Proposal review is a calculated evaluation of the proposal as well as the vendor's ability to fully execute the contract per the conditions provided in the RFP. All proposals should be reviewed equally based on the criteria agreed upon by the stakeholder review board.

Best practices recommend the development of point-based criteria for the selection of qualified bidders. These criteria may vary depending on the size and scope of the project. The stakeholder review board will determine the criteria prior to receiving proposals. Cost, past performance, and technical competency should all be part of the review. Additional criteria, such as the following, may be considered based on input from the stakeholders:

- Bonded and insured
- Local to project site
- Number of personnel technically trained and qualified per manufacturer/system requirements
- Previous similar projects completed with references

5.2.4 Bidder Conferences

Pre-bid meetings and project walkthroughs provide an opportunity for prospective bidders to see the site, ask questions, and have the stakeholders clarify specific needs and expectations. Along with technical details, general site planning can be addressed such as site access, working hours, staging areas, material storage, etc.

Pre-bid meetings are typically optional but may be deemed mandatory if the project requires on-site review prior to submitting a proposal. The pre-bid meeting also provides the solicitor an opportunity to decide if the project is in the company’s best interest.

5.3 Installation

Installations will be in accordance with federal, state, city, and other agency standards as required by the stakeholders (e.g., TSA, CBP). As some airports—because of jurisdictional agreements—can self-certify construction projects, it is important to ensure the appropriate internal code officials are involved with the project from its inception to ensure all applicable codes are addressed in the design.

Prior to installation, the contractor must provide the stakeholders with documentation showing cable routes, equipment locations, conduit and wire type, penetrations, and connection schematics. When developing a project schedule, the contractor will work with the stakeholders and Security Director to verify working hours for each area of the facility that will be affected during the project. Most areas of the airport require installations to occur during non-business hours (e.g., midnight to 5:00 am).

The contractor should provide a daily work plan to the stakeholders, to include areas of the facility that will be worked on, personnel who will be conducting the work, and what will be accomplished (cable pull from location 1 to location 2, camera #001 installed, etc.). At the end of each shift, the contractor will supply the stakeholders with documentation verifying what was completed, tested, and signed off on.

All cables should be labeled on either end with *To/From* clearly marked in accordance with the site specification.

During upgrading or replacement of a system, there will be removal of existing cameras, cables, and other accessories. If called out in the proposal, the contractor can be required to repair all damage caused by removal to meet building or fire code.

5.3.1 System Migration Plan

Upgrading cameras or replacing the system headend unit will require a documented transition procedure. This will provide clear direction for the system integrator as well as let the stakeholders know which sections of the camera system will be impacted and for how long, so that security considerations can be planned for. All work should be conducted when there is little to no passenger or airline traffic. This time may fluctuate depending on airport size and operation but should be coordinated with the stakeholder Security Director.

The Migration Plan may include inserting video encoders that will not be part of the final design but will allow for the integration of older devices like analog cameras into a new VMS so that they can be viewed and recorded. As the older cameras are replaced, the temporary devices can be removed. The use of temporary networking devices or cable runs may also be necessary to ensure as little interruption to the existing operation as possible.

It is up to the installer to program, test, and verify all devices, cables, and connections prior to replacement. Existing devices, if operable, may need to be reconnected if there are problems bringing the new equipment online.

5.3.2 Personnel

The size and complexity of the project will dictate the type, expertise, and number of personnel needed to facilitate the contract. Contract personnel who will be working in secure areas of the airport may be required to pass a background check, site-specific safety training, and testing process to obtain a SIDA badge and, if necessary, airfield driving privileges. See PARAS 0037 – *Planning and Operational Security Guidance for Construction Projects at Airports*[11] for detailed discussion of construction personnel security measures.

5.4 Testing

It is essential to test the surveillance system to ensure it meets the minimum requirements for installation, programming, and operability per the project specifications and design drawings. Testing should be done whether introducing a single camera into an existing VMS, replacing an existing camera, or introducing a brand new system into the ASP. Testing should be performed after the security contractor has completed their initial tests for operation.

Testing should be performed in a consistent and methodical manner, using established parameters and scripts, to ensure that all components are tested individually and, if necessary, with other associated components to ensure basic functionality.

Unlike other security systems, camera system testing remains subjective. There is always the challenge of whether the view could be sharper or clearer. Because this measure is subjective and varies between individuals, a final approver should be identified at the start of the project.

5.4.1 Testing Requirements

Testing of the surveillance system should include, at a minimum:

FACTORY ACCEPTANCE TESTING

If determined necessary by the stakeholders, a visit to the system manufacturer facility may be required to validate the products being delivered are manufactured in accordance with project specifications, guidelines, and governing laws. When feasible, all or an acceptable sample of the project devices can be configured, programmed, and staged in a manner that is representative of the proposed design. This test is normally performed by the vendor; however, the owner and project team may attend as well. Documentation will be provided after completion of the Factory Acceptance Testing and signed by the vendor and the owner.

SITE ACCEPTANCE TEST

Upon delivery to the site, any component that is destined to be installed should be tested to verify its operability. Site Acceptance Testing ensures that any components with discrepancies are found, reported, and shipped back to the factory, if necessary, to reduce impact on the project schedule. The project specifications should include this test to mitigate warranty issues.

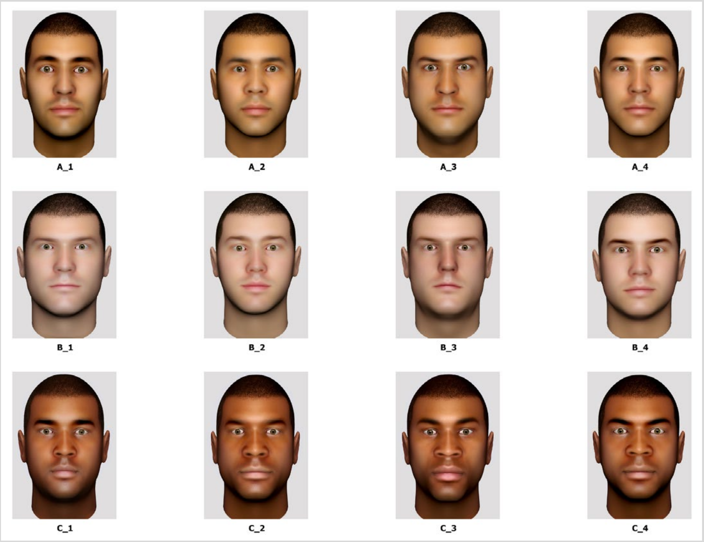
[11] **PARAS 0037:** https://www.sskies.org/images/uploads/subpage/PARAS_0037.AirportConstructionSecurity_.FinalReport_.pdf

BASIC INSTALLATION TEST

The Basic Installation Test ensures that cameras are installed per design drawings with a correct field of view, that images display on the monitors with their correct designations, and that the displayed images are clear with no distortion. While most users and those testing the system will agree on a “clear” image, standardized testing programs are limited. As a result, there is the potential for challenges from the airport, consultants, and installers as to the acceptance of a camera solution.

The British Standards Institute (BSI) has published BS EN 62676-4,[12] which provides guidance on a testing approach that utilizes standard testing cards and a Rotakin target. The Human Identification Test is used to test the camera’s capture and monitor display capabilities to ensure that the colors and graphics display align based on this set of non-descript face targets.

Figure 5-1. Human Identification Test

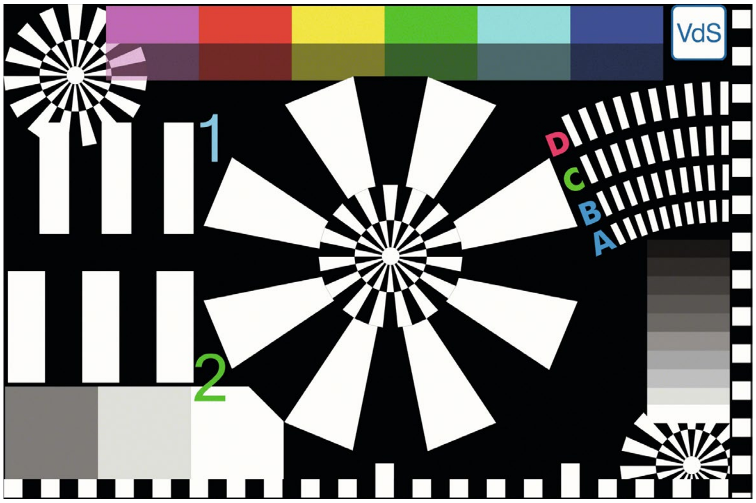


Source: www.gov.uk

The Standard Resolution and Color Rendition test chart, shown in Figure 5-2, is used to verify the camera resolution at a specific distance from the lens, and tests how it is displayed on the viewing monitor. The circular black and white patterns are utilized for this testing procedure. The tighter the distance between bands and the ability to distinguish the difference on the viewing workstation will confirm the resolution of the images captured by the camera.

[12] **BS EN 62676-4** (for purchase): https://global.ihs.com/doc_detail.cfm?document_name=BS%20EN%2062676%2D4&item_s_key=00655745

Figure 5-2. Standard Resolution and Color Rendition Test

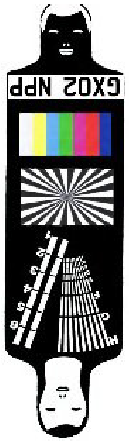


Source: www.gov.uk

The final testing procedure identified by BSI is the Rotakin and Rotastat testing target boards (Figure 5-3).[13] This procedure utilizes a high-resolution graphic target that provides a consistent image to compare colors, resolution bars, and height of the object. The Rotakin and Rotastat targets are similar, but the Rotakin has a motor that can rotate the target board at a fixed number of revolutions per minute. The rotation simulates a consistent level of activity within the scene to validate storage requirements, and also verifies the number of frames per second at which camera is transmitting and the recorders are storing video. A blurred or jumpy moving target may reflect that the frame rate for the camera or recording system is too low.

If the cameras are integrated with other systems, such as an ACS, the Basic Installation Test also confirms that alarm activations (i.e., door forced or duress) call up designated cameras with the proper view.

Figure 5-3. Rotakin Test Target



Source: rotatest.com

5.4.2 Additional Testing Considerations

If the existing camera system interfaces with an ACS, Perimeter Intrusion Detection System, Building Management System or other external systems, these interfaces must be thoroughly tested. The Security Director or delegate will verify each camera's call-ups per its associated trigger.

During interviews with airports to develop this guidebook, two primary concerns were identified with respect to camera testing:

- **Timing** – Cameras typically are one of the last devices to be installed in construction projects, as they need to be mounted to a finished surface (wall, ceiling, etc.). As a result, the testing of cameras is often at the very end of a project, right before the formal opening. Airports stated that the camera testing and sign off is often rushed to close out the project. To mitigate this risk, it is critical to ensure that camera testing is captured on the overall project schedule to ensure there is appropriate time to witness testing, confirm views, test storage rates, etc. Depending on the

[13] **Rotatest.com:** http://rotatest.com/index.html

number of cameras, no less than 30 days should be scheduled to complete camera testing properly.

- **Differing Opinions on the Image:** The anticipated camera field of view can be calculated in advance of the camera installation to ensure the functional requirement is being met. Often the challenge between the owner and the installing contractor is the quality of the image. The majority of the time, setting expectations in advance of camera selection is key. While many airports would like to be able to zoom in extreme distances and read a boarding pass, these capabilities are typically not commercially available or viable. To temper expectations, cameras to be used on the project can be set up in a test lab to simulate camera views.

5.4.3 Commissioning

Commissioning a video surveillance system should be detailed, concise, phased, and scripted. Commissioning is the final step before Owner Acceptance, and is done to ensure that every component of the system has been tested, verified, reported, and validated. The development of test scripts for the system as a standalone system, as well as for integration or interface with other systems, is important to ensure the system operates as intended.

A draft commissioning plan should be provided to the owner or project team at least 30 days prior to the commissioning to verify all parameters have been fully vetted per project specifications and airport guidelines.

5.5 Training

For any system to be effective, the staff using the system must be fully trained in the capabilities of the system's software and hardware. Commercial-off-the-shelf systems may include instructions on the use of the system "in the box," but do not instruct the end user in the operations of the system when integrated with other systems or in otherwise unique monitoring situations.

If the new technology has more capabilities than the existing system (i.e., upgrade or replacement), or if there has been a change in operation of the existing system (i.e., optimization or expansion), training will be required to maintain the security posture and operational functionality per the security program.

When upgrading the system to include new software or new system technology, the end users should be provided with at least eight hours of certification-level system training, to be performed and delivered by the installing security contractor using manufacturer-provided training materials.

Training the end users on the video camera system is important to ensure the staff is fully instructed in all system functions and integrated components. Training should focus on main system functions and in-depth use of the system capabilities that the staff will perform during their daily shifts.

To mitigate downtime, end users should also be trained on basic maintenance and troubleshooting functionalities of the new cameras and any other attached peripherals. Abnormalities beyond the capabilities of basic troubleshooting should be referred to the system installer, per warranty, or service-level agreement contract requirements.

Note that the existing security monitoring protocols, procedures, and tasks should not be altered drastically as the monitoring staff, who have been used to a certain way of performing those tasks, may develop "culture shock." New technology does not necessarily have to mean new procedures, unless that technology has never been used in the security program. Regardless of how small or large the effects of introducing or enhancing the technology, training is critical.

5.6 Owner Acceptance

As described in PARAS 0028 – *Recommended Guidelines for Airport Security Planning, Design, and Construction*,[14] Section 4.5, Owner Acceptance of a system installation is an essential step in any upgrade or replacement project. Whenever a major system is revised within a project scope, the system owner has to be satisfied that the scope of work specified in design documents and project specifications has been completed. After succesful implementation, integration, testing, commissioning, and training, the owner has to accept responsibility for the system.

If any of the work tasks of the project have not been fully reconciled or completed, the project cannot be closed out. Revisiting specific tasks to ensure complete reconcilation should be part of the work plan. Owner Acceptance is often overlooked as a project constraint, as the acceptance of the project can also affect the other constraints (i.e., budget, schedule, and scope) if the owner is not satisfied with the system as installed.

After the system has been deemed viable and complete through vigorous testing and commissioning, the system will be relinquished to the owner by the security contractor. At this point, the system will have been operational for at least several days, and any subsequent discrepancies or errors should be directed to the owner’s maintenance and warranty department for resolution.

The system warranty, as delineated during the design phase, will determine the level of resolution required by the responding agency (typically the installing contractor). The upgrade of existing systems should not preclude or override the existence of a valid existing maintenance contract. Owners should coordinate the initial warranty responsibilities with the system designer or project manager before project documents are submitted for bid. The installing contractor usually provides a warranty of at least one year; however, terms can be negotiated for continued support after the initial year.

5.7 Life Cycle Management

After successful installation, testing, and sign off, it is necessary to continually maintain and manage all parts of the camera system. Most cameras have very long life cycles and will function well past the standard warranty. It is not uncommon for a camera to function well for seven to fifteen years.

The VMS and storage devices operate on software that will continually evolve far past the hardware that they are installed on. VMS manufacturers offer agreements that provide updates to system software for as long as the product is supported. This will extend the life of the product, allowing stakeholders to purchase new server hardware as the software advances past the original platform’s performance. Keeping the operating software up to date extends the life of the system and provides security patches to reduce cyber threats.

Proper system maintenance and updates will extend the life of the product, but there are times when a manufacturer will discontinue a product and eventually stop supporting older products. It is important to keep abreast of the manufacturer’s product roadmap and updates so a plan can be put in place prior to any catastrophic failure. By reviewing the security camera system every two to four years, per the

[14] **PARAS 0028:** https://www.sskies.org/images/uploads/subpage/PARAS_0028.Recommended_Security_Guidelines_.FinalReport_.pdf

industry standard, the system optimization or replacement and budget for such items can be added as a line item to the Airport Master Plan.

Whether supporting the system in-house or using a system integrator for maintenance, having spare parts on hand reduces downtime. It also decreases the need of having to post a security officer until the component can be repaired.

REFERENCES

Document Name	Issue Date	Issued By	Website	Availability
Assessing the impact of CCTV	February 2005	UK Home office	https://techfak.unibielefeld.de/~iluetkeb/2006/surveillance/paper/social_effect/CCTV_report.pdf	Public
CCTV Technology Handbook	July 2013	DHS S&T	https://www.dhs.gov/sites/default/files/publications/CCTV-Tech-HBK_0713-508.pdf	Public
Digital Video Quality Handbook	May 2013	DHS S&T	https://www.dhs.gov/sites/default/files/publications/VQiPS_Digital-Video-Quality-HB-Appendix_180117-508.pdf	Public
PARAS 0002 – Companion Design Guide to US Customs and Border Protection's Airport Technical Design Standards	May 2017	Safe Skies	https://www.sskies.org/images/uploads/subpage/PARAS_0002.CBPATDSCompanionGuide.FinalReport.pdf	Public
PARAS 0008 – Findings and Practices in Sharing Sensitive Information (Synthesis Report)	February 2017	Safe Skies	https://www.sskies.org/images/uploads/subpage/PARAS_0008.SharingSensitiveInfo.FinalReport.pdf	Public
PARAS 0007 – Quick Guide for Airport Cybersecurity	January 2018	Safe Skies	https://www.sskies.org/images/uploads/subpage/PARAS_0007.CybersecurityQuickGuide.FinalReport.pdf	Public
PARAS 0010 – Guidance for Protecting Access to Vital Systems Impacting Airport Security	October 2017	Safe Skies	https://www.sskies.org/images/uploads/subpage/PARAS_0010.SecuritySystemsAccess.FinalReport.pdf	Public
PARAS 0015 – Guidance for Airport Perimeter Security	December 2018	Safe Skies	https://www.sskies.org/images/uploads/subpage/PARAS_0015.AirportPerimeterSecurity.FinalReport.pdf	Public
PARAS 0016 – Airport Security Vulnerability Assessments	June 2020	Safe Skies	https://www.sskies.org/images/uploads/subpage/PARAS_0016.SVAGuidebook__.Final__.pdf	
Recommendation: Closed Circuit Television (CCTV) Digital Video Export Profile – Level 0 (Revision 1)	April 2019	National Institute of Standards and Technology	https://doi.org/10.6028/NIST.IR.8161r1	Public

Document Name	Issue Date	Issued By	Website	Availability
Security Guidelines for General Aviation Airports	July 2017	TSA	https://www.tsa.gov/sites/default/files/2017_ga_security_guidelines.pdf	Public
Security Lighting - Guidance Document	February 2015	Centre for the Protection of National Infrastructure	https://www.cpni.gov.uk/system/files/documents/9f/fc/Security-lighting-guidance.pdf	Public
Surveillance Thermal Imagers - Guidance Document	January 2014	Centre for the Protection of National Infrastructure	https://www.cpni.gov.uk/system/files/documents/9f/41/surveillance-thermal-imagers.pdf	Public
TR69: Part 1:2019 - Technical Reference: Video Analytics within Video Surveillance Systems, Part 1: Reference architecture and interoperability	2019	Singapore Standards Council	https://www.singaporestandardseshop.sg/Product/SSPdtDetail/d34c32a8-6d26-4fa7-add2-8fddb418313a	For Purchase
TR69: Part 1:2019 - Technical Reference: Video Analytics within Video Surveillance Systems, Part 2: Selection, installation, and benchmarking	2019	Singapore Standards Council	https://www.singaporestandardseshop.sg/Product/SSPdtDetail/d3d8770b-56fb-4ccf-b238-d963c4b76a28	For Purchase
TSA Checkpoint Requirements and Planning Guide (CRPG)	May 2020	TSA	https://beta.sam.gov/opp/44099b735e494ef48cd27a9589c3c8ba/view	Public
TSA Electronic Baggage Screening Program (EBSP)		TSA	https://www.tsa.gov/for-industry/electronic-baggage-screening	Public
TSA NEDCTP Canine Training & Evaluations Branch		TSA NEDCTP	https://www.dhs.gov/keywords/national-explosives-detection-canine-team-program	Public
TSA Planning Guidelines and Design Standards for Checked Baggage Inspection Systems	September 2017	TSA	https://iabsc.org/pgds/	Public

Document Name	Issue Date	Issued By	Website	Availability
TSA Planning Guidelines and Design Standards for Checked Baggage Inspection Systems	September 2017	TSA	https://www.fbo.gov/spg/DHS/TSA/HQTSA/TSA25-04-03026/listing.html	Public
Video surveillance standardization activities, process, and roadmap - ERNCIP Thematic Group Video Surveillance for Security of Critical Infrastructure	August 2016	European Commission	https://ec.europa.eu/jrc/en/publication/video-surveillance-standardisation-activities-process-and-roadmap-erncip-thematic-group-video	Public
Video Surveillance System Standard for Buildings	November 2013	Singapore Police Force	https://www.police.gov.sg/~/media/05398B3543CD4A97B8D6422B9E595A1B.ashx	Public

APPENDIX A: CAMERA SYSTEM DECISION MATRIX

The below table provides sample criteria that may be used to determine whether to plan for camera system optimization, upgrade, expansion, or replacement. This list may be expanded and altered to suit the airport's anticipated change criteria and specific needs.

Criteria	Action Recommended?	Action	Advantage	Disadvantage
Camera End of Life	Yes	Replace camera **(Replacement)**	* Possible new technology introduced	* New camera capabilities may not be fully supported by existing VMS
	No	Do nothing **(Leave As-Is)**	* No additional costs	* Camera will not be supported by manufacturer * Camera may eventually need replacement
Increased Camera Field of View Coverage Required	Yes	Replace existing camera lens with greater field of view **(Upgrade)** or Replace existing camera **(Upgrade)**	* Utilize existing camera and infrastructure or * Utilize existing infrastructure to support new camera	* Cost to replace the lens * New camera may require additional VMS storage
	No	Do nothing **(Leave As-Is)**	* No additional costs	* New camera field of view will not be achieved
VMS Firmware Out of Date	Yes	Update firmware **(Optimization)**	* VMS will continue to perform efficiently * May provide new manufacturer technology not previously available * System will continue to be supported by value-added reseller	* Update could affect existing performance and behavior * Update cannot be rolled back once installed * May be required by manufacturer for continued support
	No	Do nothing **(Leave As-Is)**	* System will continue to operate as normal	* System may not work as efficiently * Latest technology from vendor will not be available * System will eventually become outdated or unsupported

Criteria	Action Recommended?	Action	Advantage	Disadvantage
New Asset / Functional Requirement Requires Monitoring	Yes	Add camera to accommodate new asset **(Expansion)**	* No local guard required	* Additional cost
	No	Do nothing **(Leave As-Is)**		* Local guard required * Additional costs