MEMORANDUM

Date: April 3, 2018

To: Security Committee

From: Jeffery Werblun, Security Chief

Subject: Summary of the Security Department Assessment and District Security Camera Strategy by Burns & McDonnell, Dated December 4, 2017

RECOMMENDED ACTION

Review summary – no recommendation.

BACKGROUND

The District retained Burns & McDonnell, Inc. (Burns & McDonnell), to conduct an assessment of the Security Department and assist in developing a Security Camera Strategy. The two (2) areas the assessment was intended to focus on are: 1) to evaluate the District's Security Department and provide recommendations regarding the operational and/or administrative improvements and suggest possible reorganizational and operation changes; and 2) to evaluate the current CCTV/camera strategy and create a new strategy for the District to implement.

Burns & McDonnell prepared their report with the agreement that the report be made available only to the District. Due to the sensitivity/confidentiality of information in the report, such as camera locations, staff scheduling, and operations, a summary is being provided to the public.

PROJECT SCOPE AND APPROACH

The District requested that Burns & McDonnell carry out two (2) primary tasks: 1) perform an assessment of the Security Department, and 2) evaluate and provide options for a District-wide Security Camera Strategy. Under the first task, assessment of the Security Department, the primary goal was to evaluate the current operations as they pertained to staffing, patrols, gate security, and administrative functions. The overall goal was to provide recommendations for operational and organizational improvements to address the current and anticipated future needs of the District.

The second task – assessment of the District's Security Camera Strategy (SCS) – consisted of identifying the current use and deployment of security cameras used by the District. The overall goal of this task was to identify and recommend options for the deployment of a new SCS that would assist the District in creating a force multiplier for the Security Department and enhancing their capabilities.

The District added a request for Burns & McDonnell to conduct a town hall meeting. The meeting was held on February 23, 2017. The main objective was to create a forum for the residents to provide feedback to the Burns & McDonnell team about security related concerns and any security related procedures or operational practices that they would like to see added, modified, or removed.

In addition to the town hall meeting, Burns & McDonnell was asked to develop a security survey that residents could complete online or manually complete and submit. The deadline for completing the survey was Friday, March 17, 2017. The meeting and survey assisted Burns & McDonnell in identifying the cultural environment of the District, the resident perspective and expectations of the security program and other special considerations that the Burns & McDonnell team may need to take into consideration during the evaluation. (See Appendix A Security Survey Results)

About 440 of approximately 5,500 residents, (about 8%) responded to the survey. Assuming each survey was submitted by a unique user, this statistically provides an approximately 95-99% confidence level with an approximately 6% margin of error for the District.

While this survey was not intended to provide a scientific indication of the perception and expectations of the security program, it was intended to provide a glimpse into desires and perspectives of the security measures and services questioned. After the town hall meeting, Burns & McDonnell concluded that most of the concerns from the residents that attended the meeting were centered on the lack of traditional law enforcement capabilities of the Security staff.

After analyzing the information obtained from the surveys, town hall meeting, and conversations with Rancho Murieta stakeholders, Burns & McDonnell concluded that residents may not be fully aware of the capabilities and areas where Security staff do and do not have authority. Some residents were unaware that the Security Patrol Officers did not have police powers, while others were concerned that Security Patrol Officers lack police powers. Many residents who responded to the survey or spoke out at the town hall meeting believe that the Security staff can and should respond to any security related incidents and handle accordingly.

Despite these misconceptions, District policy states that Security Officers are to “observe and report” incidents that they (the officers) are unable to prevent or mitigate. District Officers are not authorized to “respond” to incidents that should be handled by law enforcement or other emergency responders. For example, if a domestic violence incident is reported, Security Patrol Officers are to refer the matter to SSD, according to the Security Operations Manual.

Security measures (e.g. technology, policies, procedures, rules and regulations) – including future security enhancements – on property not owned by the District (e.g. homeowners association (HOA), Rancho Murieta Country Club (RMCC), commercial, hotel, and industrial areas) are the responsibility of the respective property owner. Without an authorizing agreement with the property owner, the District cannot implement security measures such as traffic or speed controls (e.g. speed bumps or signs), security camera installation, or security lighting on private property.

Each entity within the community maintains its own staff, property boundaries, and establishes its own rules and regulations. Entities may have varying sets of rules or levels of enforcement of those rules. Rancho Murieta Association (RMA) pays the District a fee for the enforcement of non-architectural Covenants, Conditions & Restrictions (CC&Rs) designated by RMA. This includes enforcement of overnight and driveway parking regulations. No other agreements with other HOAs were identified that would allow for the Security staff to enforce rules, regulations, ordinances, or CC&Rs outside of RMA or the District.

The District is responsible for providing some municipal services (e.g. water treatment, waste water collection), the RMA maintains ownership of most roads within the District, as well as parks, and the North Gate. The District collects a special tax to provide for security services including staffing the North and South

Gates, performing security patrols, and non-architectural and CC&R enforcement. A one-time security impact fee is also imposed on new developments to support and improve the provisions of security services to the community through the procurement of technology, facilities, and physical assets with the goal of protecting people and property. This fee can only be used for capital improvements for the security program and cannot be used as part of the general security fund, or to pay for operations and maintenance costs.

The Security Department's annual budget, which is funded in part by the Security Special Tax (paid by residents), is capped at 2% increase per year. Any increase beyond 2% would require a 2/3 majority vote of the District residents. Based on the maximum increase in the Security Department's budget that can be authorized by the Board, Burns & McDonnell is concerned that continued funding of even the existing operations of the Security Department may not be possible as the anticipated District growth occurs.

California passed into state law, effective January 1, 2017 a minimum wage increase on a yearly basis across all industries. The District may be exempt from the mandatory increase called out in the new minimum wage law; however it cannot avoid the impact the increases have on the labor market. If the District's 2% cap on budget increases limits the pay increases to the same level, current or future security officers may elect to work in another industry that may offer increased wages and the Security Department may not be able to meet the security demands or requirements of the District. Burns & McDonnell learned in interviews that benefits afforded by the District are considered superior when compared to other private security. However, it is the experience of Burns & McDonnell that personnel in similar occupations are normally not attracted to these jobs or entities for the afforded benefits. Instead, personnel in these professions are normally interested in take home wages for financial obligations. Security Patrol Officers will maintain a pay rate higher than the state minimum wage; Security Gate Officers would not match the minimum wage until after approximately eight years of service, based on the Security Departments annual 2% budget increase.

SUMMARY FINDINGS

The following is a summary of findings by Burns & McDonnell regarding the Security Assessment and Camera Strategy report. This is a summary of their findings and comments if we agree or disagree with their findings.

1. Residents do not have a clear understanding of the enforcement capabilities of the security staff. This can lead to misconceptions of the Security Patrol Officers' responsibilities and authority of the security officers. ***We agree with this statement***.

2. Security Officers perform duties that are not authorized by the District which is in reference to assisting other law enforcement agencies within the boundaries of the community or outside the community. At the time the survey was conducted part of these statements were true however, since then, the District's policy has been reinforced and is being adhered to where Security Officers do not engage in law enforcement activities or take law enforcement action. In certain limited circumstances Security Officers do assist law enforcement agencies such as traffic control at accident scenes but they are not directly involved in any law enforcement action.

3. Because the community is comprised of different HOAs and non HOA areas within its boundaries, Security Officers cannot enforce rules, regulations, ordinances or non-architectural CC&Rs throughout the entirety of the District. ***We agree with this statement*** and currently RMA is the only HOA that security has an agreement with to enforce certain CC&Rs.

4. The enforcement policies and procedures for Security are not clearly defined for all enforcement related activities. ***We do not agree with the statement***. The policies are clearly defined in the Security Operations Manual.

5. Security Gate Officers are overtasked and may not be able to efficiently or effectively perform all duties expected of them. ***We do not agree with the statement***. Although Gate Officers can get busy, they are trained to handle one vehicle at a time to ensure that the guest or vendors are properly checked in before they are allowed through the gate. They are also trained to prioritize their workload which includes phone calls, radio traffic, and vehicles in the visitor lane.

6. Current Staffing levels for the Security Patrol Officers may not allow for efficient security coverage of the District during the anticipated growth. ***We agree with the statement****.*

7. There is a disparate security camera system deployed on community property. The systems are not integrated and do not provide remote viewing capabilities for Security personnel. ***We agree with the statement***. The camera system at the South Gate has been upgraded and provides better coverage for the vehicle lanes at the South Gate, similar to what is in service at the North Gate. There are several different camera systems at various locations on community property.

8. The current camera systems deployed on District owned property does not allow for efficient security operations and may increase the operation and maintenance cost for the individual systems. ***We can neither agree nor disagree with the statement*** at this time. The costs are unknown at this time. If there was a capability of remote viewing of all of the camera systems on community property that could make operations more efficient, but may also require additional staffing to actively monitor additional cameras.

9. The District does not have detailed policies and procedures documented that would be vital to the planning, procurement, installation, operation and maintenance of a security camera system. ***We agree with the statement***. A District-wide system, although it has been studied, is not in operation; therefore there are no policies and procedures documented regarding those systems.

10. Non-District owned camera systems are not accessible by Security staff and this does not allow the Security Department to maintain effective situational awareness of properties within the District. ***We agree with the statement****.*

Summary of Recommendations

This section is a general overview of the major recommendations by Burns & McDonnell. Further recommendations are discussed in greater detail in the subsequent sections of the report.

1. The capabilities and authority of the Security staff should be documented and clearly communicated to the residents of Rancho Murieta. This may alleviate any misconceptions of the capabilities of the Security Officers.

2. Security staff should receive regular policy and procedure training explaining their authorized response capabilities.

3. Establish an agreement with the entities within the District that allow the Security staff to enforce security related rules, regulations, etc. throughout the entire District. This may allow for enforcement capabilities and procedures to be more efficient.

4. Establish and clearly document that the enforcement policies and procedures for the authorized enforcement activities of the Security staff. Agreements between the District and varying entities should also clearly state in detail the authorized rules, regulations, ordinances, or CC&Rs that can be enforced by the Security staff.

5. Utilize technology at the North and South Gates to assist Security Officers in the execution of their duties. This can include the implementation of a web-based visitor management system or shifting the issuance of bar code stickers to another department. Gateaccess.net has been implemented.

6. Plan for corresponding increases in Security staff levels as the development of commercial and residential areas occur.

7. Update the security camera systems deployed at District-owned property. A single vendor should be utilized to maintain consistency. These systems should also be integrated to allow the Security staff to view live or recorded footage on District-owned property. The South Gate camera system has been updated.

8. Establish minimum technological standards for the security camera system. This would allow the systems to be integrated, allowing for a more efficient operation. Detailed policies and procedures regarding the operation and maintenance of the system should also be developed.

9. The minimum technological standards along with the policies and procedures should be completed in coordination with the varying entities within the District. This can allow for the camera systems installed on private property to be viewed by the Security staff. This may allow for more efficient security operations by allowing Security staff to evaluate a possible security related incident remotely in order to initiate an appropriate response. This may allow the Security staff to provide a higher quality of service to the community.

SECURITY PATROL OFFICER DUTIES

A Security Patrol Officers' primary duties include "protecting lives and property by seeking to prevent an incident or offense from occurring in the District. In situations where prevention of an incident or offense is not possible, the function of Security Gate Officers or Security Patrol Officers is to observe and report the incident to a law enforcement agency."

The District's Security Department currently provides staffing 24/7/365 at two (2) stationary posts and one (1) mobile patrol with a staff of 16 proprietary Security Officers, not including the Chief. When a crime incident occurs, Security Patrol Officers and Security Gate Officers are to observe and report the incident to law enforcement, as appropriate. District Officers are not law enforcement officers and are not responsible for any law enforcement activities, including but not limited to:

- Enforcing state or local laws (including traffic laws).
- Chasing, apprehending or detaining persons.
- Criminal investigations.

Security Officers' duties include, but are not limited to, staffing the security gates, patrolling of all areas within the boundaries of the District, keep a log of daily activities, responding to calls for service, enforcing non-architectural CC&Rs, and writing detailed incident reports. Security Gate Officers and Security Patrol Officers also monitor a communication system to maintain contact with emergency services and the appropriate entities within the District.

Security Patrol Officer duties include the enforcement of non-architectural CC&Rs. To allow for this activity, the District has established an agreement with RMA that authorizes Security Patrol Officers to conduct ten (10) hours a month of CC&R enforcement of overnight street and driveway parking. Security Patrol Officers are authorized and assigned the responsibility to enforce any non-architectural CC&Rs, covered under Government Code 61105 (e), as well District Resolution 2005-17. Security Patrol Officers are authorized to issue Notice of Violations (NOV) for stop sign violations and speeding violations. Security Patrol Officers are not authorized to conduct traffic stops.

The roads inside the North and South Gates are owned by the RMA, yet traffic enforcement was not identified in the agreement between RMA and the District, except for overnight parking and driveway parking. RMA employs a full time Compliance Officer responsible for enforcement of architectural and non-architectural RMA CC&Rs, including the CC&Rs enforced by the Security Patrol Officers.

SECURITY CAMERA STRATEGY

An effective security camera program is meant to enhance the capabilities of the overall security program of any entity. The program requires a collaborative effort between the Security, Management, and Information Technology (IT) personnel.

An efficient and effective security camera system requires both initial and ongoing investments. It can positively impact the community's sense of security by allowing Security staff the ability to remotely evaluate and document areas where incidents occur and in effect detecting, assessing, and initiating the appropriate Security Patrol Officer response to incidents without being physically present. Camera systems also preserve a visual record of events to assist Security personnel, law enforcement, or other entities during an investigation. Accordingly, a system, as a record of incidents, can help to provide helpful information useful in evaluating potential liability claims.

A video management system should be capable of integrating with alarms or other systems to allow the integrated systems to annunciate and display information on a single computer workstation. This approach incorporates the need for timely identification, assessment and the initiation of the Security Patrol Officer response to incidents by the appropriate personnel.

With the exception of the North Gate, Rancho Murieta currently has disparate security camera systems deployed at the South Gate, Waste Water Treatment Plant, Water Treatment Plant (Plant), Rancho Murieta Village (MVA), and at various parks (RMA) within the community. The systems in place use a variety of hardware, cameras, various recording devices, software, are owned by different entities, and do not converge or integrate with one another in a centralized location.

Cameras located at the North and South Gates assist in maintaining a visual log of vehicles that gain access into the gated community. Cameras record the vehicles' license plates using license plate readers (LPR) as they

enter and exit the community. Cameras also show vehicles leaving the community. Officers, however, are unable to view video feeds from the other gate (e.g. North can't view South and vice versa).

PARKS

The assessment team conducted site visits to the various parks within the community. Security cameras were identified at RMA's Riverview Park, Stonehouse Park, and at the Gazebo. The assessment team was unable to identify the operational status of any of these cameras. The assessment team determined that these cameras are not owned by the District, but are owned and maintained by RMA. They were not able to determine if the cameras were operational or who to contact regarding the cameras at RMA. Documentation received by the Security team describes the location of the recording devices for these cameras but does not indicate if the cameras or recorders were operational. Security staff is unable to view footage from these systems which denies them the ability to initiate an appropriate Security Patrol Officer response to a security incident or other event.

SECURITY DEPARTMENT RECOMMENDATIONS

Typically, in the political subdivision environment, security program components that impact the entire organization (e.g. security policies, procedures, technology) would be managed at the organizational level and appropriately fall under the jurisdiction and budget of that entity (City, County, etc.). Efficiencies in security spending and improvements in security operations are gained by making strategic, scale based decisions and leveraging that spend across organizational sub-units in a way that maximizes the cost versus benefit equation. Threat and risk information is collected from various parts of the organization, and that centralized Security Department is able to assess the entire threat picture.

However, while that approach applies in most political subdivision environments, the structure of the Rancho Murieta and the entities within District boundaries is somewhat unique. Each entity is its own private organization and not a subordinate unit of the District. In the context of the overall District boundaries, there is very little real property that is actually owned by the District, and this is the only area where District Security Officers have statutory jurisdiction. The roads, public gathering spaces, and even one of the vehicle gates are all privately owned property. Each of these private organizations is free to establish their own rules and policies, to engage in contracts and agreements with other entities, and to otherwise operate as they deem appropriate (in the context of staying within the boundaries of the law).

Addressing security related concerns is, therefore, the legal and functional purview of each private owner. In the case of the entities and territory within District boundaries, differences in policies, the enforcement of those policies, and even the prioritization and expectations of the respective populations can vary significantly from one privately owned section of the District to another. For example, RMA may establish or prioritize rules regulating traffic, parking, the conduct of association members, and similar concerns. While these rules are certainly within the purview of RMA, they may be different than those established by Rancho Murieta North (RMN), RMCC, or MVA. As private organizations, it is up to each entity to determine – and enforce – their own rules and regulations.

In the opinion of Burns & McDonnell, if security management decisions, rules, and adjudication procedures were consolidated into a single entity (similar to a security department in a city or county), overall program management would become more effective and the cost of implementing security measures could be more efficiently applied. However, while such an approach would likely have a positive impact on the overall security posture, the security benefits of such a consolidation would negate many of the intrinsic benefits of living within a rural community services district (CSD) (as opposed to a city). Burns & McDonnell is also of the

opinion that such a move would likely have very little support from the community (and the private organizations within it).

The authority of a properly licensed security officer is vested in the authorization from the owner of the property to the security officer to act on the owner's behalf in protecting the property. As mentioned above, some of the organizations within District boundaries have established an agreement with the District to enforce some of their rules. With RMA for instance, agreements authorize District Security Officers to enforce non-architectural CC&Rs and RMA Gate Policies. At least one entity, Rancho Murieta Village, has an agreement that authorizes the District to provide security services under the Security Services Code, but neither the reviewed agreement nor the Security Services Code specifies details on what rules are to be enforced or prioritized, how such rules will be enforced, how identified violations will be adjudicated, or other such matters. Many of the entities within District boundaries (e.g. RMN, Villas, and Country Club) have no such agreement with the District (or an agreement was unable to be located or produced during this project).

Burns & McDonnell recommends that the District establish agreements with each entity (HOA, etc.) within District boundaries that authorize the District Security Officers to enforce the rules of that entity through the issuance of NOVs, similar to the existing one with RMA mentioned above. Each agreement should clearly identify the specific rules, actions, and expectations of each party.

Burns & McDonnell further recommends that the District lead an effort to work with all of the entities to develop a set of standardized rules and procedures for adjudicating violations within District boundaries. If successful, this standardized set of rules would assist in the fair and consistent application of enforcement efforts, may alleviate confusion caused by differing guidelines, and would likely improve the perceptive effectiveness of the security program.

For example, it is conceivable that the District would pursue and establish an authorizing agreement with the commercial property owners (or a subsequent commercial property association that the owners are members of) to extend District security services to their respective properties. The observe and report expectation should be clearly defined in such an agreement(s) to remove any confusion as to whether District Security Officers can or should engage in calls (e.g. shoplifting or public intoxication).

It was identified that Security Patrol Officers are authorized to enforce any non-architectural CC&R for the RMA, covered by Government Code 61105 (e), as well District Resolution 2005-17. However, this authorization was not clearly identified, but is considered "all-encompassing" by the Government Code 61105 (e) and District Resolution 2005-17. Burns & McDonnell recommends that the enforcement policies and procedures for CC&R violations should be clearly defined; including which CC&Rs can be enforced by Security Patrol Officers and appropriate procedures for enforcement.

SECURITY GATE OFFICERS

Burns & McDonnell recommends that the current visitor registration process used by residents be transitioned to a web-based pre-registration service. ***Gateaccess.net has been implemented***.

Burns & McDonnell recommends that the District work with RMA to adjust gate policies to include the recommended pre-authorization process and identification requirements. Additional information can be added, depending on the level of verification that may be desired (e.g. vehicle make/model, phone number). The use of this system could be utilized for vendors, contractors, or other service providers. If a resident is

expecting a service provider or contractor, the resident could input the data into the system. When the company providing the service arrives at the gate, the Security Gate Officer would check the service company's employee identification (government or company issued) and record that information. This may assist in maintaining consistent access logs and allow the security staff to trace an individual back to a company if an incident were to occur. While this same process may not be plausible for parcel delivery services (i.e. USPS, UPS, FedEx), it is suggested that the Security Gate Officers maintain an access log for these as well for the same purpose as other service providers.

The use of technology is assisting similar entities in optimizing security operations while also providing a more comprehensive record keeping system that can be referenced quickly when needed. Visitor management software has been developed for HOA based communities similar to the District to allow entities to quickly and accurately maintain visitor access records. The current visitor process, if completed properly, has the potential to overtask the Security Gate Officer and may result in unreliable logging or processing procedures (e.g. license plate log, vehicle passes issued, activity logs) or the neglect of other assigned duties (e.g. dispatch, monitor phones).

Commercially available software can maintain vehicle registration information, scan driver licenses of visitors, and even issue vehicle passes. Most systems available have web-based input portals to allow for resident interaction. Other features available include integration with LPR software, analytical modules to evaluate traffic patterns, and automation features (e.g. license plate based gate entry) that may allow for officers to dedicate time to other security tasks.

As discussed, RMA passes are issued to visitors entering through the gates. No record is kept of what pass was issued to which visitor and the passes are easily duplicated. Burns & McDonnell recommends that the District work with RMA to develop a more secure permit process that contains, at a minimum, the following components:

- The verification of authorized access / resident/visitor information.
- The logging of authorization type and duration.
- The logging of vehicle access time and destination.
- Vehicle and registration (plate) information.
- Driver information (name).
- Vehicle pass information.

The registration process of resident vehicles and the assignment of barcode decals appear to be inefficient and time consuming for both residents and Security Gate Officers. The residents are required to visit multiple locations to complete registration and receive a decal. This process can distract Security Gate Officers from other duties and reduce the effectiveness of gate security. Burns & McDonnell recommends that the District work with RMA to consolidate the issuance and installation of vehicle barcode decals to RMA staff allowing Security personnel to dedicate more time to security duties.

Following this concept, when a resident registers a vehicle, they would immediately receive a barcode decal without needing to visit the South Gate (where they currently have their information re-verified by the Security Gate Officer).

Burns & McDonnell recommends that the North and South Gates be networked together for remote operation to allow for staffing adjustments at the South Gate during non-peak hours when necessary. The Officer at the North Gate would have the ability to remotely view, communicate, and authorize with visitors at the South

gate via video phone (similar to the technology installed at the North Gate). The visitor management system recommended earlier in this section would allow the Officer to input or verify information already populated in the database. Burns & McDonnell does not recommend that the District eliminate in person coverage at the South Gate at this time, but establish the technological capability of doing so in the future if security requirements or staffing levels warrant.

SECURITY PATROL OFFICERS

The District is expecting significant growth within the next 10-15 years, including commercial (e.g. hotel, grocery and other retail, restaurants) and residential development (approximately 1,500+ additional lots). Assuming the District is authorized by the respective owners of these developments to provide security services, the increased demand may strain existing security resources. As the demand for security increases, the quality and effectiveness of those services will likely demonstrate a corresponding decrease without additional resources or efficiencies being created. As the expected developments (identified above) mature, the increased demand for security services will require additional staffing to perform the same level of service as present. Accordingly, Burns & McDonnell recommends that the District plan for corresponding increases in Security staff levels as the development of commercial and residential areas occurs. Based on current security duties and the expected growth, two (2) Security Patrol Officers assigned to each shift are a reasonably assumed minimum service level (allows for two (2) continuous roving patrols of the area or one (1) patrol simultaneous to a call for service). Adjusting staff levels to allow for two (2) Security Patrol Officers per shift would require an additional four to five (4-5) Security Patrol Officers.

Burns & McDonnell understands that such an increase in staffing would require significant budgetary change and recommends that the increase corresponds to the increase in population and commercial developments. For example, providing an additional Security Patrol Officer during peak hours is a natural first step that prevents overstaffing and allows the staff level to increase as the demand increases.

SECURITY CAMERA STRATEGY

As requested by the District, Burns & McDonnell developed three (3) Security Camera Strategy options for consideration by the District. The strategies provide various options for coverage of areas within District boundaries and the viewing / operational capabilities of District Security personnel for systems installed on property the District does not own. The options describe the progression of increased capabilities and integration of the system for use by District Security staff. System standard recommendations remain consistent with the three (3) options.

The District previously developed a Security Camera Implementation Plan in 2015; however, this document does not provide information that would be considered vital to the planning, procurement, installation, operation, and maintenance of the system. Burns & McDonnell recommends reviewing the 2015 Plan and creating additional policies and procedures for the implementation of a video management system capable of receiving footage from District owned and non-District owned cameras that meet specific minimum technological standards. Aspects that should be considered include but are not limited to:

- System Requirements
- Video Management Software
- Video surveillance system hardware (minimum requirements for server)
- Length of recording time (e.g. 30 days)
- Resolution of recording and live viewing

- Frames per second of recording
- Motion-activated recording vs. continuous recording
- Video analytics requirements (License Plate Recognition)
- Camera requirements
- Dome vs. Box Cameras
- Fixed vs. Pan-Tilt-Zoom vs. 180 and 360 Degree Panoramic Cameras
- Camera resolution (Megapixel, VGA)
- Day/Night and wide dynamic range options
- Authorized users and administrators
- Authorized use of the system
- Vendor

Policies and procedures for the operation of the system should be drafted prior to the procurement of the components necessary to implement the system. This should be accomplished to allow the District to define the objectives of the system including operational capabilities, end-user functionality, areas of coverage, fields of view, etc. This will assist in the development of a Request for Proposal (RFP) and communicating the needs to the vendor responsible for the installation.

A single vendor should be utilized for the acquisition and installation of a security camera system. By doing so, the District will be able to maintain a steady level of standards regarding the type of hardware used and the installation of those components. This can minimize the risks of components being installed inconsistently, or various products being used which can allow for a reduction in costs for the procurement of hardware and software, installation, and maintenance.

The security camera system would optimally be connected via a dedicated fiber optic cabling infrastructure that is currently available throughout the community. A dedicated network for the camera system would allow the District to implement a system with a dedicated pathway and bandwidth, minimizing possible interference from other systems using the network and optimizing system operations. Fiber can allow for the security camera system to transmit data over a dedicated communications line, minimizing latency issues.

Burns & McDonnell recommends that a phased approach be taken with the implementation of a new surveillance system since it will require a significant investment from the District.

Option 1: Stand Alone System for District Owned Properties

Option 1 requires the District to replace the existing stand-alone video recorders with a centralized video management system for District-owned properties. This system should provide live or recorded viewing capabilities from a remote location (e.g. from the North or South Gates, Security Office, patrol vehicles).

The North Gate is equipped with the most recently installed system (software and hardware) in the District. Burns & McDonnell recommends that the District consider installing an upgraded system and components similar to, and compatible with, the system installed at the North Gate.

Currently, systems in use at the various District facilities are stand-alone systems that do not have the ability to be integrated with one another and do not offer remote viewing. This does not allow Security staff to efficiently review video footage from these locations and may cause an increase in overall operations and maintenance costs, as each system must be individually maintained. An enterprise level system would give the

District the ability to provide security staff with remote viewing capabilities and extract recorded video footage without having to visit the specific location where the camera (or recorder) is installed. The District would apply updates and maintain the system from a single location rather than at those individual locations, minimizing associated operation and maintenance costs and the time required.

The system should be configured with video analytic software that detects motion and provides notification to Security personnel. Live monitoring is not anticipated or required, and such notifications would assist Security with initiating the appropriate response as early as possible. When motion is detected, the system provides automatic notifications to Security personnel and provides an option for live viewing or the review of recently recorded footage. This allows security personnel to remotely assess a situation and initiate a response if necessary, in many cases without requiring a dispatched Security Patrol Officer.

Burns & McDonnell recommends that security camera coverage around District-owned properties include perimeter coverage, access points leading from exterior to interior, parking lots entrances, vehicle or personnel gates, and exterior assets. This coverage may provide the District sufficient camera coverage, minimizing blind spots, and providing the Security staff with enhanced situational awareness, assessment and response capabilities.

Option 2: Stand Alone Systems Integrated into District Operation

Option 2 involves the District and the other property owners (HOAs, RMCC, and hotel) to install and maintain their own systems, while allowing access to District Security for live or recorded viewing capabilities. Burns & McDonnell recommends that the District coordinate closely with the various property owners to standardize system software and hardware components. This allows the District and property owners to easily add or adjust components to meet future needs while maintaining the ability to integrate with the system. This also allows changes to be made to benefit the entire system (e.g. additional data storage, software upgrades, etc.) in lieu of upgrades to individual systems or purchasing multiple components for each individual system in use. Similar to Option 1, a security camera system and components that are similar to those used at the North Gate is recommended.

As technology continues to advance, up-to-date system components could be utilized, however, the District and participating entities or property owners should confirm that these systems are backwards compatible and can be integrated with the system in use presently. Individual components (e.g. video recorders, cameras, etc.) can be installed as older components fail or can no longer be serviced. This allows the District and other entities to phase-in improvements and spread out expenditures.

Future tenants of the retail developments (i.e. chain stores) may already have a security camera strategy in place that will be used for future locations and these entities may wish to deploy the same strategy at properties established in the District. Prior coordination should be conducted with the developer and any possible future tenants to define each party's responsibilities for providing security camera coverage. Burns & McDonnell envisions that the District will be responsible for providing security coverage of public areas (e.g. parking lots, sidewalks). Cameras in these areas should be able to provide video footage of any vehicles entering or exiting the parking area to include vehicle make, model, color, license plates and possibly occupant descriptions. Side walk cameras should provide images that would allow for adequate subject description and possibly identification.

Depending on the future agreements with private property owners and possible desire or need for Security Officers to have access to these systems, the District should provide documentation about the standards for the system. This will allow for private property owners to install a system that is compatible with the District system while allowing the Security staff to view recorded or live video feeds. This access would allow Security staff to conduct remote assessments of situations to determine the appropriate response. An enterprise camera system would allow the residents and various businesses to rely on a more capable Security Department, allow for a consistent response, and assist with more efficient situational awareness.

Option 3: Live Monitoring Capabilities

Option 3 involves the District and various property owners installing a system like that discussed in Option 2, however, the Security staff would provide live monitoring capabilities. This requires an increased investment by the District and participating entities for monitoring staff as well as additional hardware, software, and the dedicated space for live monitoring. This allows the District to provide increased situational awareness in areas where the systems are installed and requires less time to identify security concerns while increasing the possibility of mitigation through more effective assessments and response initiation. The Security staff manning this post would also be able to perform other duties, such as acting as dispatch, receiving calls for service, maintaining logs and other administrative duties. This could allow the Security Gate Officers and Security Patrol Officers to dedicate attention to other security related duties, increasing proficiency, accuracy, and providing a higher quality of service to the community.

Nine (9) additional staff may be necessary to provide live monitoring 24/7. Studies have shown that for active monitoring to be effective, approximately 12-16 video feeds can be simultaneously viewed by a single person. This is assuming the operator's involvement in other low activity tasks. This is also without the use of video analytics that assist in automating the process and provide alarms and notifications to the monitoring individual. Studies for security camera feed per operator ratio have been conducted, but due to the relatively recent emergence of this technology, data is inconclusive. At least two (2) Security personnel would be required for each shift to effectively monitor camera feeds, complete other assigned tasks, and to allow for breaks. Monitoring personnel must be able to divert attention away from monitoring camera feeds to remain effective. After 12 minutes of continuous video monitoring an operator will often miss up to 45% of screen activity, after 22 minutes of viewing, up to 95% is overlooked. The table below represents the possible shift structure for monitoring personnel.

However, the assessment team believes that because of the very low threat environment and rare occurrences of incidents that may require this level of security, live monitoring may not be cost beneficial to the District. As the community grows, if the level or types of incidents changes, additional analysis may be needed to re-evaluate this option. If a system is installed as discussed in Option 1 and Option 2, this would allow the District to quickly create a space for live monitoring while minimizing costs associated with integrating the system with the monitoring center.

POSSIBLE SECURITY CAMERA MONITORING SHIFTS

(See attached table 2 at the back of this report for staffing example S/O is representative of Security Officer).

RECOMMENDATION

Burns & McDonnell recommends that the District utilize Option 2. This option allows Security staff to provide a higher quality of service to the community through enhanced situational awareness and assessment capabilities, and more efficient response initiation. The new system would provide more effective investigative

capabilities for the Security staff or local law enforcement through higher video quality and increased areas of coverage. As discussed above, Security staff would have the ability to receive notifications of abnormalities in the area(s) outside of the normal hours of use through video analytics. This may allow Security staff to provide an increased assessment and response capabilities, minimizing the impact a possible incident may have on the area or community.

Cost information in a Rough Order of Magnitude (ROM) format is also presented in Appendix B to assist the District with financial planning to allocate the appropriate resources during the upgrade. Please note that actual costs may vary dependent on the timeline the improvement is completed as well as the brand, model, hardware, and version of software used. A ROM was not provided for Option 2, as it depends on which property owners participate in the collaborative strategy.

Table 2: Possible Security Camera Monitoring Shifts

Shift	Saturday	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday
0600-1400	S/O 7	S/O 7	S/O 1	S/O 1	S/O 1	S/O 1	S/O 1
	S/O 2	S/O 2	S/O 2	S/O 2	S/O 2	S/O 7	S/O 7
1400-2200	S/O 8	S/O 3	S/O 3	S/O 3	S/O 3	S/O 3	S/O 8
	S/O 8	S/O 8	S/O 4	S/O 4	S/O 4	S/O 4	S/O 4
2200-0600	S/O 5	S/O 5	S/O 5	S/O 5	S/O 5	S/O 9	S/O 9
	S/O 6	S/O 9	S/O 9	S/O 6	S/O 6	S/O 6	S/O 6

Table 3: Strategy Activity Timeline

Activity	Description
A	Develop a committee tasked with the development of the overall strategy based on the desired system capabilities and goals. The committee should involve primarily, if not exclusively, District employees to assist with optimizing the planning process. This committee should be headed by the Security Department, which should be the primary owner of the system.
B	Committee begins development of overall goals of the strategy. This should begin with the general needs and wants of the District and may include but is not limited to the following: o Amount of coverage/areas to be equipped with security cameras o Desired capabilities of the system. o Capabilities should be compared to the staffing levels and the system's ability to create a force multiplier to better assist the Security Department in the execution of duties. This should also be based on the if the system will have active, passive, or a combination of both monitoring by the security staff. o Should include video analytics, storage requirements, and end user capabilities.
C	Identification of Information Technology (IT) infrastructure needed/available to support information gathered in Activity 2. This information should be substantiated by a 3rd party to avoid any conflicts of interest with products or services.
D	Identification of sources for financial resources available over the next 1-5 years. o The timeline needed to complete the implementation of the Strategy will be dependent on the final Strategy chosen.
E	Development of RFP for the construction or installation of the necessary supporting IT infrastructure for the Strategy. o RFPs should be gathered for the installation of fiber, microwave, or other wireless technologies. Develop RFPs for the procurement and installation of the security camera system. o RFPs should also specify the requirement for a Master Service Agreement, including regularly scheduled service or maintenance and software updates.
F	The Committee briefs the Board on the estimated costs for the installation of the new Strategy to begin the appropriate allocation of resources over the course of the implementation timeline. o While a ROM for the installation of the system components, actual costs may vary dependent on the brands and models of the hardware and software used.
G	Develop implementation timeline for the construction/installation of supporting infrastructure. o This can be phased in over the course of the project.
H	Development of time line for the installation of Strategy components.
I	Begin phased construction and installation of infrastructure and Strategy components.