UNIVERSITY OF CALIFORNIA, SAN FRANCISCO
AUDIT AND ADVISORY SERVICES

Security Services Review
Project #19-050

December 2018

University of California
San Francisco

Audit & Advisory Services
UCSF Box 0818
1855 Folsom Street
San Francisco, CA 94143
tel: 415.476.3851
fax: 415.476.3326
www.ucsf.edu

December 17, 2018

Kevin Pattison
Vice President, Supply Chain and Support Services
UCSF Health

SUBJECT: Security Services Review
Project #19-050

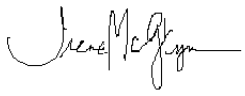
As a planned internal audit for Fiscal Year 2019, Audit and Advisory Services (A&AS) conducted an audit of the internal controls in place for video surveillance at UCSF Health (UCSFH). The purpose of this review was to evaluate the controls in place for effective and efficient video surveillance operations at UCSFH.

Our services were performed in accordance with the applicable International Standards for the Professional Practice of Internal Auditing as prescribed by the Institute of Internal Auditors.

Our review was completed and the preliminary draft report was provided to the department management in November 2018. Management provided us with their final comment and responses to our observations in December 2018. The observations and corrective actions have been discussed and agreed upon with department management and it is management's responsibility to implement the corrective actions stated in the report. In accordance with the University of California audit policy, A&AS will periodically follow up to confirm that the agreed upon management corrective actions are completed within the dates specified in the final report.

This report is intended solely for the information and internal use of UCSF management and the Ethics, Compliance and Audit Board, and is not intended to be and should not be used by any other person or entity.

Sincerely,



Irene McGlynn
Chief Audit Officer

EXECUTIVE SUMMARY

I. BACKGROUND

As a planned audit for Fiscal Year 2019, Audit and Advisory Services (A&AS) conducted an audit of the controls in place for video surveillance at UCSF Health (UCSFH). The scope of our review was video surveillance planning and operations at UCSFH, including equipment procurement, camera placement, installation, monitoring, access, maintenance, and upgrading and decommissioning.

Surveillance cameras are an integral element of the UCSFH Security Program. The UCSFH Security Program itself is a core component of UCSFH Environment of Care Program. The Director of Security has responsibility for developing, implementing, and monitoring the Security Program. Appropriate surveillance camera operations help ensure patient and employee safety, as well as surveillance of sensitive areas. However, inappropriate access to stored video files may violate patient and employee privacy and must be carefully managed.

UCSFH Security Services Department (Security Services) is tasked with the responsibility of monitoring surveillance systems[1] in and around UCSFH owned or operated buildings. Camera images are recorded and these recordings are kept for at least 30 days.

Security Services collaborates with other departments to implement their charge. UCSFH departments route service requests (e.g. for installation or maintenance of surveillance systems) to Security Services. These requests are transmitted to the Campus Facilities Customer Service Center and they place work orders in the Campus Lock shop work queue. The Campus Lock Shop performs the requested service.

Security Services is also responsible for providing access to surveillance camera images, such as fulfilling requests for video files from UCPD for their investigations and those requested through them for other agencies and providing supervisor personnel view only privileges for certain cameras (e.g. helipad, cash handling areas, etc.)

Currently there is a project to upgrade security cameras at Moffitt/Long and Mt. Zion hospitals.

II. AUDIT PURPOSE AND SCOPE

The purpose of this review was to evaluate the controls in place for effective and efficient video surveillance operations at UCSFH. The scope of our review was video surveillance planning and operations at UCSFH, including equipment procurement, camera placement, installation, monitoring, access, maintenance, and upgrading and decommissioning.

Procedures performed as part of the review included interview of personnel directing surveillance systems operations, review of related policies and procedures, and

[1] Surveillance systems include cameras, video management systems, network video recorders, and associated network infrastructure.

evaluation of surveillance systems governance and operations. For more detailed steps, please refer to Appendix A.

Work performed was limited to the specific activities and procedures described above. As such, this report is not intended to, nor can it be relied upon to provide an assessment of compliance beyond those areas specifically reviewed. Fieldwork was completed in November 2018.

III. SUMMARY

Based on work performed, UCSF Health Security Services is leveraging the expertise of other departments to enhance their operational efficiency of surveillance systems. Additionally, Management is aware of and taking steps to address outdated surveillance cameras and associated equipment.

Opportunities for improvement exist in the areas governance, operations, and IT Security.

The specific observations from this review are listed below.

1. There are insufficient controls in place for monitoring and maintaining security cameras, resulting in an unknown number of cameras out of operation and potential gaps in coverage.
2. The Campus and UCSFH use two different video management systems that do not have a cross platform interface, reducing the ability to coordinate security at UCSF.
3. User access to the UCSF Health video management system (VMS) does not comply with IS-3 – Electronic Information Security and UC Account and Authentication Management Standard.
4. Copies of security camera video files made to fulfill information requests are not stored on encrypted media.
5. Roles, responsibilities, and expectations among departments involved in camera installation and maintenance are not clearly defined, reducing coordination and limiting efficiency.
6. Two policies that govern security camera operations are in conflict with each other. Additionally, security camera operations do not always follow policy.
7. Procedures for requesting access to video files are informal and documentation of these requests is not readily accessible.
8. Procedures for requesting installation of video cameras are informal and inconsistent, reducing efficiency and timeliness of camera installation.
9. Specific details for the Moffitt/Long & Mt. Zion Security Camera Upgrade Project have not been documented, resulting in an unclear plan to meet project goals.

Additionally, during the course of this review, a potential opportunity for improvement was noted for the procurement of cameras and associated equipment.

IV. OBSERVATIONS AND MANAGEMENT CORRECTIVE ACTIONS (MCA)

No.	Observation	Risk/Effect	Recommendation	MCA
1	***There are insufficient controls in place for monitoring and maintaining security cameras, resulting in an unknown number of cameras out of operation and potential gaps in coverage.*** Current records used by management to monitor security cameras are not completely accurate. Specifically: • A complete inventory of UCSFH security cameras is not maintained. • It is unknown exactly how many of the cameras are non-functional. Based on an inventory of cameras provided by management, 40% of cameras at Parnassus, 100% of cameras at Mt. Zion, and 4% of cameras at Mission Bay were not operational/functional during a physical check of cameras on the network by UCSF Health Security Services. • There are discrepancies between the management inventory and observation conducted at Mt Zion. Two cameras observed at the Mt Zion campus were functioning, in contrast to the listing on the management inventory.	Security cameras are an integral part of the UCSFH Security program. Without monitoring and maintaining cameras in critical locations the Security program may not afford protection for patients, visitors, staff, and property as it was designed.	Management should perform a comprehensive review of security cameras at Parnassus and Mt. Zion, and prioritize fixing cameras in critical areas that are not functioning.	**Action:** Comprehensive camera inventory and validation is in process. Prioritization levels will be added to the camera inventory database as a separate data field. Inventory will be maintained in a Smartsheet database that will be used to manage assets including routine maintenance schedules for each asset. A written procedure will be developed that will address on-going maintenance to support the video assessment and surveillance system (VASS) program including routine preventative maintenance. **Responsible Party:** Director - Security Services **Target Completion Date:** May 31, 2019
2	***The Campus and UCSFH use two different video management systems that do not have a cross platform interface, reducing the ability to coordinate security at UCSF.*** UCSFH uses Milestone and UCSF Campus uses Exacq for their respective video management systems (VMS) – these are non-compatible systems and require different knowledge bases to install, operate, and maintain.	Safety of patients, visitors, staff, and property may be compromised as the UCSF PD are not able to view all camera angles from a single	Management should review aligning surveillance standards with the Campus, e.g.: • Camera placement	**Action:** Project scoping document to include one UCSF VMS standard for all new camera installations. Campus IT, Lock Shop and Finance Service Center are is integral to this project and will be moving forward in order to

No.	Observation	Risk/Effect	Recommendation	MCA
	Support of these systems would be more efficient if there were one standard across the organization. Additionally, having one standard would enable UCSF PD to more effectively monitor crowds when an Operations Center is established during strikes, Regents' meetings or periods of public disruptions or demonstrations.	location. Additionally, increased effort is needed to maintain two different VMS.	• Monitors • Cameras approved for use • What server is used • Where is the data backed-up	maintain UCSF Health's surveillance system. UCSF Health is subject to their review and approval process for hardware and software systems. Campus standards will be used as part of the project where available. **Responsible Party:** Administrative Director - Safety, Security, Emergency Management **Target Completion Date:** February 28, 2019
3	***User access to the UCSF Health video management system (VMS) does not comply with IS-3 – Electronic Information Security and UC Account and Authentication Management Standard.*** Specifically, we noted that management of user accounts did not meet the following: • Password complexity requirements • Use of multifactor authentication • Established frequency of required passphrase changes • Requirement to change passwords when logging in for the first time • Disable or remove access rights for unneeded accounts • Review of inactive accounts • Lockout accounts after 10 failed login attempts Additionally, authentication should be tied to users' UCSF Active Directory account to enable automatic deprovisioning upon user separation.	Insufficiently protected accounts could be compromised, increasing UCSF network vulnerability.	VMS Access should comply with IS-3 – Electronic Information Security and UC Account and Authentication Management Standard.	**Action:** The IS-3 – Electronic Information Security and UC Account and Authentication Management Standard (consistent with the Campus standard), will be written into the project scoping document as a project standard. **Responsible Party:** Administrative Director - Safety, Security, Emergency Management **Target Completion Date:** February 28, 2019

No.	Observation	Risk/Effect	Recommendation	MCA
	Account management and authentication mechanisms are the primary method for protecting UC's Institutional Information and IT Resources. Following the requirements in the UC Account and Authentication Management Standard ensures good security practices that help minimize cyber risk.			
4	***Copies of security camera video files made to fulfill information requests are not stored on encrypted media.*** To fulfill requests for security camera video files UCSFH Security Services reviews available security camera footage and saves copies of the appropriate views to separate video files. These files are first saved to a network server then later moved to UCSF Box folders to allow others access to them. However, the media these security files are saved to may not be encrypted. Since some of these records may contain restricted information, they should be protected from unauthorized access, disclosure and disposition.	Unauthorized access or disclosure of restricted information could result in violations of University policy and California and Federal laws.	The UCSF Box folders used to provide video files to fulfill information requests should be encrypted. The Network File Servers should be encrypted as well.	**Action:** Written standard work will be developed for video file requests which will include utilization of a "secure" Box folder. **Responsible Party:** Director - Security Services **Target Completion Date:** February 28, 2019
5	***Roles, responsibilities, and expectations among departments involved in camera installation and maintenance are not clearly defined, reducing coordination and limiting efficiency.*** Camera installation and maintenance requires coordinating information and effort among several departments between UCSFH and the Campus: • UCSFH Department: Requests camera installation or maintenance • UCSFH Security Services: Performs security survey for installation of new cameras (may be performed in conjunction with Campus Finance Service Center) • Campus Facilities Customer Service Center: Places the service request in the Lock Shop work queue • Campus Facilities Lock Shop: Estimates time and material to full request, performs service and charges relevant expenses to Work Order	Without SLAs to coordinate interaction between departments their individual roles and responsibilities may be ill-defined, leading to potential customer dissatisfaction, miscommunication between involved departments, and other inefficient processes.	Establish SLAs to establish responsibilities and expectations among stakeholders and to define and document process flow and help ensure the operations run more smoothly.	**Action:** UCSF Health Security can develop a list of requirements that are needed to support and maintain the video assessment and surveillance program. This list of requirements can then be used as criteria for SLA development as Campus departments are the primary service providers to UCSF Health as described by the observation. **Responsible Party:** Director - Security Services

No.	Observation	Risk/Effect	Recommendation	MCA
	• Campus Finance Service Center: Obtains required licenses (if any) and integrates camera into network • UCSF IT: Reviews available ports on server and establishes IP addresses for cameras While there is a MOU is in place for services provided by the Finance Service Center to UCSFH Security Services, currently, there are no Service Level Agreements (SLAs) to define interdepartmental coordination among the other departments.			**Target Completion Date:** May 31, 2019
6	***Two policies that govern security camera operations are in conflict with each other. Additionally, security camera operations do not always follow policy.*** Approval of Office of Legal Affairs and Human Resources Vice President / Director of Labor and Employee Relations is not obtained for Departmental Cameras. Additionally, while the UCSF Health Security Policy 2.1.0 states that "UCPD maintains jurisdiction for the investigation of all crimes and suspected criminal activity in Medical Center buildings and areas," this conflicts with UCSF Health Security Camera Usage Policy 3.06.11, which states "In consultation with the Office of Legal Affairs and Labor and Employee Relations, one or more of the following individuals are authorized to conduct surveillance investigations: • All Campuses – Director of Security and UCSF Health COO/Senior VP • Mount Zion Campus – Director of Security and Mount Zion Site Administrator • Mission Bay – Director of Security and BCH Vice President of Operations"	Cameras may be installed without appropriate legal review. There may be confusion regarding responsibility for conducting investigations	Policies should be updated with clarified language to coordinate with each other.	**Action:** UCSF Health Security will add clarifying language to UCSF Health Security Policy 3.06.11 that better defines surveillance investigations. **Responsible Party:** Director - Security Services **Target Completion Date:** February 28, 2019
7	***Procedures for requesting access to video files are informal and documentation of these requests is not readily accessible.***	Maintaining requests for video files in an organized way	Formalization of requests and centralization of request	**Action:** To standardize and formalize process, requests for security video files will be integrated into Medical Center

No.	Observation	Risk/Effect	Recommendation	MCA
	UCSFH Security Services receives requests from UCPD for video files to use as evidence in their investigations and investigations of other agencies. These requests are sent via email and the relevant video files are pulled down from the video management system and saved. However, Security Services does not maintain these requests in an organized fashion. While the department keeps the email requests for these files, they may be maintained in different places that do not enable efficient access when needed, and are not accessible by all parties who may have a business need to retrieve them.	would enable the Security Services Department to monitor the number of requests it receives, gauge the time it devotes to responding to the requests, and demonstrate compliance with Security Camera Usage Policy 3.06.11.	documentation will enable efficient and effective monitoring and ability to demonstrate compliance with video request requirements.	Support Services (MCSS) service request menu for security services. **Responsible Party:** Director - Security Services **Target Completion Date:** May 31, 2019
8	***Procedures for requesting installation of video cameras are informal and inconsistent, reducing efficiency and timeliness of camera installation.*** There are multiple channels by which requests for video cameras may come into UCSFH Security Services: • E-mail or phone calls to UCSF Health Security Services • Phone, e-mail, Maximo Work Order, or ServiceNow request to the Campus Facilities Customer Service Center, which is then relayed to UCSF Health Security Services for a security assessment In order to fulfill these requests, Campus Facilities Customer Service Center places the service request in the Lock Shop work queue. Due to the inconsistent intake process, not all information may be provided to Campus Facilities Customer Service Center (e.g. finding source), increasing potential delays in installation and additional efforts by the Campus Facilities Customer Service Center to research all the required information.	Ill-defined procedures may cause delays in processing, require additional handoffs or manual processing, and other inefficient processes. Funding information may not come across with the request and this could hold up the requested service.	Formalization of procedures to enhance client understanding and establish responsibilities and expectations among stakeholders	**Action:** To standardize and formalize process, requests for security system installation will be added to the Medical Center Support Services (MCSS) service request menu for security services. Service request information will be reviewed and validated by UCSF Health Security prior to creating a daughter request with the appropriate self-service portal (i.e. Campus Customer Service Center-Maximo). **Responsible Party:** Director - Security Services and Operations Manager - Security Services

No.	Observation	Risk/Effect	Recommendation	MCA
				Target Completion Date: May 31, 2019
9	***Specific details for the Moffitt/Long & Mt. Zion Security Camera Upgrade Project have not been documented, resulting in an unclear plan to meet project goals.*** Management has implemented a project to upgrade security cameras at the Moffitt/Long and Mt. Zion hospitals. However, there does not appear to be appropriate project management documentation for the project, including: • Project Charter • Project Plan • Project Executive Sponsor • Detail of specific items included in the budget Communication among the project's stakeholders of the project's objectives, timeline, budget, task prioritization, dependencies, and completion tracking is imperative for its successful completion.	Without sound project management practices, the Moffitt Long & Mt. Zion Security Camera Upgrade Project could experience scope creep and not meet its objectives or budget.	Management should develop appropriate project management documentation to help ensure that the project's objectives, timeline, budget and status are clearly communicated to key stakeholders of the project.	**Action:** UCSF Health Security will partner with Design & Construction Project Management Services to create a project scope document that will include the recommendations as written as well as the list of video assessment and surveillance standards/policies that the project has adopted. **Responsible Party:** Administrative Director - Safety, Security, Emergency Management and Director, Project Management Services **Target Completion Date:** February 28, 2019

V. OPPORTUNITIES IMPROVEMENTS

No.	Observation	Risk/Effect	Recommendation
1	***UCSF does not have purchase contracts for security cameras.*** Currently security cameras are mostly purchased from the vendor of record for physical access control used by UCSF Campus. This does allow for some cost savings. However, having purchasing agreements with multiple vendors may allow for needed flexibility and equipment availability, but also likely at an increased cost.	To help obtain optimal pricing, UCSF Health and the Campus Lock Shop should establish joint security camera standards and purchasing contracts.	Management should consider establishing purchase contracts or group purchase organizations (GPO) for potential cost savings

APPENDIX A

To conduct our review the following procedures were performed for the areas in scope:

- Reviewed policies and procedures related to surveillance planning and operations as well as those related to surveillance data access, storage and retention at UCSF Health.
- Identified and interviewed personnel relevant to the planning and operations of surveillance systems, including installation and maintenance of these systems.
- Evaluated the governance and oversight of surveillance systems as well as the processes for surveillance data access, storage, retention and distribution at UCSF Health.
- Evaluated the coordination among the various groups responsible for these functions.
- Reviewed inventory of surveillance devices and systems, and discussed coverage with relevant personnel.
- Validated that security cameras are operational on a sample basis.
- Reviewed physical security of cameras and network video recorders.
- Reviewed logical access to stored video files as well as encryption of these files.
- Reviewed login ids and passwords used to access video surveillance on a sample basis.