Access to County Buildings

Risks Require Clarity and a Comprehensive Approach

August 2018

Multnomah County Auditor's Office

Steve March, Multnomah County Auditor

Office of
Multnomah County Auditor

Steve March
County Auditor

501 SE Hawthorne Room 601
Portland, Oregon 97214
Phone: 503-988-3320

Fran Davison
Nicole Dewees
Craig Hunt
Jennifer McGuirk
Annamarie McNiel
Marc Rose
Mark Ulanowicz
Caroline Zavitkovski

Date: August 16, 2018

To: Deborah Kafoury, Chair; Marissa Madrigal, COO; Commissioners Meieran, Smith, Vega Pederson, & Stegmann; Sheriff Reese; District Attorney Underhill; Bob Leek, DCA; Naomi Butler, Facilities

From: Steve March, County Auditor

Re: Access to County Buildings

Attached our audit of Access to County Buildings. During previous work involving a fraud case we recognized a risk involving access to some County facilities and as a result we added this audit to the audit schedule.

The most common access cards are those issued to employees, however the new ERP system will makes changes in how those tracked. Non-employee access cards were somewhat more problematic because some provide access even to sensitive areas of the County, and in our survey many were unaccounted for. We have provided Facilities staff a list of those we identified as unaccounted for and they were turned off for safety and security reasons. We make a number of recommendations around access cards and consideration of risk broadly.

We have very much appreciated the cooperation of the COO, Department of County Assets, and in particular the management and staff at Facilities, as well as the staff at all County offices contacted with regard to access cards. The audit work was conducted by Principal Management Auditor Craig Hunt, CPA & Senior Management Auditor Annamarie McNiel, CPA.

C: Jenny Madkour, County Attorney; Cindy Hahn, Privacy Officer

Table of Contents

Report Highlights

What We Found

We found poor controls over building access cards that creates an unacceptable security risk to County buildings. Building access security should help protect staff and the public as well as safeguard the County's assets and confidential information. We also found active access cards in the access card tracking system that included terminated employees and other cards that departments should have deactivated. A former employee, contractor, or volunteer could use one of these cards to gain unauthorized access to County buildings. Poor data also limits the County's ability to measure and evaluate the County's access security performance.

Departments sometimes provided more access than needed for cardholders to perform their work. The County has not trained its managers on providing appropriate access levels. However, before managers can be completely trained, County buildings will need to go through a process that formally ties access levels to security risks. Instead of using professional security staff, the County currently relies on the Facilities and Property Management's Alarms Unit (FM Alarms) to raise questions when the access levels that departments request appear inappropriate.

Why We Did This Audit

While we were doing other audit work, we found inadequate controls for one department's access cards and suspected that other departments may have the same issues.

What We Recommend

County leadership first needs to take a comprehensive approach to define the level of security risks they are willing to accept and establish a security governance structure. To attain reliable building security countywide, the County should conduct regular risk assessments and evaluate access levels.

Either a standalone security function or one placed within Risk Management should be responsible for overseeing countywide building security. FM Alarms should limit their involvement to technical issues and not security functions. Even with these recommended changes, departments will still need to account for their access cards, know how to request the minimum level of access needed, and modify and terminate access cards. They will also need training as well as better administrative procedures.

To improve data quality, departments must properly complete all access card applications. Departments should also compare their inventory of access cards to the centrally maintained access card tracking system at regular intervals and deactivate missing or seldom used cards. With clean data, the County will be able to evaluate whether its performance is efficiently and effectively meeting security goals.

Background

The County is responsible for securing the access to approximately 69 buildings. The security risks of these buildings differ and call for different levels of protection for employees, the public, information, and assets. Some buildings, such as the Multnomah Building, have high public access while others, such as the Library's ISOM building, has almost no public access. County-occupied buildings may also have multiple occupants from different departments with diverse security needs.

The County limits access to and within its buildings at specific entry points (doors) to authorized people. The majority of these people are the County's approximately 6,000 employees. Departments authorize their employees to use an access card and designate the building doors that these cards can open. Based upon departments' access card applications, the Facilities and Property Management Alarm Unit (FM Alarms) activates cards to permit access to certain buildings and doors at specific times of the day. Once issued, employees can hold their cards in close proximity to a card reader to unlock doors and gain access to their worksite.

We refer to access cards for employees as picture cards in this report simply because they have employees' photos on them. These cards are also color coded to indicate the department in which the employee works. Employees are required to display their cards while at work for easy identification. While the County primarily uses picture cards for employees, a small number of other types of access card users may also use a picture card. As of March 15, 2018, the County had 7,482 active picture card records in the database.

In addition to picture cards, the County uses non-picture cards for visitors, volunteers, contractors, vendors, and community partners such as non-employee alcohol and drug counselors. The County also uses non-picture cards for unpaid interns, new employees who do not yet have a picture card or regular employees who forgot to bring their picture card. Non-picture cards frequently have a description such as "Staff" or "Loaner" written on them. Most non-picture cards look and work like picture cards minus the person's photo. The Sheriff's Office uses Frequency Operated Buttons (FOBs) and the Department of Community Justice uses some stickers about the size of a quarter (key tags) for access to gated parking. As of March 15, 2018, the County had 1,920 active non-picture card records in the database.

The County uses one software system called Entrapass to track cards and access to all its buildings except County jails, which uses its own system. Although the County acquired Entrapass almost 20 years ago, FM Alarms has kept the software updated. FM Alarms keeps access card activity current for about five years and archives prior data.

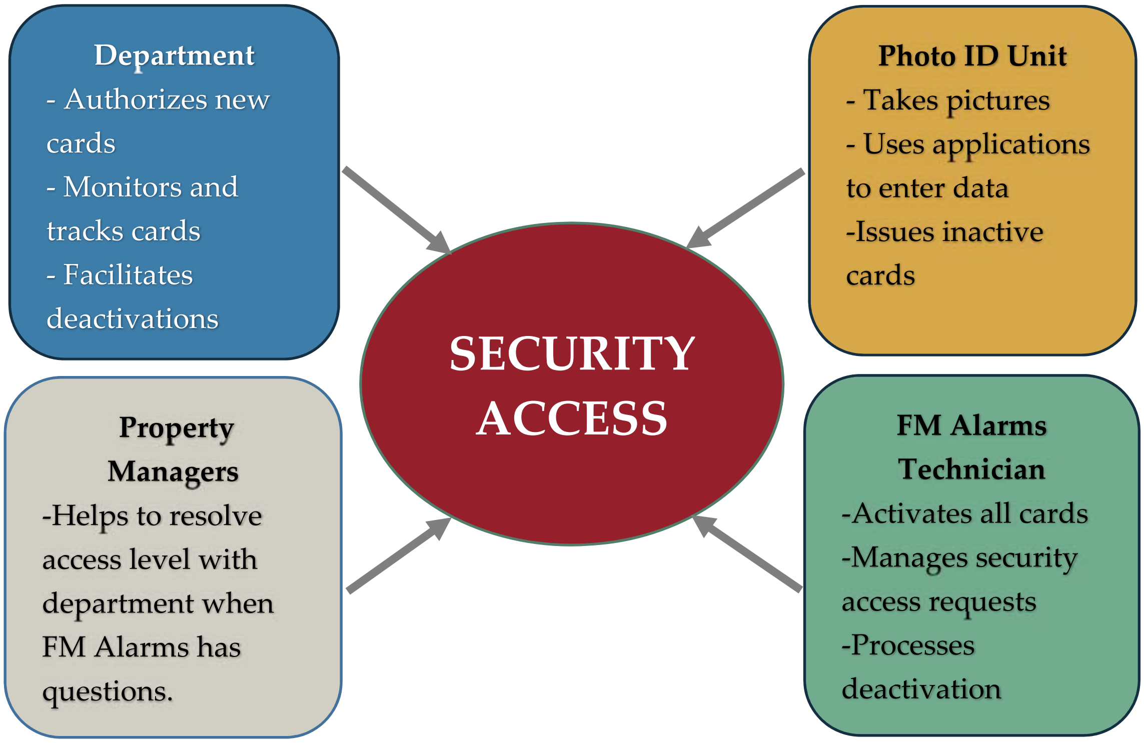
Departments initiate the access card process.

As illustrated below, when a department hires a new employee, the department completes an access card application and sends it to FM Alarm's Photo ID Unit. The Photo ID Unit enters the employee's application data into Entrapass, provides a non-active picture card to the employee and forwards the application to a FM Alarms technician. The FM Alarms technician activates the picture card on Entrapass. If the access level assigned by the department appears unusual, the FM Alarms technician may contact the building's property manager to confirm whether the access levels are appropriate. Non-picture cards follow the same general process.

Departments are responsible for monitoring their access cards and should periodically compare their records with Entrapass data. Per county procedure Fac-11, when an employee leaves the County, departments are responsible for retrieving their access card. To deactivate employee picture cards FM Alarms uses the Information Technology Termination Listing Report. However, for non-picture cards that are lost or no longer needed, the department must notify FM Alarms to deactivate the cards. The quality of Entrapass data and the effectiveness of access security depends on departments:

- Selecting the access level that provides the minimum access needed for the employee to do their work.
- Completing the application form properly.
- Properly monitoring non-picture cards and deactivating them when lost or no longer needed.

Current building access governance is lacking security expertise.



Department
- Authorizes new cards
- Monitors and tracks cards
- Facilitates deactivations

Photo ID Unit
- Takes pictures
- Uses applications to enter data
-Issues inactive cards

SECURITY ACCESS

Property Managers
-Helps to resolve access level with department when FM Alarms has questions.

FM Alarms Technician
-Activates all cards
-Manages security access requests
-Processes deactivation

Workday implementation group discovers data problems.

As part of setting up the County's future enterprise resource planning system (Workday), the County attempted to account for all picture access cards early in 2017. The Workday group found approximately 500 active picture cards on Entrapass that were not properly deactivated when employees left the County. Once set up, Workday should better automate and account for these cards than the current process. As currently planned, non-picture cards will remain a manual process.

The Sheriff's Office, District Attorney (DA) and the Department of Community Justice (DCJ) have different processes in place for access cards. The Sheriff's Office does not use Entrapass for its two jails and uses FOBs for other buildings. The DA and DCJ both use their own application forms to request picture and non-picture access cards. Entrapass tracks non-picture FOBs for the Sheriff's Office, and access cards for the DA and DCJ. Unless called out specifically, the audit results below include the Sheriff's Office, DA and DCJ.

Results

The adequacy of the County's building access security depends largely upon how much risk the County is willing to accept. The County must achieve a balance between tight security that limits access to the public versus access that is loose and unacceptably exposes people to potential harm. With budget constraints in mind, the County must thoughtfully analyze and choose what security measures reduce building access risks to a level that aligns with their risk appetite.

When functioning properly, an access security system *at minimum* should reduce risks of unauthorized physical access as well as access to confidential information to an acceptable level. Further, access security measures should prevent assaults on staff or the public, and protect the County's assets from theft. Employees should feel reasonably safe to perform their work.

While the central focus of this audit was non-picture cards, we found a number of issues that are common to both picture and non-picture cards. Weak controls over both types of cards create security risks and contributes to the poor condition of Entrapass data. Before the County can develop new policy and procedures, County leadership needs to define their security goals and use trained security professionals to work with departments instead of FM Alarms to make building access decisions. Even with security professionals, both County managers and employees will need access card training.

Poor control of access cards creates unacceptable security risks to County buildings.

Although some departments did better than others, overall we found County departments track non-picture access cards poorly. Out of 1,764 non-picture cards tested and listed as active on Entrapass, as of March 15, 2018, we could not locate 887 cards or 50.3% of non-picture cards. The access levels of missing cards ranged from a low security risk, such as interior door access only during business hours, to a high security risk of 24/7 access to exterior doors of multiple locations.

In numerous cases, departments could not determine who was responsible for tracking access cards. Accountability for non-picture cards should be clear. Departments should be able to identify their employees who are custodians of these cards. Entrapass does not currently track the custodians of non-picture access cards, which makes monitoring them difficult.

Frequently, non-picture cards are for temporary use. For example, if an employee leaves their picture access card at home, a non-picture loaner card is available for the day. Contractors use non-picture cards until their work is completed. Some County vendors may use non-picture cards for an extended duration. Nevertheless, some card users take the non-picture card home with them or otherwise do not return the cards.

The County does not have procedures for tracking non-picture cards. As a result, some departments developed their own tracking mechanisms. Among those who did, we found sign out sheets were very helpful. If, for example, an employee did not return a borrowed card, the sign out sheet identifies them. As another good practice, several departments would periodically compare their inventory of non-picture cards to Entrapass records and deactivate missing or seldom used cards.

Because the data in the County's security system is not in good condition, the County cannot use it to evaluate security.

Based on a review done in 2017 by the Workday ERP team and our work in this audit, we found that Entrapass data is not in good shape. Departments are mostly responsible for the reliability of Entrapass data and have not always provided good information on the access application form or have forgotten to request deactivation of cards no longer in use. Photo ID Unit staff and FM Alarms modify Entrapass data based upon Departments' requests.

We found that Entrapass data included both picture and non-picture cards that should have been deactivated due to employee termination or, for example, due to a contractor finishing their work. Timely card deactivation is a common problem in other jurisdictions as well. Department supervisors and managers do not always get employee terminations processed for picture cards or unneeded non-picture cards. Departments should also turn off access privileges to employees taking extended leaves of absences.

Because of the large data discrepancies, we concluded that some departments are not periodically comparing their access card information to Entrapass data. The County will need to define the frequency of these comparisons in written procedures. Finally, a standard naming convention would greatly aid comparisons of department data to Entrapass.

The number of managers in each department who are authorized to sign access card applications varies from three in the District Attorney's Office to 178 in the Health Department. While some of this variance is due to the size of departments, fewer authorized managers would likely improve the quality of data in Entrapass and make access cards easier to track.

Because Entrapass data is in poor condition, the County cannot use it at this point to evaluate access security performance. Without reliable performance measurement data, decision makers do not have information to gauge whether their investments improve security. Here are some examples of basic performance measures.

Security performance measures needed to evaluate security efforts.

- **Input.** Resource requirements such as security guard costs, cost of equipment, maintenance, testing costs and training.
- **Output.** Planned security assessments completed and number of facilities at acceptable risk levels.
- **Outcome.** Incident reduction, emergency preparedness and program efficiency.

The Entrapass system is a large database with many records and includes all departments. While FM Alarms activates and deactivates access cards, and some departments may check the accuracy of their data, there is no function that monitors and evaluates the data from a countywide perspective. Close attention to these important countywide tasks should improve Entrapass data quality.

Security risks increase when departments do not request the minimum access level needed.

Access levels are simply the locked doors a cardholder can open at a given time with their card. All access cards, whether picture or non-picture, should only allow the minimum level of access required to complete necessary work. The current access card application works against this principle (excluding the DA, DCJ and the Sheriff's Office).

We found that using the "looks like" field on the application form for access levels is expedient but not a good way to assign access levels. A "looks like" field lets a department manager requesting access for someone to indicate on the form the security card's access level should look exactly like another's. For example, new employee A's access privileges should mirror existing employee B's.

The problem with this approach is managers may not know the access levels for an existing employee or remember that they have changed. When a manager is requesting that new employee A's access should "look like" employee B's, employee B's access levels may include, for example, an interior door in the building that employee A should not have. Departments should obtain data from FM Alarms to see what the "looks like" access levels actually are.

Department managers and employees need training.

Department managers should be trained to know exactly what levels of access they are providing. However, before managers can be completely trained, County buildings will need to go through a process that formally ties levels of access to security risks. Among County buildings, security risks are as variable as building's characteristics. For example, a large building with multiple departments as tenants, a large number of employees and high public access such as the Multnomah Building is going to have a higher risk than a smaller building with few tenants and little public access like the Library's ISOM building. Aside from allowing the County to make risk-informed decisions for all its buildings, once the County conducts building risk assessments, they can also develop security training for managers.

Until the County is able to complete formal risk assessments on its buildings, department managers will still need to make appropriate access decisions. Instead of using the "looks like" approach described above, managers must understand what access levels they are providing. FM Alarms can send reports of access levels for picture or non-picture cards to managers so they can make better-informed decisions. If the County decides to shift the final responsibility for building access decisions to trained security personnel, training requirements for managers could be less.

At a more fundamental level, department managers should know how to request, change and terminate access cards. Employees should be aware of their access responsibilities such as properly wearing their card, as well as other security issues such as how to deal with "tailgaters" (following another person in a door without using an access card) and not letting unidentified people into buildings. Once procedures are in place, employees who provide non-picture cards to contractors, visitors or volunteers should better understand their responsibilities for tracking and monitoring their cards.

Upgrade policy and procedures to achieve better standardization.

The County has not developed a comprehensive, firm and principled foundation for building security that provides sufficient guidance on what is required. Accordingly, the County (preferably a security function) should revise and expand the existing administrative procedure FAC-11 for building security. For example, there is no requirement in FAC-11 for departments to monitor the accuracy of data in Entrapass or frequency in which they should do so. While the County does have an administrative procedure that addresses visitor and vendor access to restricted areas to help safeguard personally identifiable information (PHI), it does not have an administrative procedure for non-picture cards that include contractors, visitors, community partners or volunteers that extends beyond protecting PHI.

We believe that different building security philosophies as well as lack of attention have caused security access issues throughout the County. Procedures should address both leased and owned buildings, all types of access cards, building risk assessments, defined levels of protection, roles and responsibilities of departments, FM Alarms, property managers, and a security function.

FM Alarms should not make security decisions.

FM Alarms currently maintains the access software system Entrapass. When departments request activation of access cards they specify the times of day the card should work and the access levels. If any access level requested is unusual or does not look right, FM Alarms contacts the building’s property manager to confirm if the requested card’s access level is appropriate. Even though FM Alarms does not have building security training or expertise, it essentially checks the building access levels provided by departments. The County should not put FM Alarms in the position to make these types of security decisions indirectly or otherwise.

County leadership should define the level of security risk they are willing to accept and ensure building access aligns with those needs.

Based on the results of our testing, building access security has not consistently received the attention it needs. Instead of a proactive approach, it should not take preventable security breaches, stolen property or an injury to motivate needed changes. Any changes made may only be for the specific building where the breach occurred. There have been several efforts to improve County building security risks but none has gained momentum.

In 2008, Risk Management used a security expert to evaluate building risks. From 2008 through 2010, the expert assessed the security risks of several libraries including the Central Library, as well as the Multnomah Building, Health Clinics, Elections, Lincoln Building interview rooms, Gateway Children Center, Gateway WIC Clinic and the Southeast Tabor Building. While the County made some improvements, there was insufficient follow through of this work.

Before the County can fully address our concerns, it must establish a security governance structure and lay out what levels of security risks the County is willing to accept. The default reliance on departments overseeing their own security creates inconsistencies throughout the County and increases building security risks because most departments do not have personnel with a security background or training. For example, in one multiple tenant building, one department does not want to restrict access by the public in any way while another department is willing to make tradeoffs to attain higher security levels. Further, when there is disagreement about a serious security matter in a multiple tenant building, no one has clear authority to resolve the issue.

It is difficult, if not impossible, to establish security procedures and take constructive actions without sufficient guidance, authority, and support. To attain consistent and sustainable countywide security, the County should conduct regular building risk assessments and define levels of protection within the context of countywide security priorities and principles. The County must also consider the tradeoffs between security and budget at the countywide level in addition to the department level.

Like other jurisdictions, the County could establish a security function with trained security personnel with the following roles:

- Conducts building risk assessments to determine security access levels within the boundaries of the County's risk tolerances.
- Coordinates security efforts across departments and minimizes any redundancies that could be occurring.
- Checks departments' access levels, hours and days of week on the access card application for new employees and other types of users based on minimal level of access needed to perform the work.
- Routes approved access card applications to Photo ID.
- Sets criteria for background checks for employees, contractors, volunteers, community partners and unpaid interns.
- Drafts, revisits and revises written building security procedures.
- Works with departments to ensure Entrapass data is accurate.
- Uses a security performance model that measures inputs and accomplishments to evaluate whether security investments produce results that align with the County's security goals.

With a security function, the FM Alarm's responsibilities would be appropriately limited. FM Alarms would only continue to activate and modify access cards on Entrapass based upon the application form reviewed by the security function.

The County could structure building access security different ways. Building security could be a stand-alone function that reports to the COO. Alternatively, the County could place security in Risk Management. Either way, security must work collaboratively with departments but ultimately have the authority to make final security decisions based upon the County's risk appetite and written policy and procedures.

Recommendations

1. The COO should establish a security function with trained security personnel.

2. To remove FM Alarms from the building access decision-making process:

    a. Either a separate security function or one placed within Risk Management should be responsible for managing countywide building security.

    b. Departments should send access application forms to the new security function instead of the FM Alarms technician. A security expert should review access suggested by departments, make any necessary changes in consultation with the department and building property manager, and then forward the application to the Photo ID Unit for picture cards or FM Alarms for non-picture cards.

    c. The security function should draft, revisit and revise building security procedures.

    d. The security function should be responsible for security performance measures and reporting.

    e. FM Alarms should continue to activate and modify access cards but not make any building access decisions.

    f. The Photo ID Unit already maintains a spreadsheet log of cards. We recommend the spreadsheet be expanded to include whether the card is a picture or non-picture card, the name associated with the card number for picture cards, the function (such as visitor, volunteer, community partner) associated with non-picture card numbers, and the person who is responsible for tracking the non-picture card.

3. Tracking non-picture cards will likely remain a largely manual process. To improve controls over non-picture cards:

    a. Departments should be able to quickly identify all the custodians of non-picture cards.

    b. The security function should develop procedures for non-picture cards.

    c. Custodians of non-picture cards should use sign-out sheets to track non-picture card activity.

    d. Departments should compare their inventory of non-picture cards to Entrapass records at regular intervals and request deactivation of missing or seldom used cards.

4. To improve the quality of Entrapass data:

    a. Departments must properly complete access card applications before being accepted. This includes employee ID number, cost center, department, e-mail address, and manager.

    b. Like non-picture access cards, departments' should periodically compare their inventories of picture cards to Entrapass records. Workday may streamline this process.

c. County administrative procedures should define a standard naming convention for employees as well as naming of non-picture card users.

d. Departments should deactivate access privileges to employees taking extended leaves of absences.

e. The security function should maintain, monitor and evaluate Entrapass data from a countywide perspective.

f. Departments should authorize the fewest number of employees needed to process access card applications.

5. Departments should only request the minimum level of access needed for both picture and non-picture cards. As such, departments should discontinue the use of the "looks like" field on the access card application.

6. Until a security function is in place, the COO should coordinate a central training protocol for department managers and employees about building security issues.

a. Department managers must know how to request, change and terminate access cards.

b. Employees should be aware of their access responsibilities such as properly wearing their card, as well as other security issues.

c. Employees who issue non-picture cards to visitors or volunteers must understand and carry out their tasks.

7. The COO under the direction of the Chair should define their security risk appetite and take steps to ensure all its buildings are within that zone.

a. The COO under the direction of the Chair should establish a security governance structure and lay out what levels of security risks the County is willing to accept.

b. The COO should ensure that County buildings go through a process that formally ties levels of access to security risks.

c. To attain consistent countywide security, the COO should ensure regular building risk assessments that define levels of protection are conducted.

Scope and Methodology

The objectives of this audit were to:

- Determine if internal controls for non-picture access cards are adequately designed to provide sufficient security for County personnel, protected information, the public and County assets.
- Determine whether a well-functioning governance structure for the County's access security is in place and functioning to ensure the effective management of security risks.

To accomplish these objectives we:

- Interviewed Facilities and Property Management personnel including FM Alarms, Picture ID Unit and property managers as well as Risk Management and personnel in all departments about how they manage building access cards.
- Examined processes for activating, deactivating and monitoring picture and non-picture access cards.
- Made on-site visits to department buildings to inventory all non-picture access cards.
- Sent non-picture card confirmations to departments that did not have a building on-site visit.
- Researched access security literature as well as other jurisdictions' access card practices and audit reports.
- Studied administrative procedure FAC-11 and a draft revision.
- Assessed separation of duties for the current non-picture card process.
- Spoke with County personnel assigned to Workday implementation about their work to date tracking all building access cards.
- Reviewed adopted budgets and other financial information.
- Collected all building risk assessments performed that were available.

This audit was limited to building access security only. We did not look at the County's two jails that use a different security system or formally evaluate HIPAA information risks. We did not inventory picture cards because the Workday implementation team had already attempted this. We did not examine emergency procedures. The data in Entrapass was not sufficiently reliable to inventory active non-picture cards. Instead, we visited worksites and used positive confirmations to account for non-picture cards.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings, and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A

Other Observations

While the scope of the audit focused on non-picture cards, we made several observations throughout the course of our audit procedures related to picture cards. We believe these are worth bringing to the attention of management as they present unnecessary risk to the County.

- We found that several employees and contractors had more than one card/FOB assigned to them. Nearly half of the persons identified with more than one card/FOB were noted to have the exact same access on each card/FOB. Additionally, we noted that several of the additional cards/FOBs were not being used and therefore, indicate that that they are not needed and/or have been lost.
- Entrapass data does not include an expiration date for all cards. Expiration dates are part of the set up process for each card created. The FM Alarm Unit manually adds a five-year period to each card, unless departments request a shorter time. In several cases, we noted cards with no expiration date entered.
- Departments are not monitoring all vendor badges. For example, we noted one vendor with six active picture badges; however, five of the six associated persons no longer worked for the vendor – with one of the persons not working for the vendor since December 2009 but the card was still active.
- Employee leave of absences (LOA) are not taken into consideration for discontinuing access to County facilities while an employee is on a LOA. For example, we noted an employee with sensitive access levels was on a LOA for over 3.5 months and their card access remained active during this time.

Audit Staff

Annamarie McNiel, CPA, Senior Management Auditor

Craig Hunt, CPA, Principle Auditor

Department of County Management

Multnomah County

Office of the Chief Operating Officer

October 24th, 2018

Auditor Steve March
501 SE Hawthorne Blvd, Ste 600
Portland, OR 97206

Dear Auditor March:

Thank you for the opportunity to review and provide comment on the Access to County Buildings Audit. Access to County facilities is a vital aspect of the responsibility to safeguard and protect the County's assets, its personnel, visitors, and the activities performed in the wide variety and type of County facilities. In order to provide access, the County issues two types of access cards: picture cards with photos of the owner of the card, and non-picture cards used for visitors, volunteers, contractors, vendors, and community partners. The County uses one software systems to track cards and access to all of its buildings except County jails, which uses its own system. The responsibility for updating the records in the software system so that each card is coded to allow access through card readers placed in facilities throughout the County lies with the Department of County Assets, in the FM Alarms team in the Facilities Division.

We agree with the findings of the audit, and have established that the following areas will be addressed:

- We agree that County leadership needs to take a comprehensive approach to define the level of security risks we are willing to accept and establish a security governance structure.
- We agree that the function of the design of a building security system should reside with one accountable organization, responsible for establishing access levels, risk assessments, request processing workflows, audit and testing of controls, and training and education for all departments.
- We agree that Departments must identify a network of key contact points, properly complete all access card applications, regularly compare their inventory of access cards to a centrally maintained access card tracking system, and request deactivation or missing or seldom used cards.

I am pleased to confirm that I will serve as the Executive Sponsor for the work to address Access to County Buildings. I have asked Bob Leek, Multnomah County Interim Director for the Department of County Assets, to serve as the Team Leader and to work collaboratively with all of the key stakeholders, including FM Alarms, Department Leadership Teams, Department Contact Points, and Department members to address the improvements needed in Access to County Buildings. That team will propose a governance structure to oversee the creation of recommendations for administrative procedures to formalize processes.

We agree that the adequacy of the County's building access security depends largely upon how much risk the County is willing to accept. We must achieve a balance between tight security that limits access to the public versus access that supports the safe and secure delivery of the services the County provides to the public. We will define success by delivering an access security system that reduces the risks of unauthorized physical access or unauthorized access to confidential information. We also strongly agree that employees should feel reasonably safe to perform their work, and that security measures should prevent assaults on staff or the public while in our facilities, and to protect the County's assets from theft.

Thank you for your vigilance in continuing to drawing attention to this critical area and for helping us identify measures we can take to proactively address the root causes of the challenges faced with Access to County Buildings. I look forward to sharing our future progress.

Sincerely,

Marissa Madrigal
Chief Operating Officer