HARFORD COUNTY, MARYLAND
Office of the County Auditor

AUDIT OF FACILITY ACCESS CONTROLS

Report Number: 2018-A-15
Date Issued: 10/29/2018

Report Highlights

Why We Did This Audit

This audit was conducted as part of the County Auditor's risk-based Annual Audit Plan approved by the County Council for FY2018.

What We Found

Controls can be improved to ensure access to County facilities is appropriate.

What We Recommend

- Implement procedures to track physical keys and routinely change pin lock codes.
- Deactivate devices assigned to separated employees.
- Periodically review access configurations and event logs.

Council Members and County Executive Glassman:

In accordance with Section 213 of the Harford County Charter, we have performed an audit of Harford County's physical security controls. The results of that audit, our findings and recommendations for improvement are detailed in the attached report. We would like to thank the members of management for their cooperation during the audit.

The audit found procedures and controls over access to County facilities are not adequate to ensure appropriate access to all County facilities. Specifically, processes do not exist to track physical keys or to routinely change pin lock codes; some facility access rights are inappropriate or unnecessary; and County facilities utilizing electronic access control systems lack proper monitoring of after-hours facility entries.

The audit team is available to respond to any questions you have regarding the attached report.

Sincerely,

Chrystal Brooks, CPA

Chrystal Brooks
County Auditor

cc: Mr. Billy Boniface, Director of Administration
Ms. Erin Schafer, Chief, Facilities and Operations
Mr. Joe Siemek, Director of Public Works
Mr. Bill Bettin, Deputy Director, Division of Water & Sewer
Mr. Jeff Stratmeyer, Chief Engineer, Division of Highways
Mr. James Richardson, Director of Human Resources

HARFORD COUNTY, MARYLAND
Office of the County Auditor

REVIEW RESULTS

We have audited the County's facility access controls for the period of 7/1/2017 through 3/31/2018 to ensure access to the County's facilities is appropriately monitored and restricted.

Our opinion, based on the evidence obtained, is the County lacks adequate controls in place to ensure appropriate, monitored access to all County facilities. The audit approach focused on testing the key controls that address management's objectives for the process. Conclusions drawn are below.

Risk	Expected Control	Conclusion
Facilities are accessed by unauthorized personnel	• Physical barriers such as fences and walls prevent or deter intrusions	Satisfactory
	• Entry points to premises are secured and equipment is operating properly	Satisfactory
	• Physical keys are inventoried	Unsatisfactory
	• PIN lock codes are routinely changed	Unsatisfactory
	• Security personnel and surveillance cameras supplement physical and electronic controls	Satisfactory
	• Access for separated personnel is disabled timely	Needs Improvement
	• Electronic access control systems restrict access to appropriate personnel based on job status and responsibilities	Needs Improvement
	• The County maintains a complete inventory of all facilities it owns or leases under County management	Satisfactory
Use of County resources for non-County activities	• Management monitors facility access events for unusual activity	Needs Improvement

Areas for improvement are described in the Findings and Corrective Actions section of this report. Management has been provided an opportunity to respond to this report; the responses provided follow the Findings and Corrective Actions.

FINDINGS AND CORRECTIVE ACTIONS

Finding Number: 2018-A-15.01 Physical Key Management

Management does not have a process in place to track physical keys for County facilities.

Analysis: There are 83 County facilities that rely upon physical keys or PIN locks to control access. While management has some lists of the relevant locks, there are no records of the associated keys or who those keys have been assigned to. Without that information, it is impossible to ensure that keys are returned when employees transfer to different departments or leave County service. Additionally, while keys are stamped "Restricted Duplication", there is no list of copies that have are made when the County calls a locksmith.

For PIN locks, there is no policy or procedure in place to ensure that codes are changed periodically. Management has advised that they don't know when PIN locks were reprogrammed. Without such a process, separated employees may continue to have access to secured areas. All of the PIN locks that we are aware of would require a person to first gain access to a building through an external doorway.

Recommendation: We recommend management develop procedures so that, as new locks are installed, new keys are logged and assigned, and PIN locks are periodically changed.

Management Response: Management appreciates the recommendation and will be reviewing the processes and policies regarding physical key management as well as periodic reprogramming of PIN locks.

Finding Number: 2018-A-15.02 Inappropriate or Unnecessary Access

Some facility access rights are inappropriate or unnecessary.

Analysis: We obtained lists of all active electronic keys and keycards to confirm that each was assigned to a current employee or contractor. Of the 70 sampled, four were assigned to a former employee. We reviewed the access history for each and confirmed that none of the four accessed the facilities after separation their separation dates. (The process for revoking physical access will be reviewed in a separate audit of Employee Separation Procedures.)

We also noted that some active electronic key cards are assigned to generic names (like 'Spare' or 'Test') or had no names. It is not clear who monitors custody of these badges. We reviewed the access history for each and confirmed that none of the generic or unnamed key cards accessed the facilities.

Additionally, we obtained lists of all electronic key readers to confirm that access to specific entryways was limited to appropriate personnel. Our testing found 26 users have inappropriate access to various entryways. It appears that employees and contractors are usually added to pre-existing access roles and some roles need their privileges refined or corrected. We reviewed the access history of each and found that only one used the unnecessary access privilege.

The above conditions increase the risk of inappropriate access to secured areas resulting in loss, theft, or impairment to assets or data or harm to personnel.

Recommendation: Active devices assigned to separated employees, or not specifically assigned to County personnel, should be disabled. Additionally, access role configurations should be reviewed periodically and updated to reflect changes in operations.

Management Response: Management will review the access provided to employees/contractors and refine or correct their privileges.

Finding Number: 2018-A-15.03 Facility Access Monitoring

After hours facility entries are not reviewed or monitored for unusual activity.

Analysis: In accordance with Principle 16 - Perform Monitoring Activates - of the Standards for Internal Control in the Federal Government, "Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results." It goes on to say "16.05 Management performs ongoing monitoring of the design and operating effectiveness of the internal control system as part of the normal course of operations. Ongoing monitoring includes regular management and supervisory activities, comparisons, reconciliations, and other routine actions. Ongoing monitoring may include automated tools which can increase objectivity and efficiency by electronically compiling evaluations of controls and transactions."

For the various electronic security systems, events such as granted access, denials, system malfunctions are logged and were available for the audit period. Although, for the main administrative badge system, logs were only provided to us for 60 days. (A related badge system had more than one year's worth of history available.) Based on our discussions with

management, no one reviews these logs to determine that there is no unusual activity. Additionally, information for the entry gate at the Abingdon Water Treatment Plant (AWTP) was not available from the vendor managing the gate's access system. Given the lack of availability of this information, management has not been monitoring access to the plant. Furthermore, pin codes are used for gate access at Abingdon and Sod Run water treatment plants as well as the Water & Sewer Operations facilities. For agencies and vendors that frequent the plants, one code is shared among their employees. Management informed us that use of these codes is not monitored nor are the codes routinely changed, which presents a risk of inappropriate entry to the facilities.

We were advised that the Facility Safety Coordinator reviews badge system malfunctions and warnings daily, but documentation of that review or the related reports are not maintained. Further, we were advised that these reports contain access denials and errors; granted access would not trigger an alert and is not reviewed.

We reviewed access logs for the various security systems and noted more than 200 employees, contractors or customers that entered secured facilities before 6 AM, after 7PM or on weekends. Of those, 62 significantly exceeded the average number of after-hours events. Undoubtedly, some of these employees are scheduled for weekend or evening shifts. While some activity could be explained by normal employee routines or known events, others had no obvious explanation. We found 16 instances of employees with unusual after-hours activity.

Although requested, we were not provided access to time clock details to confirm whether any of this activity is unusual. Management provided explanations for the activity of six of them. Management has advised that "Anyone who enters the buildings on weekends or after hours, has been authorized to do so by [the Director of Administration]. They do not necessarily have to be working..." We were provided a summary of those approvals. Of the exceptions identified, four were included on that list.

Without reviewing the events that have occurred, unusual activity may go undetected and data for post-incident investigation may not be available for review.

Recommendation: We recommend management periodically review event logs to identify trends, ensure that unusual activity is detected and granted access remains appropriate.

Management Response: Management will create procedures/policies for management to review access event logs to identify trends or unusual activity.

MANAGEMENT RESPONSE

Management will review and/or create policies and procedures with regards to public facility access to include key inventory, facility access rights, and management's review of facility entry and unusual activity. We hope to have this completed within 9 months to 1 year.

BACKGROUND INFORMATION

PROGRAM DESCRIPTION AND KEY STATISTICS

Facility access controls are necessary to control, monitor and manage access to facilities or areas of facilities to protect against theft, loss or impairment to assets or sensitive information or actual or physical harm to personnel. Facilities and Operations, a division under the Director of Administration, is generally responsible for the management of the facilities access function over all County facilities, while sharing the responsibility for the design, implementation and oversight of facilities access controls with each respective department. Access controls over facilities used as a part of Water & Sewer and Highways operations are the responsibility of those respective divisions. Harford County owns or leases more than 450 properties; over 150 of those require controlled access. Access controls consist of physical keys and locks; electronic cards or keys or cards; fencing and gated entry; security patrol personnel and surveillance cameras. Approximately half of the controlled facilities utilize electronic access systems and the other half rely on manual security (physical keys).

REVIEW OBJECTIVE, SCOPE AND METHODOLOGY

The objective of the audit was to confirm that access to County facilities is adequately controlled and routinely monitored. The scope of the audit included all facilities managed by the County but did not include facilities physically secured by Harford County Sherriff's Office, a municipality, or the State of Maryland. The audit focused on activity during the period of 7/1/2017 through 3/31/2018. Our audit procedures included interviewing personnel, observation and testing. Specifically, we:

- Confirmed access to all County facilities is managed by some County department;
- Confirmed access to respective facilities was limited to appropriate personnel;
- Confirmed access holders of personal electronic access devices were active and appropriate based on job responsibilities
- Confirmed access to electronic access entryway readers was limited to appropriate personnel based on job responsibilities
- Confirmed administration of electronic access control systems was limited to appropriate personnel; and,

- Performed data analysis on the access histories of all facilities utilizing electronic access control systems to confirm access was properly monitored and to look for unauthorized access/breach; access rejections, and unusual access during non-operating hours.

For the 83 County facilities at varying departments throughout the County where electronic access control systems were not in place, access controls were either inadequate or did not exist. Specifically, PIN locks were not routinely changed, and a key inventory was not effectively maintained, thus the controls' effectiveness could not be tested.

Harford County management is responsible for establishing and maintaining effective internal controls. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records, effectiveness and efficiency of operations including safeguarding of assets and compliance with applicable laws, rules and regulations are achieved. Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected.

The audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient 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.

Audit Team:

Chrystal Brooks
CPA, CIA, CGAP, CISA, CGFM, CRMA
County Auditor

Brad DeLauder, CPA
Senior Auditor