

**Montgomery County, Maryland  
Office of the County Executive  
Office of Internal Audit**



**Program Assessment of the Access ID Card Program**

**Montgomery County Police Department**

**February 25, 2019**

# Highlights

## Why MCIA Did this Assessment

The Security Services Division (SSD) of the Montgomery County Police Department (MCPD) is responsible for granting and monitoring physical access to County facilities through its administration of Access ID cards, which are issued to employees, contractors, sworn police officers, and non-employees including board/committee members, volunteers, and interns.

In May 2018, the County's Office of Internal Audit (MCIA) initiated a program assessment of the Access ID card program. The focus was Access ID card administration for employees, contractors, sworn police officers, and non-employees including board/committee members, volunteers, and interns. The assessment was conducted by the accounting firm SC&H Group, Inc. (SC&H), under a contract with MCIA.

## What MCIA Recommends

MCIA is making 10 sets of recommendations to strengthen SSD's internal controls, reduce risk, increase the accuracy and reliability of cardholder data, and improve overall performance related to the oversight and management of the Access ID card process.

**February 2019**

## Program Assessment of the Montgomery County Police Department Access ID Card Program

### What MCIA Found

There is an absence of standardized operating procedures, proper oversight, and training of the Access ID card program. A lack of standardization and adequate training has led to data integrity risks. It was noted that SSD is currently in the process of updating the formal policy for the Access ID card program and revising related procedures.

We identified 10 control deficiencies that indicate the need for improved Access ID card program management. Deficiencies relate to:

- Policies, processes, and procedures
- Data quality
- Record retention
- Access oversight and segregation of duties
- SSD personnel training

**TABLE OF CONTENTS**

Objectives ..... 1

Background ..... 1

Scope and Methodology ..... 4

Findings and Recommendations ..... 5

Comments and MCIA Evaluation ..... 16

Appendix A: Montgomery County Police Department Response ..... 17

## Objectives

This report summarizes the program assessment (assessment) performed by SC&H Group, Inc. (SC&H), under contract with the Montgomery County (County) Office of Internal Audit (MCIA), of the Montgomery County Police Department's (MCPD's) Security Services Division's (SSD) Access ID card program. The assessment was focused on the administration of Access ID cards for employees, contractors, sworn police officers, and non-employees including board/committee members, volunteers, and interns.

Specifically, we were engaged by the County to perform the following objectives:

1. Understand the current practices and procedures followed in SSD's management of the Access ID card program
2. Assess SSD's oversight of Access ID cards issued to employees and contractors
3. Identify potential risks or vulnerabilities
4. Evaluate opportunities for improved controls or processes

This assessment was performed in accordance with the Statement on Standards for Consulting Services (SSCS) issued by the American Institute of Certified Public Accountants (AICPA). SC&H's proposed procedures were developed to meet the objectives stated above and were reviewed and approved in advance by MCIA. The interviews, documentation review, and fieldwork were conducted from June 2018 to December 2018.

## Background

SSD is responsible for ensuring the safety and security of County personnel, facilities, and information by restricting access to locations within each facility to individuals with an approved need. Within SSD, the Access ID card program is responsible for granting and monitoring physical access to County facilities through its administration of Access ID cards, which are issued to categories of cardholders including employees, contractors, sworn police officers, and non-employees. Non-employees include board/committee members, volunteers, and interns.

### SSD Staffing and Workload

SSD consists of a Director and approximately 40 personnel, including two Program Specialists, who are responsible for ensuring the physical security of County facilities and personnel. SSD performs approximately 34,000 Access ID card related requests each year, including issuing approximately 3,000 new and replacement cards. SSD maintains a database of approximately 25,000 cardholders.

### Access ID Card Program and Processes

#### **Systems**

SSD uses the Kantech EntraPass security system (Kantech) to administer and manage Access ID cards. Kantech is a Windows-based secure access management system used to control employee and visitor movements at County facilities by interfacing with access card readers that secure entry throughout the County's facilities. The system allows SSD to 1) create and assign Access ID cards to County employees, police officers, and to non-employee personnel and 2) authorize entry into specific areas of each County facility based on the individual's role and need. Once assigned, access rights for individual Access ID cards can be added, modified, and deleted

through Kantech as user responsibilities change, or if the user no longer requires access to County facilities.

EAI Security Systems (EAI) is a third-party vendor engaged by the County and other local government organizations to help safeguard County personnel, facilities, and information. EAI assisted in the implementation of the Kantech card system and access card readers located throughout the County's facilities. EAI also provides ongoing support and assistance to the County, including supporting Kantech.

SSD also uses Remedyforce, a web-based service management system that allows departments to submit service requests (tickets) to SSD that can be assigned, prioritized, tracked, and monitored to manage Access ID card-related requests. Remedyforce also provides reporting and dashboards for monitoring performance.

### **Administering New Access ID Cards**

SC&H requested a copy of existing process and procedure documentation from SSD and was provided a preliminary draft document that was still undergoing internal review within MCPD/SSD. SC&H conducted process walkthroughs with the Program Specialists to gain a detailed understanding of the SSD Access ID card program. Through these process walkthroughs, SC&H was provided information concerning:

- New card issuance
- Lost/stolen card replacement
- Damaged card replacement
- Granting/removing facility access
- Changes to cardholder information
- Returning/deactivating cards for separated personnel

SSD uses the following categories in administering the Access ID card program:

- County Employee: An employee of the County Government except County police personnel
- Contractors: Third party personnel performing services for the County under a procurement contract
- Non-Employee: A volunteer, intern, or board/committee member
- County Police – Sworn officer: A sworn police officer
- County Police – Other: Retired police, police intern, and County employees who require access to MCPD facilities

Prior to issuing an Access ID card to a new cardholder, SSD Program Specialists obtain supplemental documentation from the requestor. The specific documentation required to receive an ID card is unique to each cardholder category, but once the appropriate completed documentation is submitted, the process for SSD to issue the Access ID card for each cardholder category is the same. SSD's goal is to complete card requests for both new cards, replacement cards, and facility access changes within 48 hours of receipt of the request.

SSD does not retain any documentation that includes personally identifiable information (PII). The Program Specialists visually verify documentation containing PII and return the original documentation to the applicant.

### ***County Employees (all non-police County employees):***

The Office of Human Resources (OHR) emails a list of employee new hires to SSD prior to each new hire orientation. The employee new hire list is used by SSD as authorization to issue an Access ID card to the employee. The hiring department notifies the new hire employee prior to the new hire orientation that to obtain an Access ID card during his/her orientation, the employee is required to bring the following:

- A valid U.S. Government identification (for example, a passport or a military ID) or
- A state-issued identification (for example, a current driver's license or identification card)

An SSD Program Specialist attends the orientation and meets with each new hire employee to verify the required documentation and issue the Access ID card. The employee leaves the orientation with his/her issued Access ID card (used for identification). However, SSD does not grant facility access to the Access ID card until an authorized department representative submits a request to SSD with the specific access rights needed for the employee. The Program Specialist that issues the Access ID card advises the cardholder that the card is for identification only, and that the cardholder will be notified when facility access has been added.

If a new hire employee does not attend new hire orientation, the employee makes an appointment with SSD to obtain an Access ID card.

### ***Contractors and Non-Employees:***

To obtain an Access ID card, contractors<sup>1</sup> and non-employees must schedule an appointment with an SSD Program Specialist. Applicants are required to provide the following documentation:

- Completed contractor and non-employee Access ID card application (MCP 163) signed by an authorized department representative
- A valid U.S. Government or state-issued identification

Prior to issuing an Access ID card, Program Specialists verify there are no previous Access ID cards issued to the individual by conducting a name search within Kantech. If an Access ID card for the applicant exists, the Program Specialists verify that the Access ID card is disabled before issuing the new card. Differentiating between two users with the same name requires manual research by a Program Specialist to ensure the correct cardholder is identified (middle name, department, job title, photo etc.).

At the time of issuing Access ID cards to contractors, Program Specialists assign an expiration date of one year from the date of issuance. This is a process change that occurred in June 2018. Prior to the change, contractor Access ID Cards were not assigned expiration dates. The Access ID cards issued to volunteers, interns, and board/committee members are not assigned an expiration date.

### ***County Police (Sworn Officers):***

While in the police academy, police candidates receive a temporary police candidate ID card that is active while they are in the academy. For each recruit class, an officer within the Police Recruitment department sends SSD a list of candidates enrolled within the academy. During an

---

<sup>1</sup> The word "contractor" being used in this context does not refer to volunteers, interns, or board/committee members. It refers to persons who are performing services for the County under a procurement contract.

initial meet and greet between SSD and the recruits, the Police Recruitment department and the Program Specialist make an appointment for the recruits to receive their temporary police candidate ID cards. Following, the SSD Program Specialist validates the recruit's identification, creates a cardholder profile for the recruit within Kantech, takes the recruit's photograph, and provides the recruit with his/her temporary police candidate ID card.

MCPD has an established process for notifying SSD prior to police candidates graduating from the academy. The SSD Program Specialists create a new cardholder profile for each graduate who will receive an Access ID card, and the sworn officers receive their Access ID cards as part of their graduation. The Police Recruitment department is tasked with collecting and returning all temporary cards from graduates and candidates who do not graduate.

### ***Other Procedures:***

The Program Specialists also described the procedures they follow for the following situations:

- Granting additional access to existing Access ID cards
- Issuing Access ID cards for retiring police officers and police interns/civilians
- Reissuing lost or stolen Access ID Cards
- Deactivating Access ID cards for separated County employees, suspended County employees and police officers, and terminated contractors and non-employees

Each department is responsible for collecting and returning the separated employee's Access ID card(s) to SSD for destruction. There is no formal process for returning a contractor or non-employee Access ID card.

## **Scope and Methodology**

The program assessment initiated in June 2018 and fieldwork completed in December 2018. The assessment focused on controls in place at the time of the assessment. EAI also provided an Access ID card data dump from the SSD's Kantech system on July 16, 2018 in an attempt to perform data analytics.

The assessment focused on the following areas:

1. SSD's Access ID card program, specifically:
  - a. The process(es) for obtaining an Access ID card
  - b. The process(es) for adding/removing facility access rights for an active Access ID card
  - c. The process(es) for deactivating an Access ID card
  - d. The roles and responsibilities of other departments in issuing and modifying access to County facilities
2. Access ID card database maintenance

SC&H conducted a documentation review of existing policies and procedures, met with SSD and other County officials to understand the processes followed in the areas referenced above, and met with EAI personnel to better understand the structure and capabilities of the Kantech system.

# Findings and Recommendations

## Observations:

Policies and Procedures. SC&H reviewed current and proposed SSD policy/procedure and related documentation. The Security Services Division ID Card Standard Operating Procedures document reviewed was in draft form, but the documented processes in the draft reflect current procedures. Through review, it was determined that this document was more of a high-level policy document that outlines requirements for each Access ID card-related process such as card issuance, adding/removing access, and deactivation. However, it does not include a sufficient level of detail or completeness to be considered an effective set of standard operating procedures.

Process Walkthroughs. SSD has experienced turnover in the Program Specialist position and some of the personnel who filled the position over the years did not have formal Kantech training. The lack of experience and training of personnel who administered the Access ID card system was noted as the reason for inconsistently applied procedures, and a resulting loss of cardholder data integrity within Kantech discussed below.

Historically, when personnel or contractors/non-employees no longer need access to County facilities, the Access ID card record was deleted from Kantech. This resulted in the loss of cardholder activity that may be important for future reference or investigation. Following the program assessment's commencement, SSD modified the process to deactivate the card, retain the data for 90 days, and then delete the card record from Kantech.

Access ID card-related requests can be received from an authorized department representative through multiple channels:

- Emailing the SSD access request email address which generates a request ticket within Remedyforce
- Emailing the SSD department email
- Emailing a Program Specialist directly
- Calling a Program Specialist

For the last three channels, the Program Specialist is supposed to manually create a request ticket in Remedyforce based on the received email/phone call. However, there is a lack of consistency with how Access ID card requests are tracked. Requests received by email or phone are not always entered into Remedyforce. Further, tickets received through the SSD access request email address could be worked from the resulting Remedyforce ticket, or directly from the email request.

Kantech System and Data. SC&H met with representatives from EAI to review Kantech capabilities related to Access ID card administration and reporting. There are 40 customizable fields (out of 88 fields) within each cardholder profile that are available for use. Each of these fields begins with a generic field name and can then be customized at the discretion of SSD to reflect the information to be collected for each cardholder. Of the 40 customizable fields, SSD has defined four fields in Kantech:

- Field 1: Department
- Field 2: ID Card Bar Code
- Field 6: First Name
- Field 7: Last Name

While other fields may contain data/information, SSD has not designated/defined the fields in Kantech as containing specific information. SC&H also discussed data issues with the Program Specialists and noted the following:

- Kantech does not prevent multiple records with the same user name from being created.
- SSD does not apply unique identifying information, such as an employee ID number for County employees, or last four digits of a Social Security Number or other identifier for non-employees, to differentiate between employees (other than sworn police officers, for whom the badge number is recorded). SSD uses other fields such as middle name or department to differentiate the employees.

Data Analytics. EAI provided Kantech reports with authorized users of Kantech (County employees, EAI personnel, and Strathmore<sup>2</sup> employees), active County employees, and County employees who had left County employment within the last three years. Using the Access ID card data maintained by SSD, SC&H attempted to conduct data analytics focused on the following audit objectives:

- A. Evaluate the accuracy of active Access ID cards within the County
- B. Ensure that new Access ID card requests are properly supported, approved, and processed timely
- C. Ensure that users who no longer have a business need for physical access to County facilities are identified and their access rights are disabled within Kantech timely

After reviewing the Kantech reports, SC&H determined that the Access ID card data maintained within Kantech did not allow for substantive and detailed testing required to complete audit objectives A-C. Specifically:

**Objective A: Evaluate the accuracy of active Access ID cards.** A population of active Access ID cards could not be accurately/reliably confirmed because the data provided contained conflicting/inaccurate access ID card statuses, which increases the risk of inaccurate results. The data do not include Employee ID number as a unique identifier and include conflicting data (such as instances where the same employee was listed multiple times) based on preliminary testing procedures.

**Objective B: Ensure that new Access ID card requests are properly supported, approved, and processed timely.** In addition to the data issues noted for Objective A above, there is no centralized repository to store and manage new Access ID card requests. As noted above, there is a lack of consistency with how Access ID card requests are tracked: SSD does not consistently enter, process, assign, prioritize, resolve, and track all access-related requests in Remedyforce. Requests received by email or phone are not always entered into Remedyforce. Further, new hire documentation such as a Personnel Action Form or employment verification form is not collected from County employees given Access ID cards during their new hire orientation. SSD relies on the new hire list provided by OHR as verification that the employee should receive an Access

---

<sup>2</sup> Strathmore is a cultural and artistic venue and institution that is a public-private partnership between Strathmore Hall Foundation, Montgomery County, and the State of Maryland. SC&H found that Kantech user IDs were assigned to Strathmore personnel and the decision was made to include Strathmore access to Kantech in the scope of the additional procedures performed.

ID card. As a result, SSD does not have the employee's ID card application and supporting documentation on file.

**Objective C: Ensure that users who no longer have a business need for physical access to County facilities are identified and their access rights are disabled within Kantech timely.** SC&H identified 469 terminated employees who still had Access ID card profiles. However, the number of terminated employees with active Access ID card profiles may be greater than 469, since SSD does not use employee ID numbers as unique identifiers to identify County employees within Kantech. Further, the Kantech and the County's Oracle Enterprise Resource Planning (ERP) systems are maintained separately and data inputs for the same employee may differ within each system (Robert vs. Bob).

User Access to Kantech. SC&H used the Kantech reports to 1) identify all users that could modify and print cards and 2) identify which users had rights that allowed them to assign/grant access to County facilities. Based on the workspace and security level configurations, SC&H identified the following:

Organization	Number of Kantech User IDs with Specified System Rights	
	Rights to Modify and Print Access ID Cards	Rights to Grant Access to All County Facilities (excluding DOCR facilities)
SSD	6	5 <sup>a</sup>
EAI	4	4
MCFRS	2 <sup>b</sup>	0
MCPD	1	1
Strathmore	5 <sup>c</sup>	0
Unidentified <sup>d</sup>	3	2
Total	21 <sup>f</sup>	12

- <sup>a</sup> SSD has two generic Kantech user IDs, which were last logged in from an SSD Program Specialist's workstation in 2016.
- <sup>b</sup> MCFRS has one Kantech user ID that is shared by two employees and that has rights to modify access to all MCFRS facilities and doors.
- <sup>c</sup> Strathmore has one generic Kantech user ID.
- <sup>d</sup> Three user IDs could not be attributed to a specific department based on available information.
- <sup>f</sup> Ten of 21 user IDs have the ability to modify and print Access ID Cards have not logged into Kantech within the previous 12 months.
  - Two user IDs are assigned to SSD
  - One user ID is assigned to EAI
  - One user ID is assigned to MCFRS
  - Three user IDs are assigned to Strathmore
  - Assignment of three user IDs could not be determined

Roles of Other Departments in Issuing Access ID Card and Modifying Access to Facilities. SC&H met with MCFRS, DOCR<sup>3</sup>, Strathmore, and EAI representatives and discussed the role of SSD in the administration of the Access ID cards of their department personnel. SC&H reviewed the card profiles in the Access ID cards database that listed MCFRS, DOCR, and Strathmore as the

<sup>3</sup> The Department of Correction and Rehabilitation (DOCR) uses a separate security system to control employee access within DOCR facilities. Therefore, Kantech does not control access into (since such access is controlled through physical security controls and processes), nor access within, DOCR facilities.

cardholder's department, identifying instances where notes indicated actions taken by SSD personnel.

- MCFRS manages Access ID cards through Kantech for its personnel by assigning access rights to specific MCFRS facilities and printing the Access ID card to be given to the new MCFRS employees. MCFRS relies on SSD to create card profiles in Kantech, add basic cardholder information during new hire onboarding, and assigning access to non-MCFRS facilities for MCFRS employee Access ID cards.
- Strathmore manages access to Strathmore<sup>4</sup> for Strathmore personnel and relies on SSD for assigning access to non-Strathmore facilities for Strathmore personnel.
- DOCR does not use Kantech for access to its facilities but relies on SSD for assigning access to non-DOCR facilities for DOCR personnel.

#### Other Issues Noted

- SSD maintains a hard copy Authorized Signature Binder that is used as the resource for Program Specialists to validate that Access ID card requests are made by County personnel with the appropriate authorization. The Authorized Signature Binder has not been updated on a recurring basis to ensure that the information in the binder is complete and accurate.
- Both Program Specialists have Administrator-level access in Kantech. Administrator accounts allow the user to add, edit, and remove access for any cardholder. There is no process in place to monitor or review Administrator level activity for quality assurance or appropriateness, business purpose, or support.
- Approximately 320 Access ID cards were issued to generic cardholder profiles requested by specific departments (e.g., Health and Human Services, MCFRS) for facilities operated by those departments, rather than to specific individuals. Requests are made by authorized County personnel to have Access ID cards created that can be shared or passed along to subsequent users, and it was customary for SSD to provide these cards when requested, with the understanding that such Access ID cards would be the responsibility of the requesting department to control and manage such cards. Access rights on these cards were limited to specified, department-operated facilities.

SC&H identified 10 findings related to the SSD Access ID Card Program. Findings, associated risks, and recommendations are detailed below.

#### **Finding 1: Policies and Procedures**

**SSD does not have formalized and adequately documented standard operating procedures (SOPs) in place to facilitate SSD training and succession planning.**

SSD is in the process of drafting and finalizing the Security Services Division ID Card Standard Operating Procedures. While, the draft policy is near completion, SSD does not have a documented SOP capturing step-by step guidance for administration of the Access ID card

---

<sup>4</sup> Beginning in January 2019, the Strathmore Vice President of Operations assumed responsibility as the Access ID card administrator for Strathmore cardholders and access. Previously the Director of Security at Strathmore was the Access ID badge administrator. Currently, the Strathmore Director of Security position is vacant.

program and systems. SC&H noted during the program assessment that the two Program Specialists who are responsible for managing the Access ID card program do not appear to perform the same steps to complete department procedures.

### Risks

1. Outdated or undocumented processes can result in inconsistencies in the execution of the administration of physical access, particularly when there are staff transitions.
2. Lack of detailed procedural documentation increases the risk of interruption in business continuity.

### Recommendation 1.1

SSD should review, update, and finalize its draft policy and consider expanding to include detailed instructions on how to receive, process, and close Access ID card related requests. This will help SSD ensure that processes are performed in a consistent manner and limit the loss of undocumented business process knowledge through turnover, retirement, or resignation. The updated policy and procedures document should also address relevant Access ID card responsibilities performed by non-SSD personnel, as well as responsibilities of SSD personnel for MCFRS, DOCR, and Strathmore personnel.

### Recommendation 1.2

Once finalized and implemented, SSD Management should implement a required policy to annually review the policy/SOPs and update as necessary. SSD Management should also ensure, through sample testing or other means, that the policy and SOPs are adhered to.

## **Finding 2: Inefficient Process for Receiving Requests Related to Access ID Cards**

**Access ID Card related requests are received through multiple channels and are not centralized for processing.**

Through inquiry, we learned that there is not a single all-inclusive method for capturing and routing Access ID card-related requests to SSD for processing. Authorized department representatives (for new card access) and employees (for lost/stolen cards) can currently notify the SSD through multiple avenues:

- Email: POL..ssdrf@montgomerycountymd.gov
- Email: SSD Helpdesk Ticket email
- Email: Directly to a Program Specialist's personal County email
- Phone call: Directly to a Program Specialist

The method of request submission impacts whether a ticket is generated within the Remedyforce system. Further, both Program Specialists are jointly responsible for monitoring the SSD Helpdesk Ticket Inbox and expected to keep track of and resolve requests which they opened. A formal method of assigning or labeling emails is not in place. As a result, the ability to assign, prioritize, monitor productivity and effectiveness by comparing received/resolved date, and understand volume is negatively impacted by requests processed outside of Remedyforce.

## Risks

1. Without centralized request intake and tracking, system and personnel resources may be deployed ineffectively or inefficiently towards the completion of access-related requests.
2. There is no accurate or reliable way to track the volume of access related requests performed by each Program Specialist to balance workload, or to manage and monitor timeliness of resolutions or assess productivity.
3. Access ID card requests may not be processed timely, or at all, impacting the physical security of County personnel, facilities, and information.

## Recommendation 2.1

SSD should consider consolidating the method of submission for Access ID card requests (e.g. through a single channel method) and requiring all authorized department personnel to submit requests accordingly. This would allow for increased efficiency and more effective management and oversight of the program. As part of this process, SSD Management should perform a formal, comprehensive evaluation of the capabilities and functionality of Remedyforce to determine whether the system can be effectively used to manage SSD's Access ID card program. If Management determines that Remedyforce is the appropriate solution, SSD should re-design the Access ID card process workflow to direct access request activity solely through Remedyforce.

## **Finding 3: Improvements Needed to Ensure Quality of Access ID Cardholder Data**

**A formalized process is not in place to validate the accuracy of active Access ID cardholders on a defined periodic basis. In addition, opportunities to improve data quality through the use of a unique identifier, such as the employee ID for County employees, are not being implemented. Further, the data download of Kantech cardholders found in the system identified approximately 320 Access ID cards that were issued to generic cardholder profiles, rather than to specific individuals.**

Cardholder data integrity issues were noted during the conduct of the program assessment. While SC&H was advised that SSD is currently performing an internal review of the Access ID cardholder database to "clean-up" the cardholder information and card data found in Kantech, no formal process is documented requiring a periodic review of the cardholder data to ensure its integrity.

In addition, SSD does not currently use a unique identifier such as employee ID to easily and accurately identify each cardholder. Differentiating between two users with the same name requires manual research by a Program Specialist to ensure the correct cardholder is identified (middle name, department, job title, etc.). SC&H was advised that in July 2018, SSD began recording employee ID numbers for any new Department of Liquor Control (DLC) Access ID cards, but that this is only performed for DLC personnel because the department is providing SSD with the information. SSD did not formally define a field in Kantech to capture or require employee ID numbers. SC&H was advised that Program Specialists re-purposed a blank field to informally capture this information for the new DLC employees.

- SSD has not coordinated with OHR to require an employee ID number during the onboarding process

- While SSD is currently performing its internal review and clean-up of the Access ID cardholder database, employee ID numbers are not being retroactively added to cardholder profiles
- SSD does not require periodic formal reviews of active Access ID cards to confirm accuracy of Kantech and active cards

### Risks

1. Active Access ID cards held by terminated or unauthorized individuals can result in unwarranted access to County buildings or information.
2. The lack of a defined periodic review of active Access ID cards increases the risk that cards belonging to unauthorized individuals remain active within Kantech.
3. The lack of properly defined and consistently used fields creates unreliable data, negatively impacting the ability to effectively manage access to County facilities.
4. Access ID cards issued to a generic user (rather than to a specific individual), limits SSD's ability to resolve misappropriation of County assets or other access related incidents.

### Recommendation 3.1

As part of the current internal review and cardholder data update being performed by SSD of the existing cardholder data in Kantech to improve data integrity, allow for accurate reporting, and ensure that existing cardholder data allows for the consistent application of new processes. This cardholder data update process should address the following:

- SSD should consider establishment of appropriate unique identifiers for each card category (e.g. employee ID for County employees) and should formally review, identify, define, and document consistent, mandatory fields for each cardholder profile within Kantech. For contractors, SSD should consider requiring the collection and recording of unique fields to be used to identify contractors, such as applicable contract number, and responsible using/authorizing department. This would allow for improved tracking and accountability of contractor personnel. Appropriate processes to obtain and include the unique identifiers should be formalized and incorporated in the standard operating procedures and applications.
- SSD should work to reduce the number of Access ID sub-category card types from the current 50 sub-categories. The amount of role types increases the level of effort necessary to properly ensure assigned roles and accesses are appropriate and effectively controlled.
- Ensure that all Access ID cards issued to general or generic cardholder profiles can be accounted for by the using department, and that continued need for each card is validated.

### Recommendation 3.2

To promote increased data integrity of the cardholder data in the future, SSD should implement a regular review of the Access ID cardholder data in Kantech, including the need for cards issued to general or generic cardholder profiles.

#### **Finding 4: Removal of Cardholder Access**

**Improvements are needed to ensure County facility access changes for contractors and non-employee personnel are updated timely.**

Through inquiry, SC&H determined that current SSD practices that rely on County departments to notify SSD when contractor or non-employee personnel are no longer authorized to access County facilities and to return to SSD contractor and non-employee Access ID cards once they no longer perform work for the County do not consistently result in timely removal of cardholder access and return of Access ID cards for personnel that are no longer authorized access.

Risks - Contractor or non-employee personnel could retain unauthorized access to County personnel, facilities, and information.

#### **Recommendation 4.1**

SSD should consider implementing expiration dates for contractor and non-employee personnel card categories. Specifically, SSD Management should consider:

1. Establishing and enforcing expiration dates (preferably no longer than one year) for all contractor and non-employee personnel Access ID cards.
2. Prior to the expiration date, require contractor and non-employee Access ID card application to be completed and signed by authorized department representatives. This will help to ensure that contractor and non-employee personnel do not retain unwarranted facility access beyond their approved relationship with the County.

#### **Recommendation 4.2**

SSD should consider other changes to strengthen control over contractor and non-employee personnel Access ID cards, including, but not limited to the following:

- Issuing guidance to departments regarding off-boarding of contractor/non-employee personnel that would require collection and return of the Access ID card;
- Using the “Card Type” and “Department” fields within Kantech, identify the population of contractor cardholders specific to each department and work with department contacts to identify and record the corresponding contract administrator; and designate an unused field within Kantech to record the contract administrator for each contractor cardholder.
- Changing characteristics (e.g. color) of the ID cards for all contractor and non-employee personnel each year.
- Working with the Office of Procurement to explore potential changes in Contractor Administrator training and other process changes to emphasize the responsibilities of Contractor Administrators in ensuring that contractor employee Access ID cards are deactivated and collected/returned to SSD timely.

#### **Finding 5: Record Retention**

**SSD documentation to support authorized department representatives designated to approve Access ID card related requests should be regularly updated to ensure it is current and accurate.**

SSD maintains an Authorized Signature Binder that is used as the resource for Program Specialists to ensure the approval provided on an access-related request is from an authorized department representative. The binder contains the names of County employees organized by

department who are authorized to approve Access ID card requests, and their corresponding signature. Program Specialists are responsible for reviewing and updating the binder regularly to ensure accuracy. However, the Authorized Signature Binder is not updated on a consistent basis. Currently, Program Specialists rely on internal and historical knowledge of County personnel to verify that the employees submitting Access ID card ticket requests are authorized department representatives.

Risks - Access ID cards could be approved by unauthorized individuals, resulting in unwarranted access to County personnel, facilities, or information.

#### Recommendation 5.1

SSD should establish a documented periodic review of the Authorized Signature Binder to ensure department representatives listed are complete and accurate.

#### Recommendation 5.2

SSD should consider the feasibility of investigating and implementing an alternative system-based approach for Access ID card related requests to be routed based on established workflows for review and approval. An automated solution will rely on established system workflows to route applications to authorized personnel for review and approval and would eliminate the need to retain and update a manual binder of approved County personnel who can approve Access ID card applications.

### **Finding 6: Record Retention**

**Access ID cardholder history is set to be deleted following expiration or status change to inactive.**

SSD recently implemented a change that Kantech Access ID cardholder profiles and history are set to be deleted/erased within 30 days of expiration without consideration of potential retention needs. Prior to June 2018, card history and cardholder profile were both deleted immediately upon expiration or deactivation.

Risks - Deleting card history and cardholder profiles immediately after deactivation results in the inability to utilize card access history and could impact incident investigations.

#### Recommendation 6.1

SSD, in coordination with the Office of the County Attorney, should determine an appropriate retention period for all card activity and cardholder profiles. SSD should then document this retention period in their standard operating procedures and implement the retention period as timely as possible.

### **Finding 7: Record Retention**

**A formalized process is not in place to communicate with department heads regarding reported lost/stolen cards or to ensure all inactive ID cards are collected and destroyed.**

There appears to have been more than 100 cards recorded as lost or stolen in Kantech. It is uncommon for departments or terminated employees, contractors, and other non-employees to return Access ID cards to SSD for proper disposal and destruction. This information is not currently captured in Kantech to be quantified.

Additionally, there are no processes in place for SSD to report to department management instances of repeated loss of Access ID cards by an individual or failing to return cards upon separation from the County.

#### Risks

1. Lost, stolen, or unreturned access cards can remain active and result in unwarranted or unauthorized access to County buildings.
2. Excessive lost or stolen cards can result in increased replacement costs and inefficient use of resources needed to process these types of requests.

#### Recommendation 7.1

Upon receiving Access ID card replacement requests, SSD should notify department management of each incident. Further, on a periodic basis, SSD should trend lost or stolen activity and notify department management for personnel training and/or correction.

#### Recommendation 7.2

SSD should consider adding a field in Kantech to capture whether an inactive Access ID card was collected and destroyed.

#### Recommendation 7.3

SSD should consider issuing a periodic reminder of the importance of supervisors fulfilling their responsibilities during the employee and non-employee exit process, including the importance of collecting the Access ID card from departing personnel.

### **Finding 8: Kantech User Access Oversight and Segregation of Duties**

#### **Authorized User Access to Kantech should be periodically reviewed and validated.**

The list of users with authorized access to Kantech is not current. There is not currently a process in place to review Kantech user access on a defined, recurring basis to ensure that personnel with access to Kantech have an appropriate need for access.

#### Risks:

1. The lack of appropriate monitoring of Kantech access could result in inappropriate and unauthorized changes to card profiles or accesses.
2. The use of a generic user ID card prevents individual accountability for all changes made to card profiles and accesses.

#### Recommendation 8.1

The SSD Director should ensure that the current list of users with authorized access to Kantech is updated, and should establish a defined, periodic review of user ID access and rights within Kantech to ensure that User IDs that no longer support a continued business need are deactivated. Further, SSD should ensure that all Kantech users have a unique user ID and password, and that users are limited to one user ID. The documented Access ID Card policy should prohibit sharing user IDs and passwords with other individuals or issuing multiple user IDs to the same user.

### **Finding 9: Kantech User Access Oversight and Segregation of Duties**

**Administrator level access and activity in Kantech is not monitored for appropriateness or compliance with expected procedures.**

Both Program Specialists have Administrator-level access in Kantech. Currently, there is no process in place to monitor or review Administrator level activity for appropriateness, business purpose, or support. Further, a process is not in place to monitor administrative user activity for quality assurance or appropriateness of changes on a periodic basis.

Risks - Lack of monitoring over Administrator access can result in undetected/undesired behavior an increased risk of segregation of duties conflicts.

#### **Recommendation 9.1**

The SSD Director should periodically review Administrator activity audit reporting and select a sample of access related changes to evaluate for appropriateness, business purpose, documentation support, and policy compliance. Per EAI, the Operator Report is available within Kantech and provides the history of cards accessed and changes made by each User ID. The review should be documented, and unexpected activity should be reviewed, discussed, and resolved.

### **Finding 10: Training of SSD Personnel**

**SSD personnel do not receive adequate Kantech and Remedyforce training.**

The lack of experience or training of Program Specialists hired in 2014 and volunteer/intern personnel who were responsible for administering the Access ID card program from 2014 through July 2017 appears to have contributed to data and process consistency issues. Additionally, the lack of training provided to the current Program Specialists has resulted in the inability to utilize all system capabilities and functionalities, leading to decreased efficiency. The SSD Director also has not received adequate Kantech training, which impacts the level of possible oversight and management for the Access ID card program activities and personnel.

Further, no formal Remedyforce training has been provided to the Program Specialists or the SSD Director, which has impacted its adoption and prevented the realization of potential system-provided efficiencies such as the ability to enter, process, assign, prioritize, resolve, track, and manage all access related requests.

Risks - Lack of formal system training sufficient to understand the system capabilities can result in inefficient and ineffective use of resources (systems and personnel), as well as inconsistent processes and unreliable data for reporting and monitoring.

#### **Recommendation 10.1**

SSD should establish and document a formal training plan to ensure the SSD Director and the Program Specialists have an adequate level of understanding of the system and their capabilities to properly use and maximize the opportunities for efficiencies available with the systems in place to perform the roles and responsibilities associated with the Access ID card program.

## **Comments and MCIA Evaluation**

We provided the Montgomery County Police Department (MCPD) with a draft of this report for review and comment on January 28, 2019 and MCPD responded with comments on February 21, 2019. MCPD's response notes the progress the department has made since the initiation of the review in addressing findings, as well as some of the challenges they will face in the future. The report findings and recommendations remain unchanged. The MCPD response has been incorporated in the report at Appendix A.

# Appendix A: Montgomery County Police Department Response



DEPARTMENT OF POLICE

Marc Elrich  
*County Executive*

J. Thomas Manger  
*Chief of Police*

February 21, 2019

Dear Mr. William Broglie:

The purpose of this memorandum is to formally acknowledge receipt of the Program Assessment of the Department's/County's Access ID Card Program. I would like to recognize the work by the Office of Internal Audit during this Assessment. More specifically, Mr. William Broglie as the lead auditor and his team comprised of SC&H personnel. Your work has been thorough and insightful. It is obvious that the Department/County continues to face challenges with our ID Access Card Program, and we are working to correct the identified deficiencies. We are also grateful to have additional detail provided to us regarding this system as it pertains to other departments. This information is useful in understanding how other departments use/administer their ID Access Card Programs and how contractor information is tracked by the County. Over the past several months, my staff worked with the audit team to afford unfettered access to information and begin the process of improving our processes. At this point, we are confident that the Department can address all your recommendations given the proper resources, compliance from other departments, and funding.

The remainder of this document will briefly address each of the ten findings and associated recommendations.

## **Finding 1: Policies and Procedures**

**Security Services Divisions (SSD) does not have formalized and adequately documented standard operating procedures (SOPs) in place to facilitate SSD training and succession planning.**

The Department has created an overall SOP/Policy for the processing, issuance, deactivation, and deletion of Kantech Access ID cards (Kantech cards). A more detailed training manual will be developed with the assistance of experts from Kantech and/or EAI. We acknowledge the best practice of having multiple employees trained in this system. The need for regular use of the system, however, hampers this ability since SSD works with a very limited staff. The majority of the SSD staff are also unable to be effectively cross-trained on Kantech due to their assigned primary duties and limited time to use the system each workweek. This limitation requires a dedicated Program Manager to oversee and supervise the two employees whose primary responsibilities include the daily use of the Kantech system. This Program Manager would also audit the system, review and edit SOPs, and ensure compliance with SSD policies pertaining to the Kantech system.

---

Office of the Chief of Police

Public Safety Headquarters • 100 Edison Park Drive • Gaithersburg, Maryland 20878  
www.montgomerycountymd.gov • www.mymcpnews.com • MCPDChief@montgomerycountymd.gov

montgomerycountymd.gov/311  Maryland Relay 711

**Finding 2: Inefficient Process for Receiving Requests Related to Access ID Cards.**

Captain Paul Starks has been working with Remedy Force, and coordinating with Director Michael Gordy, to ensure that all Kantech system work requests flow solely through Helpdesk tickets. This has been occurring to some degree but not entirely. The SSD staff, in the spirit of customer service, has allowed requests to flow through phone calls and emails without always requiring a helpdesk ticket. While we appreciate the spirit of our staff to assist other departments, the lack of data from helpdesk tickets presents challenges in assessing workload. This is again another area where a dedicated Program Manager can effectively ensure compliance to staff exclusively responding to helpdesk tickets. It should be noted, however, that without compliance by all departments there is a risk that certain Kantech cards will not be deactivated if a request is not sent via the helpdesk. This will be a cultural shift for some departments.

**Finding 3: Improvements Needed to Ensure Quality of Access ID Cardholder Data.**

SSD is currently auditing the system one building at a time to ensure accuracy of Kantech profile and access information. We are working directly with each department's Building Representative to accomplish this task. SSD relies heavily on information from each county department to update Kantech cardholder data. Any delay, or lack of communication, to SSD by other departments regarding Kantech cardholders will create "quality" concerns. This part of the process will continue to remain a challenge for SSD. The volume of work for the two employees in SSD is in the tens of thousands for Kantech card requests and audit verifications each year. Once we are able to successfully complete this initial audit of all buildings a recurring building audit will be in place beyond normal data exchange between other departments and SSD. All departments have been advised to notify SSD of any changes to an employee's cardholder status. Any quality assessment would likely be random reviews of cardholder permissions along with annual audit of each building. Additionally, SSD has recently been allowed to access Oracle numbers as a unique identifier. SSD plans to update Kantech profiles with these numbers following this initial audit of buildings. Generic cards do still exist but have been reduced to those required for Fire Rescue to access buildings and all others specifically requested to the Director of SSD by a particular department. Additionally, we are now using Oracle numbers in Kantech profiles when on-boarding new employees.

**Finding 4: Improvements are needed to ensure County facility access changes for contractors and non-employee personnel are updated timely.**

Again, SSD is reliant upon this information coming from County departments hiring contractors or on-boarding non-employees. The CAO and SSD sent out reminder email messages regarding the process of notifying SSD of non-employees being removed from the Kantech system. SSD has implemented a one-year expiration date for all contractor Kantech cards (effective July 1, 2018). Additionally, SSD has explored the potential of turning off all Kantech cards which have not been used in the past 45 days. Unfortunately, according to EAI, this would have resulted in 7,000 cards being deactivated. EAI has explained that this is since not all cardholders need to use their card to access buildings. A decision to turn off cards based on this criteria, or similar factors, could result in an unintended spike in requests to reactivate cards.

**Finding 5: SSD documentation to support authorized department representatives designated to approve Access ID card related requests should be regularly updated to ensure it is current and accurate.**

SSD is now reviewing the "Signature Binder" annually. Department heads will also receive email messages from SSD indicating who is listed as authorized signators for each respective department with a note to immediately notify SSD of any changes. This email to Department heads will occur twice per year.

**Finding 6: Record Retention**

**Access ID cardholder history is set to be deleted following expiration or status change to inactive.**

SSD has been deactivating, but not deleting, cardholder history since May of 2018. The deactivated card history is retained for three years. This is specifically delineated in the SSD SOP.

**Finding 7: A formalized process is not in place to communicate with department heads regarding reported lost/stolen cards or to ensure all inactive ID cards are collected and destroyed.**

These findings are two distinct issues. The first issue of lost/stolen id cards can only come to the attention of SSD from the employee or respective department. SSD has implemented a new SOP that requires notification to each department signator (by SSD) prior to issuance of a replacement Kantech card. It should be noted, however, that SSD has always required a police report to be on file prior to the issuance of any Kantech card and the old card has always been deactivated at the time they are notified of the card being lost or stolen.

The issue of the collection of cards revisits the SSD reliance on other departments to have cards turned in to SSD. Once cards are received a notation is made in the deactivated profile, along with the SSD staff initials, and the card is shredded. If a card is not received, under the new SSD SOP, a notice will be sent to the department signator. Again, it should be noted that SSD is reliant upon outside departments to comply with our processes.

**Finding 8: Kantech User Access Oversight and Segregation of Duties**

**Authorized User Access to Kantech should be periodically reviewed and validated.**

**Finding 9: Kantech User Access Oversight and Segregation of Duties**

**Administrator level access and activity in Kantech is not monitored for appropriateness or compliance with expected procedures.**

The Kantech system requires a level of technical expertise and repeated use to successfully review and validate data/entries in the system. The two most knowledgeable staff are the two Program Specialist entering thousands of cards profiles and permissions each year. Each of these specialists have collateral duties which also create other demands that can interfere with Kantech entries and do not afford much, if any, time for a review of work. The SSD Lieutenant overseeing these specialists is scheduled for training on the system, but has the responsibility of supervising all SSD guards in the County. This Lieutenant has limited time to conduct reviews and the program would greatly benefit from a dedicated Program Manager to oversee Kantech.

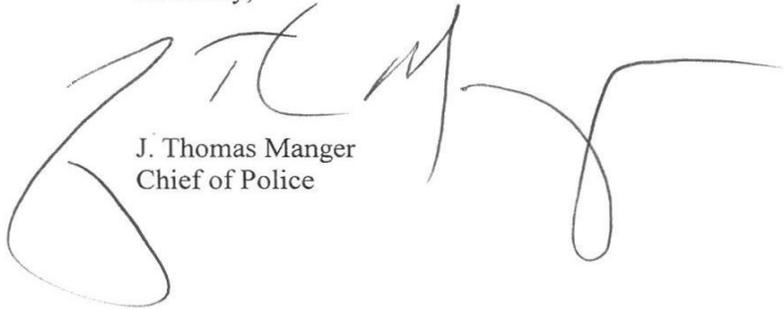
**Finding 10: Training of SSD Personnel**

**SSD personnel do not receive adequate Kantech and Remedyforce training.**

Captain Paul Starks has been assigned to specifically focus on the issue of Kantech and has scheduled training for additional SSD personnel to include the Director of SSD and his Lieutenant who has oversight of Kantech. Kantech personnel have conducted refresher training for the two current Program Specialists assigned these duties. They reported that this training was a good review for them of the system. Refresher training will be held annually for all SSD personnel with access to the system.

Again, I appreciate the work of the Office of Internal Audit and my staff will remain available to answer any further questions that may arise in the future.

Sincerely,

A handwritten signature in black ink, appearing to read 'J. Thomas Manger', is written over the typed name. The signature is fluid and cursive, with a large loop at the end.

J. Thomas Manger  
Chief of Police