



Internal Audit
Department

301 W Jefferson St
Suite 660
Phoenix, AZ 85003

[maricopa.gov/
internalaudit](http://maricopa.gov/internalaudit)
602.506.1585

Ross L. Tate
County Auditor

Protective Services Department

July 2016

*Internal Audit Report Authorized by the
Maricopa County Board of Supervisors*

Report Highlights	Page
Panic alarms were working properly; panic alarm testing documentation will be strengthened.	1
Controls over badge access will be improved.	2
Background check procedures will be enhanced.	5
Records retention requirements will be developed; policies and procedures will be updated.	5
Strategic plans will be updated.	9
Controls over information technology (IT) will be improved.	10
Training is monitored; some officers' first aid certifications have expired.	15
Revenue and cash procedures will be documented.	16
Controls over weapons inventory and equipment will be enhanced.	18

Objectives	To determine that Protective Services': <ul style="list-style-type: none">• Controls over Command Center operations are sufficient.• Building access and identification badge controls are sufficient to ensure appropriate facility access.• IT general and critical application controls over data confidentiality, integrity, and availability are adequate.• Officers are receiving and maintaining the appropriate level of training to perform their job duties.• Controls over cash and revenues are adequate.• Tactical equipment is restricted and tracked appropriately.
-------------------	---

Scope	This audit primarily focused on controls in place in FY 2016. To perform this audit we: 1) interviewed PS management and staff, and Office of Enterprise Technology (OET) staff; 2) observed PS Command Center operations and cash controls; 3) tested panic alarms and badge access; and 4) inventoried equipment. We reviewed: policies and procedures, one contract, badge requests, training and inventory logs, and other supporting documentation.
--------------	--

Standards	This audit was approved by the Board of Supervisors and was conducted in conformance with International Standards for the Professional Practice of Internal Auditing. The specific areas reviewed were selected through a formal risk-assessment process.
------------------	---

Auditors	Stella Fusaro, Audit Manager, CIA, CGAP, CRMA, CFE Christina Black, Audit Supervisor, CIA, CGAP, CRMA Susan Adams, Senior IT Auditor, MBA, CISA, ITIL, CLEA Dan Griedl, Senior Auditor, CIA Megan McPherson, Senior Auditor, MEd Kenton Schaben, Internal Auditor
-----------------	--

This report is intended primarily for the information and use of the County Board of Supervisors, County leadership, and other County stakeholders. However, this report is a public record and its distribution is not limited. We have reviewed this information with Protective Services' management. The Action Plan was approved by Jim Brown, Protective Services Chief, and Reid Spaulding, Deputy County Manager, on July 19, 2016. If you have any questions about this report, please contact Stella Fusaro, Audit Manager, at 602-506-1777.

Audit Results

Issue #1: Panic Alarms

Observation: We tested 21 Administrative Building panic alarms to determine that controls were sufficient. We found all tested alarms alerted the Command Center; however, controls could be improved. Tests were not documented in a panic alarm log book as stated in policy. In addition, Protective Services' (PS) was not able to provide a list of all 1,300 countywide panic alarm buttons and their locations, or to provide documentation indicating all alarms were tested.

Although the Administrative Building policy and procedures require that panic alarms be tested and logged in a panic alarm log book, the frequency of the required tests was not noted. In addition, PS policies and procedures do not address panic alarm tests for the Human Services Campus and for the Durango Complex. During our site visits to the Command Centers, we observed PS officers logging panic alarm tests in the Daily Activity Logs; however, it would be difficult and labor intensive to determine if all panic alarms were tested using these logs.

Conclusion #1A: All panic alarms in our sample worked properly.	
Recommendation	PS Action Plan
None	N/A
Conclusion #1B: Panic alarm testing documentation is not sufficient to verify that all panic alarms are tested periodically.	
Recommendations	PS Action Plan
1B-1 Update panic alarm policies and procedures, and establish panic alarm testing requirements for all locations. Include the required test frequency.	Concur – in progress We will review current policy & practices, make needed/necessary changes, and assure appropriate documentation as to procedures for testing & frequency. Target Date: 9/2/2016
1B-2 Locate and document the location of all panic alarms and call boxes.	Concur – completed

Recommendations	PS Action Plan
<p>1B-3 Develop a log to track panic alarm and call box testing, and implement periodic testing according to updated policies and procedures.</p>	<p>Concur – in progress</p> <p>We will review current policy & practices, make needed/necessary changes, and assure appropriate documentation as to testing. We'll also assure the creation of a separate log for testing.</p> <p>Target Date: 9/2/2016</p>

Issue #2: Badge Access to Door Card Readers

Observation: We tested a sample of 12 card readers to determine that badge access was appropriate. We found that 58% (7 of 12) of the card readers had what appeared to be excessive access granted. In several instances, the excessive access was to highly secured areas. For example, 451 individuals had access to the Office of the Medical Examiner's (OME) exam room, and 242 individuals had access to the Office of Enterprise Technology (OET) server room.

We also determined that five (42%) of the card readers tested gave access to individuals that were from other agencies, which appeared inappropriate. For example, in addition to giving access to its own employees, the OME exam room card reader granted access to employees from the Department of Transportation, the Sheriff's Office, the County Manager's Office, Human Resources, the County Attorney's Office, Superior Court, Equipment Services, the Office of Procurement Services, and the Department of Finance. The Treasurer's card reader allowed access to employees from the Department of Transportation, Correctional Health Services, Clerk of the Superior Court, and the Sheriff's Office.

We also noted that Facilities Management Department and PS employees are routinely given access to most card readers. According to PS, there is no way to verify that access was approved for individuals for each card reader, because access is assigned by door groups rather than by individual card reader. Excessive or inappropriate badge access could result in unauthorized entry, theft, and unsafe conditions.

Conclusion #2A: Access to some County facilities controlled by card readers appears excessive.	
Recommendations	PS Action Plan
2A-1 Review door groups to ensure proper access is approved and appropriate.	Concur – in progress The entire system is being formally assessed/evaluated by Benson Systems which will address this issue. This is a time-consuming and complex task which may take 6 mos. to 1yr to accomplish. Target Date: July 2017
2A-2 Work with agency management to identify high security areas. Periodically send card reader access reports to management in high security areas so they can verify that access is appropriate.	Concur – in progress The entire system is being formally assessed/evaluated by Benson Systems which will address this issue. This is a time-consuming and complex task which may take 6 mos. to 1yr to accomplish. Managers in various departments will need to take a more active role in our process as they alone know access permissibility. Target Date: July 2017

Issue #3: Badge Access Authorization and Termination

Observation: We tested 24 employees to determine that their badge access was authorized and appropriate. We found that 12 employees had badge access levels that matched the levels authorized on the Photo ID Forms (a form agencies submit to obtain badge access). For the other 12 employees: 11 forms were incomplete, and appropriate access could not be verified. One employee had access levels that did not match the level indicated on the form.

We attempted to verify that contractor badge access was authorized and appropriate. However, PS did not have Photo ID Forms for 7 of the 10 contractors. For the three contractor badges tested, we found one form was missing, one contractor’s access levels were authorized and appropriate, and one contractor had more access than authorized on the form.

We also noted that PS does not track badge creation dates in the badge access system and Photo ID Forms are only retained for one year. This means that most active badges have no source documentation. In addition, no clear documentation exists when access levels are modified. We also noted that the forms do not require specific access level

information, only garage and building information, with time restrictions. This makes determining the appropriateness of approvals and access levels difficult.

We also compared payroll termination records to the badge access system termination log for 1,038 employees. We found that 6 terminated employees were not in the log. We verified that these 6 employees still had active badges. We reviewed 10 contractors to determine that badges were set to expire per PS policy and found no exceptions.

Conclusion #3A: PS did not have sufficient documentation to show that access levels were approved for selected employees and contractors.	
Recommendations	PS Action Plan
3A-1 Develop procedures that will address how incomplete Photo ID Forms will be handled.	Concur – in progress We'll address the development of procedures that will address how incomplete photo ID forms will be handled. Target Date: 9/2/2016
3A-2 Capture relevant employee badge information including creation dates in the badge access system.	Concur – in progress We'll make certain the relevant employee badge information becomes a component of the application process and the entry of the information into the system. Target Date: 9/2/2016
3A-3 Enhance Photo ID Forms to require more specific access information.	Concur – in progress Modify photo ID forms as needed/necessary to capture specific, pertinent info, and provide access to limited areas through demonstrated need. Target Date: 9/2/2016
Conclusion #3B: Badge access was appropriately revoked for 99% of terminated employees tested. Six terminated employees had active badges.	
Recommendation	PS Action Plan
3B-1 Enhance and document procedures to ensure badge access is revoked upon employee termination.	Concur – in progress Modify and/or create documentation to assure access revocation at the time of separation. Target Date: 9/2/2016

Conclusion #3C: All contractor badges tested were set to expire according to policy.	
Recommendation	PS Action Plan
None	N/A

Issue #4: Background Checks

Observation: PS conducts background checks prior to issuing badges to employees and contractors. We selected 50 employees and 10 contractors and verified that PS performed background checks for 30 of 50 (60%) employees and 3 of 10 (30%) contractors. PS could not provide documentation for the remaining 20 employees. We could not verify the seven remaining contractors because, although PS stated that they kept records for three years, we found that they only retained records for a year and a half.

Conclusion #4A: Documentation was not sufficient to determine that all background checks were conducted.	
Recommendation	PS Action Plan
4A-1 Update procedures to ensure that background checks are performed and documented. Procedures should address either a secondary reviewer or alternative measures to ensure all background checks are performed.	<p>Concur – in progress</p> <p>Examine current procedures and modify accordingly. A recently modified background checks policy speaks to a “secondary reviewer.”</p> <p>Note: We’re dependent on HR for new-hire information so checks can be completed.</p> <p>Target Date: 9/2/2016</p>

Issue #5: Badge Access and Background Check Policies and Procedures

Observation: We reviewed the PS Access and Key Control Policy and the Background Check Policy, and noted that the policies do not contain specific information for granting badge access. The Access and Key Control Policy mainly covers physical key controls. The Background Check Policy covers the background check process.

We found that PS does not have any policies or procedures related to the physical control of badges. PS indicated that badges not currently in the badge printer are secured in numbered boxes. We reviewed the employee and contractor badge creation forms. We found that an expiration date was present on the contractor form and that an authorized signature was required on both. However, we noted that the forms do not require specific access level information, only garage and building information with time restrictions.

Conclusion #5A: PS' Access and Key Control Policy does not contain specific information on granting badge access and on the physical control of badges.	
Recommendation	PS Action Plan
5A-1 Update badge access policies, procedures, and forms to include more specific requirements for granting badge access. Address procedures for physical control over the badges.	Concur – in progress This is a fairly complex task and the cooperation of the hiring authority in providing us with specific access requirements is essential if this is to be successful. SOP development will probably occur via a contract with a technical writer. Target Date: May 2017
Conclusion #5B: PS' Background Check policy details the process for completing background checks.	
Recommendation	PS Action Plan
None	N/A

Issue #6: Video Security System Recordings

Observation: We reviewed controls over video recording and found that PS does not have policies and procedures. In addition, no documentation exists of video security system training provided to the employees operating the system. Interviewed employees stated they have not received formal training.

Conclusion #6A: PS does not have policies and procedures for video recordings.	
Recommendations	PS Action Plan
6A-1 Develop policies and procedures for video recording. Consider using the U.S. Privacy Act of 1974 and the Department of Homeland Security's Best Practices for Government Use of CCTV in developing these policies.	Concur – will implement with modifications We will develop policy as it relates to recording requests, associated documentation, etc., to include authorizations and approvals. We will utilize Homeland Security "Best Practices" for new camera additions. Target Date: 10/7/2016

Recommendations	PS Action Plan
<p>6A-2 Ensure video security system operators are trained in the acceptable use and safe operation of the equipment. Ensure that training is documented.</p>	<p>Concur – will implement with modifications</p> <p>Training is site-specific and handled by personnel assigned to the site. We will however create documentation indicating training has been provided. In many instances, it's on-going for several weeks.</p> <p>Target Date: 10/7/2016</p>

Issue #7: Records Retention

Observation: We found that PS does not have a formal records retention schedule or policy. In addition, PS recordkeeping for badge access, background check documentation, and video recordings do not comply with state records retention requirements. We noted that the PS Access and Key Controls policy does not mention any records retention requirements for badge documentation. PS indicated that they keep individual badge access data (the doors individuals have access to, or have tried to access) for one month, but the state records retention requirement is one year.

The PS Background Check Policy mentions that background check logs are kept according to "Record Retention Schedule," but there is no indication of what records retention schedule was used. According to PS, background check logs are kept for three years and background check documents are shredded after the check has been performed. State records retention requirements for background checks are five years for an official copy, six months for any non-official copies, and six years for contractor background checks.

State records retention requirements indicate that surveillance recordings should be retained for 14 days. PS reports that video images are kept anywhere from three weeks to six months depending on the Digital Video Recorder (DVR) capacity.

Conclusion #7A: PS' badge, background check, and video retention practices do not comply with state records retention requirements.	
Recommendation	PS Action Plan
7A-1 Document and implement procedures to ensure compliance with records retention requirements for badge access, background checks, and video recordings. If PS determines that a different retention period is appropriate, submit a PS records retention schedule to the Arizona State Library, Archives and Public Records for approval.	Concur – will implement with modifications We will need to develop a comprehensive policy to speak to these issues; however, that won't be done without an ARS review and, perhaps, a legal review as to absolute requirements versus suggested requirements. Target Date: February 2017

Issue #8: Command Centers

Observation: We visited the Command Centers at the Administration Building, the Human Services Campus, and the Durango complex, and performed a ride-a-long with a mobile patrol officer to determine that the officers were completing their duties according to PS' policies and procedures. We observed that officers completed the Daily Activity Logs with all details of notable video monitoring, remote access assistance, alarms answered and resolved, disturbances, perimeter checks, exterior and interior building checks, officer movement, and radio contact in chronological order. However, we found that for two of the three locations, officer duties performed did not agree with the duties outlined in the policies and procedures. For example, timeframes did not match the procedures indicated, and building and equipment names and locations were outdated. In addition, none of the officers had a Field Interview Report Card to document the contact of a suspicious person or a package to be investigated, as stated in the policy.

We also noted that staffing did not match the levels identified in the procedures during our site visits. At the Administration Building, we noted there was an officer at the screening station, but a second lobby officer was not present. Similarly, no officer was available for foot patrol or mobile patrol.

Conclusion #8A: Controls are in place to ensure Command Centers are operating according to PS' policy; however, procedures need to be updated.	
Recommendation	PS Action Plan
8A-1 Update officer duties in PS' policies and procedures.	Concur – in progress Review and update patrol operations policy where needed/necessary. Target Date: 10/7/2016

Issue #9 Strategic Planning

Observation: We interviewed PS management and reviewed the department's only FY 2017 strategic goal, developed by the previous management team. The goal is to ensure that fewer than 10% of group demonstrations in County buildings on County property disrupt County business. Current management reports that the goal is not meaningful, useful, or measured appropriately.

We also reviewed the last PS organizational assessment study which was completed in 2005. The study reviewed staffing requirements, and determined the resources necessary to provide the desired level of service. We compared current staffing levels to those recommended and noted that current staffing is lower than what was recommended by the study; many changes have occurred with coverage areas and scope of duties in the last 11 years. For example, officers were eliminated at libraries, and at Women, Infants, and Children Food and Nutrition Service (WIC) Centers; officers were reduced at the County Administration Building and downtown Clerk of the Court; and, officers were increased at the Human Services Campus. Without clear strategic goals and an up-to-date organizational assessment, it is difficult for the department to determine if they are providing the desired level of core services in the most effective manner.

Conclusion #9A: PS' strategic goal and organizational assessment are outdated.	
Recommendations	PS Action Plan
9A-1 Develop strategic goals that are meaningful, useful, and measurable.	Concur – in progress New strategic goals based on a modified reporting system/structure have been set and we're awaiting direction from OMB as to how to proceed with changes. Target Date: 10/7/2016

Recommendations	PS Action Plan
<p>9A-2 Conduct an organizational assessment study to ensure that the scope of the department's duties and the resources required to perform those duties are aligned.</p>	<p>Concur – in progress Current planning is under-way and not for publication at this time. Target Date: TBD</p>

Issue #10: Information Technology (IT) – General Controls

Observation: To determine that IT general computing controls were sufficient, we reviewed controls over: (1) disaster recovery and business continuity, (2) system backups, (3) IT strategic planning, (4) physical security, (5) security awareness and training, (6) IT policy change management, and (7) anti-virus protection, intrusion detection, and remote access. PS relies on the Office of Enterprise Technology (OET) for IT network and infrastructure support. PS is responsible for the Velocity Security Management System (Velocity) application. Velocity is management software for access control and physical security, including door control, alarm monitoring, and photo badging.

Disaster Recovery and Business Continuity: We found PS has documented disaster recovery and business continuity policies for Velocity to ensure continued operations in the event of a disaster. We noted that both policies were last revised in 2006 (10 years ago). While the plans have not been tested, PS verifies that tapes are correctly backing up data.

System Backups: We reviewed documentation and observed the backup and off-site rotation processes for Velocity. We found that backups are performed and stored off-site. However, while PS has informal procedures, PS does not have written policies addressing backup procedures or off-site tape rotation for Velocity. PS relies on OET's backup and off-site rotation process for non-Velocity data and systems. We reviewed documentation and observed the off-site rotation process for PS non-Velocity backup data and found that appropriate backups were performed and rotated off-site.

IT Strategic Planning: We found that PS does not have a documented IT Strategic Plan, IT Risk Assessment, IT Budget, or IT Governance policy. IT planning is informal and IT needs/costs are considered on a case-by-case basis, dependent upon available resources. PS does not formally establish an IT budget based on strategic priorities.

Physical Security: PS' Velocity servers share a server room with OET. PS' servers are partitioned off from the OET servers via a locked metal cage. We observed that the server room was clean, and had adequate temperature controls, fire suppression, and uninterruptible power supply units. We reviewed access to the PS server cage and found it was appropriately restricted to four employees requiring access for job duties. However, we found that 242 badge holders have access to the OET server room. OET management confirmed this as excessive access.

Security Awareness and Training: We reviewed documentation for 10 of 64 (16%) current employees to determine if the employees had appropriately signed *Acceptable Use of County Resources and Electronic Mail* acknowledgement forms as required by County policy. We found 10 of 10 (100%) employees tested had signed the forms. While PS relies on County policies to address security awareness, PS does not conduct IT security awareness training for its employees to help ensure employees have a clear understanding of County IT security policies, procedures, and best practices. We observed that PS has established procedures to ensure PS' employees are informed regarding current and new IT policies.

Anti-Virus Protection, Intrusion Detection, and Remote Access: We reviewed 5 of 5 (100%) PS' servers and 20 PS' workstations and determined they appear to be appropriately protected by anti-virus software. We reviewed 2 of 2 (100%) employees with remote access to PS' systems and found that both users were current employees. PS relies on OET for monitoring and detecting unauthorized access to the network. Through inquiry, we determined that OET uses network security solutions (e.g., firewalls, network accounts, password parameters) and intrusion detection tools for monitoring unauthorized access to PS' systems.

Conclusion #10A: PS has controls in place for the following areas: disaster recovery and business continuity, system backups, physical security, policy changes, remote access, virus protection, and intrusion detection.	
Recommendation	PS Action Plan
None	N/A
Conclusion #10B: Disaster Recovery and Business Continuity Plans were developed, but are outdated.	
Recommendation	PS Action Plan
10B-1 Update the Disaster Recovery and Business Continuity Plans to ensure they are complete and apply to the current PS' environment. The plans should address equipment, software, and personnel issues.	Concur – in progress The entire system is being formally assessed/evaluated by Benson Systems which will address issues such as this. Additionally, OET will probably play a role in this as well. Target Date: February 2017

Conclusion #10C: Controls over system backups and off-site tape rotation need to be strengthened.	
Recommendation	PS Action Plan
10C-1 Document backup and off-site storage rotation policies and procedures to ensure PS' systems are consistently backed up and that off-site storage rotation is appropriate.	Concur – in progress The entire system is being formally assessed/evaluated by Benson Systems which will address issues such as this. Additionally, OET will play a role in this matter as well. Target Date: February 2017
Conclusion #10D: PS' controls over IT strategic planning could be improved.	
Recommendation	PS Action Plan
10D-1 Establish IT strategic planning policies and procedures to ensure PS' IT operations align with PS' business needs and meet overall business goals. Policies should address a documented IT Strategic Plan, IT Budget, IT Risk Assessment, and IT Governance.	Concur – in progress The entire system is being formally assessed/evaluated by Benson Systems which will address issues such as this. Additionally, OET will play a role in this matter as well. Target Date: February 2017
Conclusion #10E: PS' controls over server room access could be strengthened.	
Recommendation	PS Action Plan
10E-1 Evaluate server room badge access and work with OET to ensure access is appropriately limited.	Concur – in progress The entire system is being formally assessed/evaluated by Benson Systems which will address issues such as this. OET will play a role in this matter as well. Target Date: February 2017

Conclusion #10F: PS' controls over security awareness and training need improvement.	
Recommendations	PS Action Plan
10F-1 Establish written procedures to ensure that PS' employees receive end-user security awareness training to reduce the risk of improper data usage or exposure of sensitive data.	Concur – in progress SOP development with OET guidance and direction will probably occur via a contract with a technical writer. Target Date: May 2017
10F-2 Review, and update as necessary, the Acceptable Use of Protective Services Computing Resources policy.	Concur – in progress A review of all County policies as it relates to the utilization of computers should satisfy this requirement. A signature affirmation will solidify this requirement as well. Target Date: 9/2/2016

Issue #11: Information Technology – Velocity Application Controls

Observation: We tested 36 of 64 (56%) Velocity user accounts and found 12 user accounts were generic (not tied to a specific user). However, all 12 were appropriately restricted to read-only access. Eight user accounts belonged to terminated employees. All eight had been disabled on the network, which indirectly removed access to Velocity. Ten user accounts selected for additional testing were granted an appropriate level of access based on their job duties. Six user accounts had administrator access. These accounts have the highest level of privileges and access. Five had appropriate administrator access based on job responsibilities and one account was disabled. PS relies on County and OET policies for security management, user access, and account management. PS established an additional policy as an addendum to County policy to clarify expectations of PS employees. However, being issued in May 2003, we found the policy outdated.

We found that Velocity has built-in password controls to ensure appropriate password length, complexity, and expiration. Most password settings comply with OET's password policy; however, password length and expiration are not consistent with the policy. OET policy requires passwords be a minimum of eight characters, while Velocity is set for a minimum of six characters. OET policy requires that passwords expire every 60 days; Velocity passwords expire every 90 days.

We reviewed PS documentation and found patches are performed regularly, but are not documented. We also noted that access to Velocity is restricted; the application sends alerts to the administrators when a compromise occurs.

Conclusion #11A: PS has implemented key controls over user access and application updates.	
Recommendation	PS Action Plan
None	N/A
Conclusion #11B: Velocity passwords are not consistent with OET policy requirements.	
Recommendation	PS Action Plan
11B-1 Update Velocity password settings to ensure they comply with OET password policies.	Concur – in progress The system administrator along with OET guidance and direction will be responsible for making this happen based on policies in-place. Target Date: 10/28/2016
Conclusion #11C: Policies are outdated and procedures have not been documented.	
Recommendations	PS Action Plan
11C-1 Establish written policies for conducting regular reviews of Velocity user access accounts to ensure only current employees have active accounts. Remove Velocity user accounts belonging to terminated employees.	Concur – in progress The entire system is being formally assessed/evaluated by Benson Systems which will address issues such as this. OET will play a role in this matter as well. SOP development with OET guidance and direction will probably occur via a contract with a technical writer. Target Date: February 2017
11C-2 Update virus and patch management procedures to include retaining documentation regarding system patches/updates and testing performed.	Concur – in progress The entire system is being formally assessed/evaluated by Benson Systems which will address issues such as this. OET will play a role in this matter as well. SOP development with OET guidance and direction will probably occur via a contract with a technical writer. Target Date: February 2017

Issue #12: Officer Training

Observation: According to the PS' training officer, training was not regularly tracked or logged prior to 2015. Procedures have since been implemented.

We reviewed the training officer's records and determined that his training was current. We reviewed training files and the master training log for 10 out of 64 officers to ensure all required training had been completed. We found 10 (100%) officers had current Carrying a Concealed Weapon permits, firearm training certificates, and firearm range qualification certificates. However, two (20%) officers' first aid, CPR, and AED certifications had lapsed in February 2016 and December 2015, respectively. The training officer stated that all non-firearms related training was canceled due to staffing constraints. Because of this, he projects that additional officers will have their certifications lapse. Additionally, we noted that one (10%) officer's file was missing his new hire training certificates; however, the master training log noted that the training was completed. According to the training officer, the certificates were not retained because the officer was going to be leaving the position soon. We also noted that the training log and copies of employees' certifications are maintained on the training officer's desktop computer rather than on the shared drive.

Conclusion #12A: PS has implemented training requirements and tracking procedures to ensure staff is appropriately trained and certified.	
Recommendation	PS Action Plan
None	N/A
Conclusion #12B: All officers in our sample were current in firearms training.	
Recommendation	PS Action Plan
None	N/A
Conclusion #12C: Some officers did not have current first aid, CPR, and AED certifications and some training completion certificates were missing.	
Recommendations	PS Action Plan
12C-1 As soon as practical, resume non-firearms related training to ensure all officers are prepared to respond to safety events.	Concur – will implement with modifications Anticipated organizational changes will drive this process and those in-need of training will be provided the training. Target Date: February 2017

Recommendations	PS Action Plan
<p>12C-2 Retain copies of all training and certification documentation.</p>	<p>Concur – in progress</p> <p>We will make certain that all training certificates are accounted-for when training is completed.</p> <p>Target Date: Beginning immediately</p>
<p>12C-3 Retain logs in a shared electronic file to ensure documentation is backed up and can be accessed by management.</p>	<p>Concur – in progress</p> <p>Training officer will coordinate getting this accomplished with the assistance of the Administrative Captain (adding records to the “S” drive with limited access to supervisory staff).</p> <p>Target Date: 9/9/2016</p>

Issue #13: Contract Revenues

Observation: PS provides security services at the Human Services Campus (HSC) and bills the campus for those services. We reviewed nine FY 2016 monthly invoices to determine that the amount billed was accurate and payment was made on time. We found that the monthly invoice amount did not match the billing terms and conditions in the contract. In addition, PS was unable to provide any documentation to support the monthly discount that has been on invoices since 2007. The net effect was \$56,600 below the contracted amount in FY 2016 (as of April 2016). In addition, we reviewed payments received from HSC and noted that they are three months (February-April 2016) behind in payment for security services. PS does not have procedures in place to collect the delinquent payment.

The contract states that by April 1 each year, the County is to notify HSC of charges for services requested for the following fiscal year and to provide a calculation of those charges. No documentation was submitted for an increase in any year since the contract was executed. No charges were forwarded as of April 1, 2016 for the next fiscal year.

<p>Conclusion #13A: Controls over the Human Service Campus revenue contract could be improved. PS under-billed the Human Services Campus \$56,600 in FY 2016.</p>	
Recommendations	PS Action Plan
<p>13A-1 Invoice HSC in accordance with the contract billing terms or formally amend the contract.</p>	<p>Concur – in process</p> <p>This responsibility will be coordinated by FMD finance staff...moving forward.</p> <p>Target Date: 7/29/2016</p>

Recommendations	PS Action Plan
<p>13A-2 Develop procedures to collect delinquent amounts. Contact HSC management and determine when they will be current on the past-due amounts.</p>	<p>Concur – in progress This responsibility will be coordinated by FMD finance staff...moving forward. Target Date: 7/29/2016</p>
<p>13A-3 Prepare an annual cost analysis and notify HSC of changes to costs in accordance with the contract requirements.</p>	<p>Concur – in progress This responsibility will be coordinated by FMD finance staff in coordination with the Chief of Protective Services. Target Date: April 2017</p>

Issue #14: Cash Controls

Observation: We reviewed policies, procedures, and controls over checks, cash, and coins and found that procedures exist, but are not documented. The controls for the parking meter revenue were documented appropriately. A daily cash log was maintained and a receipt book was used. A safe was used to secure the checks and cash until a deposit was prepared.

<p>Conclusion #14A: PS has established procedures for handling checks and cash; controls appear to be sufficient, but were not documented.</p>	
Recommendation	PS Action Plan
<p>14A-1 Document all cash control policies and procedures.</p>	<p>Concur – in process This responsibility will be coordinated by FMD finance staff...moving forward. Protective Services staff will no longer be directly involved in cash control. Target Date: 7/29/2016</p>
<p>Conclusion #14B: Procedures for parking meter revenues are adequately documented.</p>	
Recommendation	PS Action Plan
<p>None</p>	<p>N/A</p>

Issue #15: Weapons and Equipment Inventory

Observation: According to the PS training officer, prior to 2015, inventory was not well tracked and no inventory logs existed. Significant progress has been made to inventory procedures. However, we noted some opportunities for improvement. Multiple logs track the same information creating an opportunity for discrepancies. Inventory records are not periodically reconciled so errors will carry over. We also noted that logs are kept on the training officer's desktop computer rather than on the shared drive. We reviewed the badge access report for the inventory room and noted all individuals with access are appropriate; however, they all have access to unsecured inventory in the storage room. We counted inventory and compared the counts to those on the physical inventory logs. We noted four of five (80%) inventory logs did not match physical counts.

Tasers: We counted Tasers and compared the count on the inventory log. No variances were noted. We found that cartridges were not inventoried. Used Tasers, cartridges and batteries were in a locked cabinet; however, new Tasers and unused cartridges were kept in an unlocked file cabinet.

Ammunition: We counted ammunition and compared the count to the inventory log. The duty ammunition log was over by 106 duty bullets, and the range ammunition log was under by 4,080 range bullets. The variance was mostly due to new inventory that was not logged. We also noted loose ammunition was in the safe that the PS' training officer said was there since he took over. PS reports that expired ammunition is removed from inventory and used for range ammunition and it is not tracked. Ammunition was properly secured in a safe and access was appropriate. We also noted that logs do not include who the ammunition was issued to or returned from, or the purpose of the transaction.

Pepper Spray: We counted pepper spray canisters and compared the count to the inventory log. We counted 42 canisters, while 51 were on the log; 9 canisters expired and were not removed from the inventory log. We also noted that pepper spray was kept on top of the safe in the storage room. Expired canisters, taken out of inventory for destruction, were not tracked.

Handcuffs: We counted handcuffs and compared the count to the inventory log. All handcuffs were accounted for. We noted a minor discrepancy, which was the result of incorrect serial numbers on the log. Handcuffs are kept in an unlocked file cabinet in the storage room.

We reviewed the issue and return documentation for three terminated PS officers. We found that returned ammunition was not documented on two return forms and equipment issued and returned was not fully documented on the three issue and return forms.

Conclusion #15A: PS has implemented inventory procedures to track ammunition and equipment.	
Recommendation	PS Action Plan
None	N/A
Conclusion #15B: Inventory procedures could be improved; some equipment was not inventoried and physical counts varied from log counts.	
Recommendations	PS Action Plan
15B-1 Establish and document inventory procedures. Procedures should include inventory, issue/return, tracking/logging, expiration/destruction, and periodic reconciliations.	Concur – in progress Written policy/procedure will be authored to speak to these issues. Target Date: 10/28/2016
15B-2 Remove or destroy any loose and/or expired ammunition and equipment.	Concur – in progress We will destroy any loose ammunition not able to be utilized in the field as duty ammo. Some damaged rounds will however be retained as “raining tools” as to what can go wrong. Target Date: 9/30/2016
15B-3 Secure all tactical equipment.	Concur – completed All equipment has been locked in available file cabinets within a secured storage area accessible by card access.
15B-4 Revise logs (duty and range ammo logs, ammo and equipment issue/return logs, and equipment logs) to include who ammo/equipment was issued to/returned from, the purpose of the transaction, quantities, and issue/return dates.	Concur – completed All inventory logs have been modified to capture the requested information.

Recommendations	PS Action Plan
<p>15B-5 Simplify logging procedures and ensure that logs are kept in a shared electronic file.</p>	<p>Concur – in progress</p> <p>Logging procedures will be “simplified” as determined to be appropriate by the Training Officer. All logs and logging procedures will be kept on the “S” drive with limited access by supervisory staff members only.</p> <p>Target Date: 9/2/2016</p>

Issue #16: Security Equipment Outages and Work Orders

Observation: No formal procedures are in place to review the extent and duration of security equipment outages. In addition, no periodic report is used to track open work orders. To verify the status and timeliness of equipment repairs, we reviewed a sample of 19 “in progress” PS’ repair work orders for cameras, card readers, panic alarms, control panels, and Digital Video Recorders (DVRs). At the time of our test, 7 of the 19 repair orders were resolved; however, 4 of those were still listed as “in progress.” Two requests have remained unresolved for more than 230 days, and another 2 have remained unresolved for more than 100 days. The remaining 8 have remained unresolved anywhere from 22-70 days.

We also noted that PS does not maintain an asset list of cameras in use. They do not track the camera models, serial numbers, original cost, date placed in service, and original and current locations of the cameras.

<p>Conclusion #16A: Tracking and monitoring of security equipment outages and work orders needs improvement.</p>	
Recommendations	PS Action Plan
<p>16A-1 Develop and implement procedures to track outages and repair work orders, and follow-up if repairs are not completed in a reasonable time.</p>	<p>Concur – in progress</p> <p>The IT Manager and/or his designee will be responsible for developing these procedures.</p> <p>Target Date: 10/28/2016</p>

Recommendations	PS Action Plan
<p>16A-2 Prepare an asset list of the security equipment including cameras, DVRs, panic buttons, etc. Include the equipment location for preventive maintenance procedures, potential warranty coverage, retirement, and replacement of equipment.</p>	<p>Concur – in progress</p> <p>This is a monumental task that will take 6-12 months to complete. (As it pertains to cameras and maintenance- this has been a combined responsibility with FMD and that working relationship will be expanded now that PS is a division of FMD)</p> <p>Target Date: July 2017</p>