OCALA

Agenda Item # 12
Report # 3

September 30, 2016

To: Greg Graham, Chief, Ocala Police Department
Rodney Smith, Deputy Chief, Ocala Police Department

From: Emory Roberts Jr., Internal City Auditor

Re: Ocala Police Department IT General Controls - Project 2016-12

Internal Audit has completed a review of Ocala Police Department (OPD) Information Technology (IT) General Controls. The objectives of this audit were to determine that internal controls exist and are effective in the areas of access to programs and data, program changes/system development, and computer operations.

To accomplish our objectives, we interviewed OPD IT and Support Services management personnel, reviewed OPD Department Directives and other documentation, performed selective testing of various areas, and assessed internal controls over operational processes. Additionally, we visited the OPD IT off-site back-up locations to view the backup hardware and the associated physical security of each location.

The general controls included in the scope of our review were user provisioning/de-provisioning, password requirements, IT security management, change management, and physical security. We excluded the area of data back-up and recovery from our review due to the on-going implementation of new related back-up virtualization hardware and software.

Based upon the work performed, we found that the reviewed OPD IT general internal controls exist and are operating effectively in the areas of access to programs and data, program changes/system development, computer operations, and physical security.

We found one opportunity to strengthen password requirements by enabling password complexity in the Active Directory Default Domain Policy to comply with current OPD Department Directive 7.15, PASSWORDS section.

We have provided a high level summary of the audit results below:

Internal Control Strengths:

- The design for logical security which helps provide for data integrity was adequate to address password administration and identity management. Management complies with Criminal Justice Information Systems (CJIS) requirements for logical security.

- Physical security for IT facilities was adequate and working effectively to safeguard IT resources. We reviewed access controls to the primary building and to sensitive restricted areas for both the OPD and the off-site locations.

- The use of the new Track-It! Help Desk software provides for proper management and tracking of user issues and requests, as well as asset management and change management.

- The use of an OPD Sharepoint site for user provisioning and de-provisioning for new employees, transfers or terminations provides real time notification of IT support personnel and a tracking and documentation process for reference.

- The use of advanced software solutions for network monitoring, detection of suspicious activities, and web filtering and security ensures the latest criteria and specifications are utilized for all areas.

We appreciate the assistance of all OPD personnel involved in the review, especially Joshua Sasso and Mindy Stewart. Please let us know if you have any questions.

Cc: R. Kent Guinn, Mayor

BACKGROUND

The background information provides relevant and pertinent information to assist the reader with gaining a reasonable understanding of the activity under review.

OPD uses various technologies to effectively and efficiently carry out policing operations. Without the support of information technology, it would be very difficult for OPD to successfully carry out its mission. Therefore, since there is a substantial dependence on information technology; general controls should be designed, implemented, and monitored, to provide reasonable assurance of continuous, reliable, and adequate IT support for Police operations.

Governance is critical component of any control environment and OPD's written governance is the Federal Bureau of Investigation's (FBI) Criminal Justice Information Systems (CJIS) Security Policy which as stated by management has been formally adopted beyond the CJIS networked applications.

OPD has an IT staff to manage the IT environment that includes hardware (equipment), software (programs and applications), data (electronic records), and facilities. The IT staff and data center are located at OPD Police Headquarters.

OPD uses Active Directory, a directory service created by Microsoft for Windows domain networks, which provides the capability to centrally manage network users and system information while enforcing OPD's security standards and standardizing network configuration.

This audit looked at IT general controls, which are those internal controls that relate to the overall IT environment, rather than to specific applications or systems.

Opportunities for Improvement

Our audit disclosed certain policies, procedures and practices that could be improved. Our audit was neither designed nor intended to be a detailed study of every relevant system, procedure or transaction. Accordingly, the Opportunities for Improvement presented in this report may not be all-inclusive of areas where improvement may be needed.

Password Management We found that password complexity was disabled in the Active Directory Default Domain Policy. Current OPD Department Directive 7.15, in the PASSWORDS section (page 5), states in part that *"The end-user password, generated automatically upon first logon (and reset, but not known, by MIS personnel if needed), will be of at least 8 characters, include at least one special character (number, punctuation), changed every 90 days, and not one of the last 10 passwords used"*.

Although OPD currently uses a strong eight character password requirement, the use of complexity as stated in the Directive will also require the use of an uppercase character, and a number or special (non-alphabetic) character that will further strengthen password security.

We recommend that IT Management enable password complexity per current OPD Directive 7.15 and require the additional use of an uppercase character, and a number or special (non-alphabetic) character that will further strengthen password security. Once changed, the complexity requirements are enforced when passwords are changed or created.

Management Response - We agree with the findings and have a target date of 12-31-16 to have everyone corrected. We are updating the AD policy and as passwords expire the change will be effective for them.