Audit of Department of Public Works License Plate Recognition System

MARTIN MATSON
City Comptroller

ADAM FIGON
Audit Manager

City of Milwaukee, Wisconsin

November 2017

Table of Contents

Martin Matson
Comptroller

Aycha Sirvanci, CPA, CIA
Deputy Comptroller

Toni Biscobing
Special Deputy Comptroller

Rocklan Wruck, CPA
Special Deputy Comptroller

Office of the Comptroller

November 15, 2017

Honorable Tom Barrett, Mayor
The Members of the Common Council
City of Milwaukee
Milwaukee, WI 53202

Dear Mayor and Council Members:

The attached report summarizes the results of the audit of the Department of Public Works License Plate Recognition (LPR) system. The scope of the audit included selected operational, data management and security controls over automated parking enforcement and the LPR system. The time period under review was September 2015 through March 2017. The audit objectives were to:

1. Determine whether the LPR system's access policies and procedures to manage and store data generated provide adequate data security, permit only the authorized use of data and are compliant with best practice criteria.
2. Assess the adequacy and effectiveness of internal controls over the LPR system and the automated parking enforcement process.

The audit concluded that the automated parking enforcement data management and security controls in place over the LPR system are adequately designed and are operating effectively. However, for certain controls identified within this report, several enhancements should be made in the control design to further improve the process. This report identifies three recommendations to address these issues.

It is noted that for certain controls identified within this report department management proactively initiated mitigating actions necessary to address some of the issues encountered during the performance of the audit.

Audit findings are discussed in the Audit Conclusions and Recommendations section of this report, and are followed by management's response.

Appreciation is expressed for the cooperation extended to the auditors by the personnel of the Department of Public Works – Parking Enforcement.

Sincerely,

Adam Figon

Adam Figon, MBA, CRMA
Audit Manager

AF/rk

I. Audit Scope and Objectives

The audit examined the Department of Public Works (DPW), Parking Fund administration of the License Plate Recognition (LPR) application software. The application was first installed in 2013 in approximately twenty-eight parking enforcement vehicles to initiate electronic tracking of issued night parking permits and permissions by DPW, Parking Enforcement. The scope of the audit included selected operational, data management and security controls over automated parking enforcement and the LPR system. The time period under review was September 2015 through March 2017. The audit encompassed the collection, access, authorized use and the storage and dissemination of data accumulated through the LPR system.

The objectives of the audit were to:

1. Determine whether the LPR system's access policies and procedures to manage and store data generated provide adequate data security, permit only the authorized use of data and are compliant with best practice criteria.

2. Assess the adequacy and effectiveness of internal controls over the LPR system and the automated parking enforcement process.

The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. Internal Audit believes that the evidence obtained provides a reasonable basis for the audit's findings and conclusions based on the audit objectives.

Methodology

The audit methodology included developing an understanding of the risks, processes and controls over the LPR system and parking operations. To assess the risk of the LPR system, Internal Audit performed audit procedures to identify and test management controls over safeguarding personally identifiable information (PII).

PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or combined with other personal or identifying information that is linked or linkable to a specific individual. PII is not anchored to any single category of information or technology. It requires a case-by-case assessment of the specific risk that an individual can be identified.[1]

The audit procedure developed to evaluate the processes and controls to meet the audit objectives included initial research, process walk-throughs, inspection of relevant control documentation and the testing of controls as follows:

- Interviewed management and staff within the DPW, Parking Enforcement.
- Reviewed internal policies, procedures, guidelines and system information.
- Assessed compliance with the City Password Policy.
- Reviewed LPR information technology flowcharts and process maps.
- Determined LPR data set risks – non-PII (low risk).
- Assessed the adequacy of user access change control management and monitoring.
- Verified authorization and approval of application change control management.
- Assessed the application's risks, internal controls and third party vendor performance.

Notables

Audit procedures confirmed the adequacy and effectiveness of internal controls over the LPR system and the automated parking enforcement process:

- Testing indicated that management has implemented controls that allow only authorized user access to the LPR system and data.
- Internal Audit confirmed through discussions with management and the review of the LPR system and supporting documentation that the LPR system does not collect and store PII.
- The information/data collected by the LPR system and utilized by Parking Enforcement management is stored on servers residing, and secured, in the Information Technology Management Division (ITMD) Data Center with physical and logical access limited to authorized personnel and the system administrators.

[1] U.S. General Services Administration (GSA) Privacy Program – Rules and Policies – Protecting PII Privacy Act

Thus, initial risk analysis and testing determined that the internal controls over this low-risk data set are adequate to mitigate applicable identified risks.

II. Organization and Fiscal Impact

The Department of Public Works consists of four main divisions which include Administrative Services, Infrastructure, Operations, Parking Services and Water Works. Collectively, these divisions have a significant impact on daily life in the City of Milwaukee. The DPW contributes to the quality of life and economic development of Milwaukee via, at a minimum, the following responsibilities: the planning and construction of public improvements throughout the city; the design, maintenance and operation of streets, sidewalks, alleys, bridges, water mains, traffic signals and street lighting; the timely completion of sewer, water and paving projects; snow and ice control; and the oversight and operation of various parking functions.[2]

The Parking Fund

The mission of the Parking Fund, an enterprise fund administered by the DPW, is to leverage city parking assets and programs to improve the City's fiscal capacity to support city goals and diversify the City's financial basis. Its functions include managing city owned parking structures and lots, vehicle towing, storage and disposal, parking enforcement, information desk operations and citation processing.[3] The annual parking citation revenue in 2015 was approximately $18.6 million dollars and over 700,000 parking citations were issued.[4] Additionally, the Parking Fund operates and maintains approximately 6,800 on-street parking spaces.

Parking Enforcement: LPR-Patroller and Night Operations

The AutoVu LPR system software was developed and is supported by the third party vendor Genetec Inc. The LPR–Patroller system has been installed on the computers in Parking Enforcement's patrol vehicles to expedite parking enforcement operations.

---

[2] Department of Public Works – Official Website of the City of Milwaukee – http://city.milwaukee.gov/mpw#.WdvJMdKWy70

[3] Department of Administration, Budget and Management Division 2016 Plan and Budget Summary, p. 191

[4] City of Milwaukee 2017 Plan and Budget Summary, p. 209

Presently, there are a total of forty Parking Enforcement vehicles equipped with the LPR-Patroller system. LPR-Patroller units are used to identify vehicles that do not possess valid night parking permits or night parking permissions. Twenty-four vehicles are equipped with the LPR-Patroller-University Kit, which includes front cameras and a Global Positioning System (GPS) antenna; and sixteen are equipped with the LPR-Patroller-Overtime Kit which includes GPS, front cameras and rear tire cameras for enhanced parking enforcement.

At 2:00 a.m., 4:00 a.m. and 6:00 a.m. the LPR-Patroller-GPS is utilized to locate each Parking Enforcement vehicle in the field to ensure the safety of Parking Ambassadors (parking enforcement field personnel) and to confirm they are in their designated patrolling areas. The GPS is only used for tracking the location of Parking Enforcement vehicles, monitoring the enforcement individual and the overall performance of parking enforcement. The location of citizen vehicle license plates is not determined and captured by the LPR-Patroller-GPS system. Parking Enforcement Ambassadors do not possess the systematic capability to alter the license plate data captured via LPR-Patroller system during enforcement operations.

System Administration, Access, Change Control and Data Management

Security Desk, AutoVu's back-office or administrative software (also known as Security Center) is a non-web-based program that enables DPW management to govern parking regulations, permits and permissions internally. The software requires installation on each authorized user's desktop computer and is accessed via user ID and password. Access to the Security Desk application is restricted to two managers and three shift supervisors who are designated as the system administrators. The system administrators utilize Security Desk to perform updates to user access, grant permissions and initial authorizations, and remove or disable user access upon employee termination or transfer. Access changes can be systematically traced to the administrator specifically responsible for the performance of the access update.

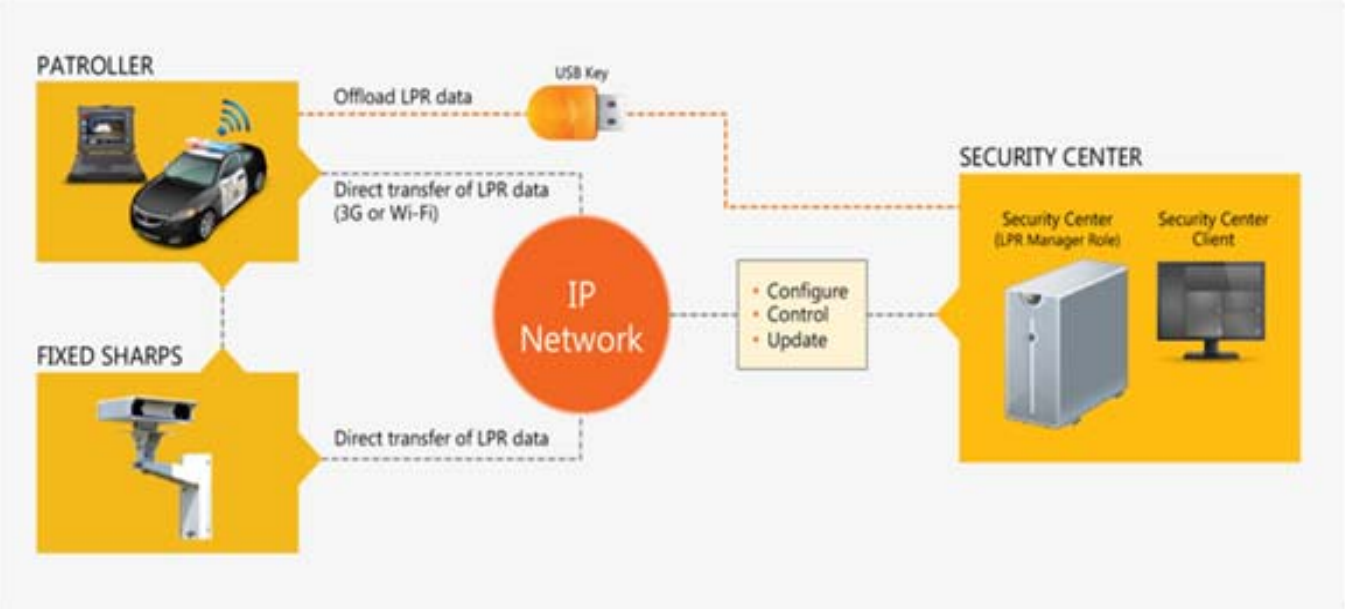
The ITMD and vendor do not have access to the Security Desk software. As a part of normal operations, the ITMD and vendor personnel have no need to access the software. Only the vendor can access the software, if a need were to arise (potential troubleshooting), provided permission is granted by ITMD. To date, it has not been necessary to give the vendor access to the software.

Parking administrator's only control the established functionality and parameters provided by the LPR system; thus, they can turn on or off certain features programmed into the system. Parking administrators and ITMD cannot alter the software itself.

During each Parking Ambassador's nightly shift, the data collected by the LPR-Patroller is continuously transmitted to the ITMD Data Center server without any need for operator intervention. This continuous transmission does not include the license plate picture data. At the end of the shift, the system asks the operator if they wish to offload the picture data. The standard procedure is for the operator to click 'start'. If the standard procedure is not followed, the next time a Parking Ambassador powers the system on they have the option to offload the previous Parking Ambassador's data, prior to the start of their shift. The system automatically offloads the data if the system has been in an idle mode for an extended period of time; pictures will then be transmitted to the ITMD server.

A high-level overview of the LPR-Patroller system operation is presented below in Figure 1 and summarizes the recording, transfer, security and reporting of parking data.[5]

Figure 1
Overview of the LPR-Patroller System Operation



[5] https://www.genetec.com

The Security Desk software can directly access the LPR-Patroller data from the ITMD server. The servers hosting the data tables are maintained by the ITMD and are secured in the ITMD Data Center. The LPR-Patroller software also continuously captures the date, time and GPS longitude and latitude of the City's enforcement vehicle and also transmits this information nonstop back to the ITMD server.

Additionally, Security Desk offers extensive reporting and operational data-mining capabilities such as route playback, occupancy counts, parking citation statistics and individual staff performance statistics. Data collected from the LPR system during enforcement operations is captured, stored and retained within the parameters identified in the City record retention policy.

Audit procedures confirmed that the LPR system does not collect PII.

Law Enforcement Activities and Data

Parking Ambassadors only enforce City parking regulations and are not responsible or involved with any other type of law enforcement activity, such as the identification, reporting, or recovery of stolen vehicles. Additionally, the DPW parking database does not contain any information regarding stolen vehicles as it is physically separate from, and is independent of, the Milwaukee Police Department (MPD) database. MPD is solely responsible for enforcing laws regarding the identification and recovery of stolen vehicles.

III. Audit Conclusions and Recommendations

The internal controls developed and implemented by DPW management over parking enforcement operations have been designed to provide management with assurance that processes and controls are performed consistently and are in compliance with policy, procedure, parking regulations, and best practice. The audit concluded that the automated parking enforcement data management and security controls in place over the LPR system are adequately designed and are operating effectively. However, for certain controls, identified within this report, several enhancements should be made in the control design to further improve the process. This audit report identifies three recommendations to address these issues:

1. Develop and document policies and procedures over the License Plate Recognition system key processes and controls.
2. Develop and implement controls over vehicle keys, cell phones and mobile devices.
3. Configure the License Plate Recognition system for compliance with the City Password Policy.

Additional details regarding the recommendations for improvement are provided in the remaining sections of this report.

A. Policies and Procedures

In accordance with best practice, including the *2013 COSO Framework–Principle 12*: Management should implement control activities through policies that establish what is expected and in procedures that put policies into action.

Written policies and procedures should be: developed and enforced for all operations; made accessible and communicated to all personnel; and, reviewed and updated as needed. Well-defined policies, procedures and processes outline current requirements, operations, interdependencies, risks and controls, and they can help identify improvement opportunities. Per best practice:

- Policies contain high-level principles or requirements that a certain department or functional area of the organization must follow, as formally agreed upon by management.
- Procedures are affiliated with particular policies and define lower-level processes, such as daily, weekly or quarterly functions and job activities.
- Processes are contained within procedures, defining in detail how regular business functions are performed whether on a repeating or as-needed basis, and show interrelationships and dependencies with other processes, organizational areas or technologies.

Documented policies and procedures provide insight into standardized functions, key risks and controls that need to be monitored, and simplify risk assessments, risk mitigation and audit efforts.

The DPW, Parking Enforcement does not have comprehensive, formal, documented policies and procedures governing the internal operations that utilize the LPR-Patroller system. However, it is noted that during the performance of the audit applicable policies were in a draft format, and extensive LPR system user manuals and guides were available and have been included in day-to-day Parking Enforcement operations and training.

Recommendation 1: Develop and document policies and procedures over the License Plate Recognition system key processes and controls.

Management should develop and document formal comprehensive policies and procedures to govern the following operations that utilize the LPR system:

- The Parking Administrator procedure over the use of the Security Desk software.
- The Parking Ambassador operations including the use of the LPR system.
- The documentation of LPR system training and completion of training.
- The practice of offloading LPR data from the enforcement vehicle LPR-Patroller units to the Security Desk at the end of each shift to ensure the complete transfer of enforcement data.

Policies and procedures should be stored in an accessible location and updated as needed.

B. Inventory Management and Safeguarding

In accordance with best practice and standard convention proper inventory accountability requires that:

- Detailed records of produced, acquired or distributed inventory be maintained.
- Inventory has been safeguarded to provide reasonable assurance regarding the prevention or timely detection of unauthorized acquisition, use or disposition of the City's assets.

Physical controls and accountability reduce the risk of potentially undetected theft and loss, unexpected shortages of critical items, and unnecessary purchases of items already on hand. These controls improve visibility and accountability over the inventory which help ensure continuation of operations and productivity.

Key card system controls limit accessibility to the Parking Enforcement Operations area; however, vehicle keys, mobile devices and cell phones used by the Parking Ambassadors are stored in unlocked cabinets.

Recommendation 2 Develop and implement controls over vehicle keys, cell phones and mobile devices.

To strengthen physical security controls over Parking Enforcement assets and inventory, Management should:

1. Develop and implement inventory access controls to ensure that access to City vehicles, assets or equipment is limited to authorized employees.
2. Repair and use the lock on the parking enforcement vehicle key storage cabinet.
3. Install and use locks on the storage cabinets containing hand held citation issuance devices and cell phones.

C. Access Control Configuration

All City departments that maintain information systems must ensure that access to these applications is adequately restricted. Passwords are an important aspect of computer system security. [6] Employees with administrative access to City applications are responsible for taking the appropriate steps to implement and secure end-user passwords configured to enforce the minimum security standards set by the City's Password Policy.

The LPR-Patroller system password configuration does not comply with the City's Password Policy. LPR-Patroller is not configured for the use of a password whereas the City Password Policy requires an eight-character password. The LPR system password configurations were established according to the vendor's specifications when the application was originally implemented in 2013.

The use of the LPR-Patroller system is limited to the parking enforcement vehicles and is only used to identify vehicles that are illegally parked.

Recommendation 3: Configure the License Plate Recognition–Patroller system for compliance with the City Password Policy.

To strengthen user access control over the LPR-Patroller system, Management should configure the system password parameters to be compliant with City password requirements as follows:

- All passwords set to be at least eight characters long.
- All passwords must be alphanumeric (contain at least one (1) letter and (1) number).
- All passwords are set to change at least every 90 days.
- All passwords are locked out after five unsuccessful access attempts.

---

[6] City of Milwaukee Password Policy dated June 11, 2011

City of Milwaukee

Department of Public Works
Operations Division

Ghassan Korban P.E.
Commissioner of Public Works

Laura Daniels
Director of Operations

November 9, 2017

Adam Figon
Audit Manager
200 E. Wells St. Rm. 404
Milwaukee, WI 53202

RE: Department of Public Works (DPW) Audit of License Plate Recognition System

Dear Mr. Figon:

We are writing in response to the "Summary of Findings and Recommendations dated 7-11-17, regarding DPW Operations Parking Service's license plate recognition (LPR) system.

In reply to the audit, we offer the following responses:

Recommendation 1: Develop and implement policies and procedures.

At the time of the audit, Parking Services had a policy in draft form pertaining to Automated License Plate Readers (ALPR). That policy is now formally in place and covers the conditions of the release of data. An addition was added to the draft policy which now requires users to off load data at the end of shift unless the data is specifically used by following shifts for overtime enforcement.

Parking Services also maintains a user manual for the Security Center back office software. That user manual is a guide to the functions of the system. Pertinent controls regarding security and use of the data from Security Center are addressed in the ALPR Policy and the City Wide computer policy.

Parking Services also has a user training manual for the user side of the ALPR system which is called Patroller. The manual describes the Parking Services Ambassador processes and use of the LPR system. This training document will be transcribed into a standardized DPW Operations SOP format.

All users are formally trained by supplying the user with the user manual and then trained through a hand on program conducted by an experienced user. We have implemented a training document. Once the trainee has demonstrated the knowledge of all the objectives of the Patroller software, the trainee and trainer sign off on a completed training document. That document will be kept in the employee's training file.

The response to this recommendation has been completed.

Recommendation 2: Inventory Management and Safeguarding

Parking Services best management practices for inventory control include that the entire facility is only accessible by Parking Services employee's through card access system and cabinets for vehicle keys and equipment are located in Supervisor controlled areas.

Due to the nature of around the clock operation with overlapping shifts, access to keys and equipment is essential to support efficient changeover of staff while maintaining some presence on the street. For that reason, we have located the vehicle key cabinet in the supervisor work area for regular oversight and observation of access. The phone and handheld device cabinet is located within view of the supervisor offices. However, to enhance controls we have installed a security camera system at these locations to record employee activity in the event that a need arises.

The response to this recommendation has been completed.

Recommendation 3: LPR System Password Use

Patroller users, the front end interface for the LPR system, will be assigned passwords which will meet as many of the following City of Milwaukee Password Policies in place for information systems and networks as possible based on the limits of the software, if all points are not possible we will ask the software developers to work towards providing us passwords to these standards:

- Passwords must be at least eight characters long
- Contain at least one letter and one number
- Must require change every 90 days
- Allow only 5 unsuccessful consecutive attempts
- The initial password assigned by the administrator should be valid only on the user's first session

The Patroller user data access is limited to data captured on individual Patrollers units. The units are used to identify vehicles that are illegally parked. The computers, which are part of the APLR hardware, are used to operate and drive the APLPR software; they are not network linked computers.

Administration users cannot delete License Plate Recognition System records.

Our system integrator is working on a password secured login process that will encompass as many of the standards as possible. The response to this request is expected to be completed during the next on site service visit from our system integrator which will be in spring of 2018. We expect to be compliant to this recommendation by 06-01-18.

If you require clarification on any of the responses above, please contact Laura Daniels, DPW Operations Manager at Laura.Daniels@milwaukee.gov or 286-3302 or Richard Dollhopf, Parking Enforcement Manager at Richard.Dollhopf@milwaukee.gov or 286-8365. Thank You.

Very truly yours,

Ghassan Korban P.E.
Commissioner of Public Works

GK:LD:kjj

cc: L. Daniels
T. Woznick