APRIL 2018

CITY OF CHICAGO
OFFICE OF INSPECTOR GENERAL

OFFICE OF EMERGENCY MANAGEMENT AND COMMUNICATIONS PUBLIC SAFETY CAMERAS FOLLOW-UP INQUIRY

REPORT OF THE OFFICE OF INSPECTOR GENERAL

JOSEPH M. FERGUSON
INSPECTOR GENERAL

CITY OF CHICAGO
OFFICE OF INSPECTOR GENERAL
740 NORTH SEDGWICK STREET, SUITE 200
CHICAGO, ILLINOIS 60654
TELEPHONE: (773) 478-7799
FAX: (773) 478-3949

APRIL 30, 2018

TO THE MAYOR, MEMBERS OF THE CITY COUNCIL, THE CITY CLERK, THE CITY TREASURER, AND THE RESIDENTS OF THE CITY OF CHICAGO:

The City of Chicago Office of Inspector General (OIG) has completed a follow-up to its December 2016 audit of the Office of Emergency Management and Communications' (OEMC) management of public safety cameras. Based on the Department's responses, OIG concludes that OEMC has implemented two corrective actions related to the audit findings and has begun to implement three others.

The 2016 audit assessed the effectiveness of OEMC's management of public safety cameras by testing whether the cameras worked properly, whether the cameras received necessary repairs in a timely manner, whether the cameras retained footage for the required number of days, and whether access to the cameras was limited to appropriately authorized personnel.

OIG found that, in managing public safety cameras, OEMC did not comply with, and did not require other departments to comply with, citywide policies regulating access to information systems. As a result, OEMC could not, in most instances, determine which individuals accessed the camera system or how those individuals used the cameras. We also found that OEMC did not establish and enforce operational objectives for public safety cameras, and therefore could not determine whether operational levels were optimal. OIG further found that although OEMC's project manager—the Public Building Commission (PBC)—received and reviewed deliverables as required, minor deficiencies in PBC's vendor monitoring prevented it from fully executing its responsibilities as a project manager.

Based upon the results of the audit, OIG recommended that OEMC implement policies and practices regulating access to public safety cameras, develop and enforce reasonable standards for system performance, and review and identify opportunities to improve PBC's oversight of its vendor for camera repair and maintenance, Motorola. In its response to the audit, OEMC described a number of corrective actions it would take.

In December 2017, OIG inquired about corrective actions taken by OEMC in response to the audit. Based on OEMC's follow-up response, OIG concludes that OEMC has implemented two corrective actions and has three corrective actions pending implementation. Specifically, OEMC assumed direct management of the Motorola contract, implementing corrective actions related to the establishment of performance measures and increased contract oversight. OEMC is in the

process of implementing corrective actions to address compliance with the City's Information Security and Technology Policies. Once fully implemented, OIG believes the corrective actions reported by OEMC may reasonably be expected to resolve the core findings noted in the audit. Below, we summarize the audit findings and recommendations, as well as the Department's response to our follow-up inquiry

We thank the staff and leadership of OEMC for their cooperation during the audit and responsiveness to our follow-up inquiries

Respectfully,

Joseph M. Ferguson
Inspector General
City of Chicago

FOLLOW-UP RESULTS

In December 2017, OIG followed up on a December 2016 audit of the Office of Emergency Management and Communications' (OEMC) management of public safety cameras.[1] OEMC responded by describing the corrective actions it has taken since receiving the audit and providing supporting documentation. Below, we summarize the three findings, the associated recommendations, and the status of the Office's corrective actions. Our follow-up inquiry did not observe or test implementation of the new procedures; thus, we make no determination as to their effectiveness, which would require a new audit with full testing.

OIG uses four categories to describe the Status of Corrective Action:

- Implemented - The department has implemented actions that may reasonably be expected to resolve the core findings/concerns noted in the audit.
- Partially Implemented - The department has implemented actions in response to the audit, but the actions do not fully address the findings/concerns raised in the audit.
- Pending Implementation - The department has initiated action plans that, if fully implemented, may reasonably be expected to resolve the core findings of the audit. However, the department has not completed implementation.
- Not Implemented - The department has not initiated or implemented any actions responsive to OIG's findings.

FINDING 1:

OEMC DID NOT COMPLY WITH, AND COULD NOT ENSURE THAT OTHER DEPARTMENTS COMPLIED WITH, CITYWIDE POLICIES RELATING TO INFORMATION ACCESS CONTROLS, AND, THUS, DID NOT HAVE REASONABLE ASSURANCE THAT ONLY APPROVED PERSONNEL HAD ACCESSED ITS PUBLIC SAFETY CAMERA SYSTEM AND USED IT APPROPRIATELY.

OIG Recommendation 1:

OEMC should require each user to log into the Security Center application using a unique username and password, and automatically prompt users to change their passwords every 90 days. In addition, OEMC should assess the feasibility of having the vendor add a function to the application that would allow the Office to generate reports of all users, their login times, and their permission levels. Until these solutions can be implemented,

[1] The 2016 audit report is available on the OIG website: http://chicagoinspectorgeneral.org/wp-content/uploads/2016/12/Audit-of-OEMC-Public-Safety-Cameras.pdf.

OEMC should as an interim measure, minimally, require all users of group logins to create physical records of their identities, possibly by using a sign-in sheet associated with every computer terminal, prior to accessing the public safety camera network.

Status of Corrective Action: **Pending Implementation**

OEMC has implemented two active directory connections for the public safety camera network—one for the Chicago Police Department (CPD) and one for all other users. Thus, all network users now have unique login credentials. The active directory connection to the CPD domain requires members to access the camera network with their unique CPD username and password. CPD's current password rules do not require password changes every 90 days. However, CPD expects to implement this requirement by the end of April 2018 as part of its migration to a new e-mail system. CPD members have access to all cameras within the public safety camera network, with two exceptions. First, CPD members can only view indoor cameras for the district office to which they are assigned, and, second, access to lock-up cell cameras is restricted by gender. Only female members can view female lock-up cell areas and only male members can view male lock-up cell areas. The system generates automated user status reports daily to confirm that each CPD user's level of access continues to match their designated district office and gender. Motorola reviews the reports and brings any errors to OEMC's attention for troubleshooting. All non-CPD users access the network by connecting to the OEMC domain and entering a unique username and password. Users are required to change their passwords every 90 days; a password management server automatically prompts users to reset their passwords seven days before expiration. Motorola is responsible for managing permission levels and troubleshooting access errors.

OEMC now has multiple camera-access monitoring capabilities. OEMC is able to track each user's activity in the system, search each individual camera or group of cameras, and report on all activity for the previous 30-day period. Camera activity reports include information such as the identities of users who accessed a particular camera, whether they utilized pan-tilt-zoom functions, and the specific time frame within which they livestreamed a camera feed or viewed prerecorded video. OEMC system administrators also have the capability to run real-time reports that display a variety of data, including the location and configuration of each camera, and the access level and last login date of each user.

OIG Recommendation 2:

To address the issue of ensuring that outside agencies comply

with the City's Information Security and Technology Policies (ISTP), OEMC should require all outside agencies to abide by a user agreement as a condition of Security Center access. The agreement should reflect the access control policies described in the ISTP. If OEMC determines that an agency is not in compliance, OEMC should consider revoking the agency's access.

Status of Corrective Action: **Pending Implementation**

OEMC finalized a Memorandum of Understanding (MOU) in 2017 for execution with external agencies that are authorized to access the public safety camera network. In January 2018, OEMC incorporated the City's ISTP into its MOU template, and it will amend its current MOU with the Illinois State Police and the Chicago Cubs to require compliance with the City's ISTP. OEMC will also revise its existing Intergovernmental Agreement with the Chicago Transit Authority, and sign new MOUs that incorporate the ISTP with Navy Pier, the Federal Bureau of Investigation, the University of Illinois at Chicago, and McCormick Place.

In addition, as of April 2017, external users of the public safety camera system must complete an Access Request Form providing personal identifying information, a business justification for access to the system, and a defined time period (in years, months, days, and hours) during which they require access. Every external user accessing the system must act in accordance with privacy policies, and maintain updated security and anti-virus software on the computer used to access the system. Each outside user also agrees to utilize the system only for work-related activities and to not share their log-in credentials. Finally, the OEMC Managing Deputy Director of Public Safety Information and Technology and the First Deputy must both review and approve each Access Request Form.

OIG Recommendation 3:

OEMC should create and document policies outlining a process for determining who should have camera access, as well as what level of access they should have. These policies should require OEMC to document the business reason for granting privileged access, and to set out the Office's rationale for permitting or denying access to each particular party.

Status of Corrective Action: **Pending Implementation**

OEMC is in the process of developing a written policy aligning with its mission statement that formalizes the criteria used to grant, deny, and rescind access to the camera system.

FINDING 2: OEMC DID NOT ESTABLISH OPERATIONAL OBJECTIVES FOR THE PUBLIC SAFETY CAMERAS, AND THEREFORE COULD NOT DETERMINE IF CURRENT OPERATIONAL LEVELS AND THE VENDOR'S EFFORTS TO MAINTAIN THOSE LEVELS ARE OPTIMAL.

OIG Recommendation 4:

OEMC should develop and document performance measures that capture optimal system operational levels such as uptime. The Office should collaborate with departments that use the public safety camera network to establish performance measures that are cost effective and meet the operational needs of those departments. OEMC and the Public Building Commission (PBC) should collaborate to determine the cost and benefit of introducing this new performance measure into the current Motorola camera maintenance contract, as well as any future contracts. Documented performance metrics will ensure the vendor and the system are evaluated by the same criteria irrespective of who is conducting the evaluation.

Status of Corrective Action: **Implemented**

According to OEMC, "The PBC is no longer OEMC's project manager. The PBC is closing out one final undertaking and no new undertakings have been issued to the PBC. The OEMC has assumed the PBC-Motorola contract with a few modifications." As part of OEMC's direct management of the Motorola contract, it has established monthly uptime performance measures for the public safety camera system. Per OEMC's modified contract with Motorola, the Genetec environment, camera storage capacity, and core network availability must be functional for at least 99% of each calendar month, and the camera viewing availability must be operational for at least 94% of each calendar month. OEMC now utilizes multiple systems to monitor daily, weekly, and monthly headend application availability, camera viewing availability, camera storage, and availability of the core network. Motorola, with oversight from OEMC project managers, is responsible for ensuring the day-to-day functionality of the system.

FINDING 3: OEMC'S PROJECT MANAGER, PBC, EVALUATED MOTOROLA'S PERFORMANCE AS REQUIRED BY THE MAINTENANCE TASK ORDER, BUT ADJUSTMENTS COULD BE MADE TO IMPROVE ITS VENDOR OVERSIGHT.

OIG Recommendation 5:

OEMC should work with PBC to improve PBC's vendor oversight. These improvements could include: documenting any modifications to service levels listed in task orders and recording the vendor's compliance with those service levels; reviewing Motorola's quarterly report for errors; and developing percentile measurements for repair timeliness and assessing vendor performance against those measurements. Finally, OEMC should work with PBC to determine if the deliverables and service levels described in the maintenance task order adequately assess the vendor's performance.

If implemented, the improvements would help ensure that PBC uses a robust set of tools to evaluate the vendor's performance, demonstrating with a greater degree of confidence that the vendor is providing cost efficient and effective services.

Status of Corrective Action: **Implemented**

OEMC has assumed direct management of the Motorola contract and added the following language: "Each Prospective Task Order involving maintenance will specify applicable service level agreements (SLAs) capturing optimal system operational levels, such as uptime. Changes to SLAs will be denoted in writing via task order." OEMC stated it is "now directly responsible for all task order scopes and reviews all Statement of Works for accuracy and completeness before signing." To manage the Motorola contract, OEMC "has hired two project managers, with a third project manager likely to be hired in 2018, to oversee and enforce the contract." The project managers oversee Motorola's reporting on camera network issues and deficiencies, repair data, new camera installation, and compliance with contract service levels

MISSION

The City of Chicago Office of Inspector General (OIG) is an independent, nonpartisan oversight agency whose mission is to promote economy, efficiency, effectiveness, and integrity in the administration of programs and operations of City government. OIG achieves this mission through,

- administrative and criminal investigations by its Investigations Section;
- performance audits of City programs and operations by its Audit and Program Review Section;
- inspections, evaluations and reviews of City police and police accountability programs, operations, and policies by its Public Safety Section; and
- compliance audit and monitoring of City hiring and employment activities by its Hiring Oversight Unit.

From these activities, OIG issues reports of findings and disciplinary and other recommendations to assure that City officials, employees, and vendors are held accountable for violations of laws and policies; to improve the efficiency, cost-effectiveness government operations and further to prevent, detect, identify, expose and eliminate waste, inefficiency, misconduct, fraud, corruption, and abuse of public authority and resources.

AUTHORITY

OIG's authority to produce reports of its findings and recommendations is established in the City of Chicago Municipal Code §§ 2-56-030(d), -035(c), -110, -230, and 240.

Cover image courtesy of City of Chicago Department of Fleet and Facility Management.

PUBLIC INQUIRIES:
DANIELLE PERRY: (773) 478-0534
DPERRY@IGCHICAGO.ORG

**TO SUGGEST WAYS TO IMPROVE CITY GOVERNMENT,
VISIT OUR WEBSITE:**
WWW.CHICAGOINSPECTORGENERAL.ORG/GET-INVOLVED/HELP-IMPROVE-CITY-GOVERNMENT

TO REPORT FRAUD, WASTE, AND ABUSE IN CITY PROGRAMS:
CALL OIG'S TOLL-FREE HOTLINE
(866) 448-4754 / TTY: (773) 478-2066

OR VISIT OUR WEBSITE
WWW.CHICAGOINSPECTORGENERAL.ORG/GET-INVOLVED/FIGHT-WASTE-FRAUD-AND-ABUSE