Office of Inspector General

City of Chicago

Report of the Office of Inspector General:

•4.-::.'-

****

Office of Emergency Management and communica tions public sa fety cameras a udit

*.-<st f ?'$!} S F '^*

r n ^' ^ -t

m

OO
***•**

v3

866-IG-TIPLINE (866-448-4754) www, chicaeoinspectoreeneral. ore

Joseph M. Ferguson Inspector General

OFFICE OF INSPECTOR GENERAL

City of Chicago

740 N. Sedgwick Sheet, Suite 200 Chicago. Illinois 60654 Telephone: (773) 478-7799 Fax: (773) 47S-3949

December 12, 2016

To the Mayor, Members of the City Council, City Clerk, City Treasurer, and residents ofthe City of Chicago:

The City of Chicago Office of Inspector General (OIG) has completed an audit of the Office of Emergency Management and Communications's (OEMC) management of public safety cameras. OEMC is responsible for managing nearly 2,700 City-owned public safety cameras. OEMC also manages City, state, and federal access to a wider network of City, sister agency, and private cameras that includes more than 27,000 surveillance cameras.

OIG's audit focused on functionality and maintenance of City-owned public safety cameras, as well as whether OEMC provided camera network access to only the appropriate personnel. We found that OEMC did not comply with, and did not require other departments to comply with, Citywide policies regulating access to information systems. We also found that OEMC did not establish and enforce operational objectives for the public safety camera program and that, as a result, OEMC cannot evaluate the adequacy of current operational levels. Finally, OIG found that while OEMC's camera system project manager-the Public Building Commission (PBC)- received and reviewed vendor deliverables, adjustments could meaningfully improve PBC's vendor oversight. OIG recommends that OEMC implement robust IT security practices, develop performance measures for system operability, and review PBC's vendor oversight.

In response to the audit, OEMC agrees with our recommendations and has already initiated some corrective actions. In late 2015, OEMC began improving network access controls by replacing group logins with unique usernames and passwords. OEMC also plans to work with PBC to develop performance measures for the camera network and improve contractor oversight, while exploring alternative arrangements for program management.

The public safety camera network is a powerful tool that requires diligent management to ensure it fulfills its operational mission. These cameras are a vital component of the City's security portfolio; they enable public safety personnel to monitor incidents, including criminal activity, car accidents, and terrorist threats. Any deficiency in the network's operation creates a potentially serious safety risk, both to the public and to the first responders who rely on the cameras to provide information that often plays a vital role in assessing the scene of an incident

prior to arrival. In addition, ineffective management leaves open the possibility of unauthorized and other inappropriate use of the cameras.

Therefore, we encourage OEMC to adopt management techniques aimed at ensuring optimal performance of the public safety camera network and maintaining the public trust.

We thank OEMC, CPD, and PBC management and staff for their cooperation on this audit.

Respectfully,

Joseph M. Ferguson Inspector General
City of Chicago

OIG File #14-0568
OEMC Public Safety'Cameras Audit

Table of Contents

Acronyms

CDOT	Chicago Department of Transportation
CFD	Chicago Fire Department
CPD	Chicago Police Department
DHS	United States Department of Homeland Security
DOIT	Department of Innovation and Technology
IBM	International Business Machines Corporation
IGA	Intergovernmental Agreement
ISTP	Information Technology and Security Policies
OEMC	Office of Emergency Management and Communications
EOC	Emergency Operations Center
OVS	Operation Virtual Shield
PBC	Public Building Commission
POD	Police Observation Device
PSGS	Port Security Grant Initiative
PTZ	Pan, Tilt, Zoom
UASI	Urban Areas Security Initiative

OIG File #14-0568
OEMC Public Safety Cameras Audit

I. Executive Summary

The Office of Inspector General (OIG) conducted an audit of the Office of Emergency Management and Communications's (OEMC) management of approximately 2,700 cameras ("public safety cameras") originally purchased by OEMC, the Chicago Police Department (CPD), and the Chicago Fire Department (CFD).[1] The objective of the audit was to determine if OEMC has effectively managed these cameras. OIG assessed the effectiveness of OEMC's management by testing whether the public safety 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 the 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 the 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.

We recommend that OEMC implement policies and practices regulating access to the public safety cameras that comply with the Department of Innovation and Technology's (DOIT) Information Security and Technology Policies (ISTP), and require other entities that use the cameras to do the same. In addition, OEMC should develop and enforce reasonable standards for system performance. Finally, OIG concludes that PBC could increase the effectiveness of its vendor monitoring by implementing minor improvements. We recommend that OEMC review PBC's vendor oversight practices to identify any additional opportunities for improvement beyond those identified in this audit.

In response to our audit findings and recommendations, OEMC agreed with the findings and committed to take corrective actions, some of which have already been initiated. Specifically, based on the preliminary findings of this audit, OEMC, in late 2015, began replacing group logins with unique usernames and passwords for all Security Center users except CPD personnel in the district stations. To further strengthen its user access protocols, OEMC plans to eventually require all camera users to log in with their unique e-mail credentials, require users to abide by the City's ISTP, and develop and document policies to determine who should be granted access to the network.

In addition to access security, OEMC stated that it will develop performance measures, that will allow the Department to assess the major components of the camera system. Finally, OEMC is exploring future program management alternatives but until then, will work with PBC to improve contractor oversight. PBC agreed to document service level agreements in each task

See the Background section of this report for examples of public safety cameras and Appendix A for current camera locations.

OIG File #14-0568
OEMC Public Safety Cameras Audit

order, collaborate with OEMC to ensure vendor deliverables are documented, and provide OEMC with monthly reports on repair data and issues related to vendor reporting.

The specific recommendations related to each finding, and OEMC's response, are described in the "Audit Findings and Recommendations" section of this report.

Background

The mission of OEMC "is to manage incidents, coordinate events, operate communications systems, and provide technology, among other forms of support, to City services to strengthen
their respective missions and to protect lives and property in the City of Chicago." Part of this mission entails managing a large network of City-owned and non-City-owned security cameras.

A. The History of Chicago's Public Safety Camera Program[3]

The first public safety cameras installed in Chicago were Police Observation Devices (PODs) or "blue light" cameras.[4] CPD began installing PODs in 2003, placing some of these cameras in areas known to have high crime rates and others in locations requested by aldermen. The original CPD PODs were designed to be seen; many featured CPD logos and blue flashing lights, as shown below in the photo on the left. Subsequent models were "smaller, less overt" cameras, as shown below in the photo on the right.[5] According to OEMC, CPD has not installed a new POD camera for "three to four years." However, aldermen continue to request installation of POD cameras through the Aldermanic Menu Program.[6] Following their installation, these cameras are treated the same as any other POD.

Older model "blue light" POD camera Source: CPD's "POD Program" webpage

According to OEMC, the Office launched its own camera program, Operation Virtual Shield (OVS), around 2005. Initial funding for OVS came from the U.S. Department of Homeland

[2] City of Chicago, Office of Emergency Management and Communications, "Mission," accessed March 22, 2016, hltp://www.citvofchicago.org/citv/en/depts/oeiWauto <http://www.citvofchicago.org/citv/en/depts/oeiWauto> generated/oemmission.html,

[3] To the extent possible, OIG relied on documentary evidence to reconstruct the history of the public safety camera program. When wc could not find documentary evidence, we relied on testimonial evidence from various sources. The timeline of events presented in this report represents our best attempt to accurately describe the history of Chicago's public safety cameras.

[4] As used in this report, the term "public safety cameras" means those cameras purchased by the City's primary public safety departments: CPD, OEMC, and CFD. As we explain below, public safety cameras make up approximately 10% ofthe approximately 27,000 cameras in the City's "federated" camera network.

[5] City of Chicago, Chicago Police Department, "POD Program," accessed June 22, 2016, <http://home.chicagopolice.org/inside-the-cpd/pod-prograrn/>. To our knowledge, the photo on the left (a "blue light" camera) is no longer available on the CPD web page.

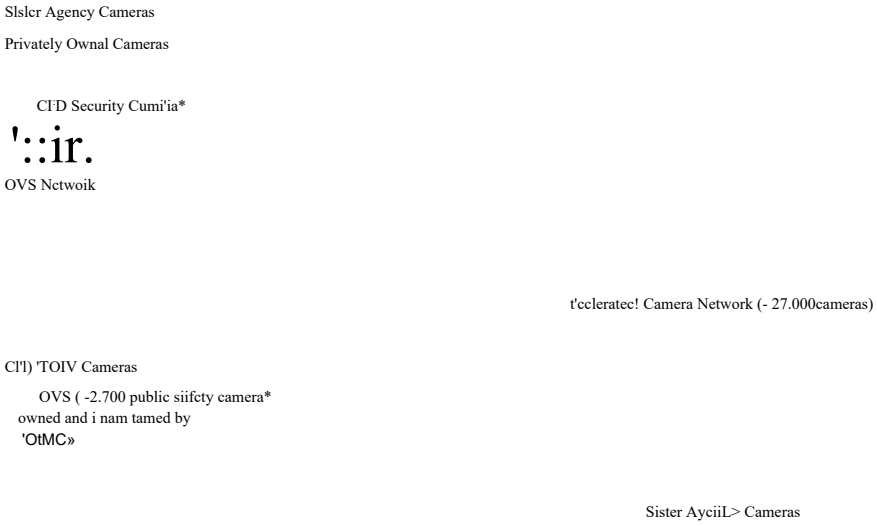
[6] The Chicago Department of Transportation's (CDOT) Aldermanic Menu Program provides each of the 50 aldermen with SI.3 million per year for residential infrastructure projects. Public safety cameras are on the Aldermanic Menu, currently priced at $22,500 each.

Security (DHS), with a mandate to install cameras near locations determined to be potential targets for terrorists.[7] Accordingly, OEMC installed most of the original OVS cameras near event spaces, within sight of significant infrastructure, and in the central business district.[8]

Over time, OEMC shifted its focus from installing new cameras to expanding the OVS network by incorporating all other existing City-owned cameras. Historically, OEMC and CPD shared video, but maintained separate contracts for camera services and software. Then, around 2009, OEMC began to incorporate CPD cameras into OVS. CPD moved its camera unit into OEMC's building, and assimilated its POD cameras into OEMC's existing service agreement. According to CPD, it now partners with OEMC in the public safety camera program, with OEMC acting as the lead agency-a role that includes dealing with vendors and signing and managing contracts. By 2012, OEMC had also incorporated CFD's security cameras (e.g., security cameras at firehouses) into OVS.

In addition to City-owned cameras, OEMC invited private businesses and sister agencies (e.g., the Chicago Park District and Chicago Transit Authority) to link their cameras to the City's network, thereby creating a broader federated network that OEMC estimates now includes over 27,000 cameras.[9] OEMC is currently responsible for maintaining the approximately 2,700 City-owned cameras that constitute OVS, as well as managing the IT infrastructure supporting the federated network. The figure below illustrates the evolution of Chicago's camera network from 2003 to date.

Evolution of Chicago's Public Safety Camera Network



Source: OIG illustration based on information provided by OEMC.

[7] DHS provided federal funding through the Urban Areas Security Initiative (UASI) grant.

[R] With OVS, as is generally the case, camera location is dictated by the funding source. Another example of funding determining camera placement is the Aldermanic Menu Program. OEMC explained that a camera requested through the Program must be placed in, and remain in, that alderman's ward. However, most aldermen who choose cameras from the menu consult with CPD personnel to detennine placement.

[9] For more information on OEMC's "Private Sector Camera Initiative," including information regarding how to link a private camera to the network, see
httn://www.cityofchicago.org/city/en/dcpts/oem/provdrs/tcch/svcs/link
<http://www.cityofchicago.org/city/en/dcpts/oem/provdrs/tcch/svcs/link> your cameras.html.

OIG File #14-0568
OEMC Public Safety Cameras Audit

OEMC reported that it has spent $139.8 million on the camera program since 2006. It estimated that the portion paid to PBC for its services-described in the next section-is 8-10% of the total, or $11.1-S14.0 million, as shown in this table.[10]

Year	Expenditures	Estimated Portion @8%@ 10%	for PBC Services
2006 j$S	*2/^299.46*	*$ 1,982,023.96^ ^477,529l>5*	
_ 2007	*. ' . -*		
[:■ ;!2j$8/rF	*^W^ie.iTt;^*		
2009	2,597,212.35	207,776.99	259,721.24
% JP°JI	8,250,577.76	' . _; . 660,046.22..F' 82p57.7j||j	
2011	16,233,300.58	'1,298,664.05	1,623,330.06
2013	32,674,804.04	2,613,984.32	3,267,480.40
■ M°HM	20,295,315,86 L..	i^'.;- ■ ;J.,623,625i27	|·2,02p31.59]
2015 9,326,591.03	*746,127.28*	*932,659.10*"*	
*["'^2016W ':M8M2l&9^^*			
TOTAL	$ 139,767,240.87	$ 11,181,379.27	$ 13,976,724.09

Source: OEMC

According to OEMC, the majority of funding for the camera program has come from DHS Urban Area Security Initiative (UASI) grants. Other sources include DHS Port Security Grant Program (PSGP) and Emergency Operations Center (EOC) grants as well as private funding from Chase Bank, as shown in the table below." However, OEMC could not provide a complete accounting for all funding sources. Regarding the unknown sources, OEMC explained that "grants are separated in our finance system by a 'Fund Number.' In older years fund numbers were re-used thus making it difficult to distinguish between certain funding sources. The fund report also did not generate results prior to 2009 therefore there are unknowns."

OEMC pays PBC on a reimbursement basis bul does not track what portion of each payment is for the services of PBC, Motorola, or any sub-contractors. This detail is only available on individual task orders. OEMC reviewed a selection of task orders and estimated that the portion for PBC's services averaged 8-10%. In 2006, PBC signed a contract with International Business Machines Corporation (IBM) for the development and maintenance of a citywide camera network. In 2010, PBC signed a contract with Motorola for the "OEMC camera infrastructure program."
" According to OEMC, "J.P. Morgan Chase Bank provided the City with a grant to install additional cameras around Chicago Public Schools."

Amount

521,253.87

8,27i,134?90

12,558,399.07'
16,385,545.57
17,203,440^21

4,821,475.03
11226,206^67^
■.Tim...

■fe:.,^.. i.,;,„L294;79J2fr6 '

UASI 2007

UASI 2009
■§|v UAsF20'i0orEOC2010 UASI 2011/UASI 2012/Park District

UASI 2014

:'':$§WASI2015
Non-OEMC grants or Corporate
Unknown CPD grant
f||Y2obc^
9,929,420.45
$139,767,240.87

: finance fund report. ^
Unknown. Did not appear on finance fund report.

TOTAL

Source: OEMC

B. Public Safety Camera Operation and Maintenance

In 2006, OEMC entered into its initial intergovernmental agreement (IGA) with PBC[12] to build out OVS.[13] PBC's role was to retain a vendor to create and integrate a network and surveillance system, and to serve as the project manager on the City's behalf. In 2011, OEMC and PBC executed the current IGA, which assigns PBC the authority to enter into contracts with one or more vendors for the purpose of maintaining and enhancing OVS, and to enforce the terms and conditions of any vendor contracts.[14] The IGA authorizes PBC to issue task orders to the vendor describing the "Services and Deliverables" the vendor is expected to provide in "accordance with applicable provisions" of the contract and IGA.

On December 30, 2010, PBC entered into a five-year contract with Motorola to provide public safety camera "System Integration Services."[15] Specifically, the contract calls for Motorola to upgrade the City's fiber optic surveillance network, to build a platform to view camera feeds, and to provide ongoing repair and maintenance.

The contract contemplates the issuance of task

[12] PBC was created in 1956 by the City of Chicago pursuant to the State of Illinois Public Building Commission Act, 50 ILCS 20, to oversee and ensure the quality of public construction projects.
[13] OEMC and PBC implemented OVS in four phases, corresponding to IGAs dated June 30, 2006, July 31, 2006, October 1, 2009, and March 15, 2010.
[14] Specifically, the IGA requires PBC to "enforce the terms and conditions of the Program Agreement and avail itself of the rights and remedies in the Program Agreement and all other agreements pertaining to the Program, consistent with the requirements thereof in order to protect the best interests ofthe City and PBC." The IGA defines the Program Agreement as "one or more contracts between PBC and the Vendor, and any amendments or modifications thereto, including all of the contract documents and exhibits described therein, and providing for Services, Deliverables, Goods, labor, materials, equipment, custom software, software licenses, software systems integration, arid other consulting services required for the implementation of the Program."
[15] Public Building Commission of Chicago, Contract Number PS1836, December 30, 2010, accessed March 24, 2016, <http://www.pbcchicago.com/upload/arlicleDoc_3639.pdf>. The original contract was effective through December 31, 2015 and has been extended through December 31, 2016.

orders directing Motorola to perform services, "determined on an as-needed basis and as described in a Task Order Services Request." According to PBC, the contract provides the general framework for the camera program while task orders specify the services needed. A task order may cover a variety of services, including installation of new cameras, camera maintenance, and software support, and may apply to a discrete set of cameras and equipment. PBC explained that a task order supersedes any requirements stipulated in the contract as well as any services required by previous task orders. PBC stated that it has issued more than 90 task orders pursuant to the Motorola contract, and that it issued the first maintenance task order three months after the contract went into effect. PBC issued the current maintenance task order, number 893, on December 9, 2015.

The service level agreement included in the contract requires Motorola to report on a quarterly and monthly basis how its performance has compared to five service level measures, including call back time for service requests, arrival time at service locations, and completion of root cause analysis for camera failures. [6] The contract provides that if Motorola fails to meet any of these service levels, PBC is entitled to certain credits against amounts owed-credits that would then be passed along to OEMC through PBC's invoices. However, PBC's current maintenance task order replaced the five service level measures with two: "response time on site" and repair time. Repair time remains the only service level with a financial penalty for default. If Motorola fails to meet the repair time service level for specific repair types, the vendor is liable for a credit worth up to $500.00 per occurrence.[17] In addition to the service level provision, the current maintenance task order includes other deliverables, such as quarterly reports on the inventory of spare parts and weekly updates on the status of network equipment.

OEMC explained to OIG that the City's cameras are used both proactively (e.g., by zooming in on a crime in progress) and retrospectively (e.g., by accessing archived footage of a crime). Therefore, a fully functional camera must be capable of both recording footage and transmitting live images. Based on OEMC's explanation, OIG conducted its review and analysis on two distinct categories of functionality. The first category, referred to here as optical operability, is defined as a camera that transmits a clear image, has pan-tilt-zoom (PTZ) capability, and has the ability to auto-focus.[19] The second category, footage retention, is defined in relation to OEMC's policy generally requiring most public safety cameras to retain footage for 30 days, factoring in stated exceptions including for CPD POD cameras, which have a 15-day retention requirement, and older-model cellular cameras, which retain footage for 72 hours.[20]

[16] Public Building Commission of Chicago, Contract Number PS1836, December 30, 2010, Schedule 3.1(f), accessed October 31, 2016, <http://www.pbcchicago.com/upload/articleDoc> 3639.pdf.
[17] The task order defines three levels of malfunction severity and provides that Severity 1 issues (the most severe) must be repaired in 8 hours while Severity 2 issues must be repaired in 48 hours when "feasible." The task order defines feasible repairs as "those where spare parts are in-stock and available for immediate deployment into the field." See Appendix C for details.
[IS] See Appendix C for a description of the task order 893 service levels and deliverables.
[19] Pan-tilt-zoom (PTZ) refers to a camera's capability to move left, right, up, and down, and to zoom in and out. Auto-focus refers to a camera's capability to refocus subsequent to movement. Certain cameras qualify as operational despite lacking one or more of the three capabilities identified by OEMC. For example, some older, "fixed" cameras lack PTZ capability.
[20] OEMC stated that it would be better if all cameras were held to a 30-day retention schedule, but the City has neither the infrastructure nor the money to bring all cameras up to this standard. OEMC explained that detectives

OEMC expects that cameras will be. maintained in working condition. However, it has no documented goal for what percentage of cameras should be fully functional at any given time.

In the event a user, for example a CPD detective, discovers that a particular camera is not working properly, he or she can submit a repair request to OEMC. If OEMC approves the request, it sends a work order to Motorola and PBC.[21] Motorola then dispatches a crew to assess the situation. PBC, however, must approve all repairs before the vendor can begin work. To close out a work order, the vendor must submit screen shots of the repair to PBC and OEMC, and an end user confirms that the relevant camera is working properly. OEMC stated that it relies on PBC's project management expertise to ensure that all installations and repairs are completed as required under the contract.

C. Public Safety Camera Access

A single individual at OEMC holds the authority to determine who is allowed to access public safety camera feeds. According to the Office, the decision to grant access, at what level, and for how long is based on the requesting party's job duties. If OEMC approves a request, it contacts Motorola, and the vendor creates a new user ID. OEMC may also grant temporary access to federal and state agencies during special events.[22] A user can access camera feeds and archives through the Genetec "Security Center" application, provided that his or her computer terminal falls within a specific Internet Protocol (IP) address range.[3] Most users, including police officers, have limited privileges, which allow them to view live feeds, move the camera, and view archived footage.[24] Only a few users have administrator privileges, which allow them the additional authority to download, as opposed to simply view, archived footage and to configure system settings.[25] Non-administrators who wish to download archived video must request it from an administrator.

The same individual at OEMC who approves new user access also reviews and updates the user list. According to the Office, these reviews occur approximately every quarter. To conduct its review, OEMC requests the current user list from Motorola and reviews each username to ensure that access is limited to the appropriate personnel. If OEMC discovers that a user changed jobs, was terminated, has not recently logged on, or temporary access is no longer needed, the Office

investigating a crime arc responsible for filing a timely footage request, and that if they wait too long and the footage no longer exists, the blame resides with them.
*' In some cases OEMC may determine that it is more cost effective to replace rather than repair a camera, therefore it would not approve the repair request.
[22] For example, during the 2012 NATO Summit, OEMC granted public-safety-camera access to the FBI, the Secret

Service, and the Illinois State Police.
[23] Genetec, a software company specializing in IP video surveillance, is a subcontractor for Motorola. See Appendix B for an example of Genetec's Security Center application.
[24] According to OEMC, only public safety personnel are allowed access to public safety cameras because those cameras focus on "critical infrastructure protection." For this reason, OEMC denies Freedom of Infonnation Act requests for public safety camera video. OEMC is concerned that, if placed in the wrong hands, public safety camera live feeds and footage could reveal blind spots in the City's security network.
"[5] Administrators can also set up "partitions" that limit which cameras a user can view. At the time of this audit, there were five administrator accounts dedicated to City employees and seven accounts dedicated to the vendors (three accounts for Motorola, three for Genetec, and one for Quantum Crossings, another subcontractor for Motorola).

directs Motorola to remove the user. OEMC does not independently determine employment status of Security Center users. Rather, OEMC relies on users to notify it of personnel changes.

III. Objectives, Scope, and Methodology

A. Objectives

The objective of this audit was to determine if OEMC effectively managed the City's public safety cameras. OIG defined effective management as ensuring,

- camera optical operability;
- camera footage retention for the required amount of time;
- reasonable timelines for camera repair and maintenance; and
- appropriate restrictions on access to cameras and footage.

B. Scope

OIG's audit reviewed OEMC's management of approximately 2,700 public safety cameras- those cameras originally purchased and installed by CPD, CFD, or OEMC.[26] When we began the audit, we sought to evaluate how PBC monitored the vendor's compliance with the service level agreement included in the Motorola contract. During the audit, PBC informed us that the service levels and deliverables described in maintenance task orders superseded the service level agreement in the contract. Therefore, we limited our review to maintenance task orders.

We did not review camera placement, because choice of location is often dictated by the funding source.[27] In addition, OEMC explained that its primary concern is the repair and maintenance of existing cameras, not the installation of new cameras. At this time, we did not evaluate the effectiveness ofthe public safety camera network.[28] Nor did we consider any effect public safety cameras may have on individuals' constitutional and other legal rights. Finally, this audit does not address the use and oversight of police dashboard cameras or body cameras.

C. Methodology

To ensure that OEMC provided OIG a complete and reliable list of public safety cameras, we compared OEMC's, CPD's, and PBC's inventory records.[29] We then created a list of cameras found in CPD's and PBC's records, but not OEMC's, and

asked OEMC to explain these differences. Explaining that the inventory list it provided to OIG contained only "street" cameras, OEMC, at our request, provided a more complete inventory list that included cameras mounted in City Hall and the Chicago Pedway. Based on our comparison testing and follow-up

[26] This inventory also includes cameras purchased through the Aldermanic Menu Program.
[27] As noted in the Background section of this report, the federal grant required that OVS cameras be installed near locations determined to be potential targets for terrorists. Similarly, aldermen control camera location for cameras installed through the Aldermanic Menu Program.
[2R] Some of the effects of public safety cameras are easily measureablc, while others are more complicated. For example, police officers can indicate in their reports if a POD camera assisted in an arrest. In 2015, officers reported that POD cameras assisted in 0.2% of CPD's total arrests (233 out of 113,928). Other effects are more complicated and difficult to measure. For example, the deterrent effect, if any, of the public safety cameras is not easy to quantify.
[29] Because CFD's camera inventory was relatively small and OEMC expressed confidence that its list included all CFD cameras, we did not request a separate inventory from CFD.

questions, we found the public safety camera inventory records sufficiently reliable for testing purposes.

To determine if public safety cameras were fully functional, OIG reviewed camera optical operability and footage retention.[30] To review optical operability, we drew a simple random sample of public safety cameras. We then accessed the feed of each camera in our sample on an OEMC computer terminal that was connected to the Security Center network. To qualify as optically operational, a camera needed to have PTZ capabilities, have a working auto-focus feature, and broadcast a clear image. If a camera did not meet one or more of these criteria, or if it was not connected to the network, we considered the camera non-operational.[31] To assess footage retention, OIG drew a second simple random sample from the list of public safety cameras, excluding 505 older model "cellular" cameras because they record to an internal drive rather than to the network.[32] We accessed this sample of cameras at OEMC. OEMC and CFD cameras were required to retain footage for 30 days, while CPD cameras were required to retain footage for 15 days.[33] If a camera had not retained footage for the required number of days or was disconnected from the network, we considered the footage retention insufficient.[34]

To evaluate whether the City's cameras were repaired and maintained expeditiously, OIG interviewed PBC, OEMC, and vendor staff. We conducted a ride-along with maintenance staff, and analyzed PBC's and Motorola's maintenance records to determine camera repair times. We compared our findings with the responsibilities set out in the IGA between OEMC and PBC, and the deliverables described in task order 893.

To ensure the reliability of PBC's repair and maintenance records, OIG interviewed PBC staff and compared records maintained by PBC and Motorola. We discovered some data-reliability issues, but opted to proceed with our analysis of PBC's data in order to offer at least an estimate of repair time.[35]

To assess whether OEMC limited access to public safety cameras to appropriately authorized personnel, OIG interviewed OEMC staff, and compared the Office's security practices to the

' See "Camera Operations and Maintenance" in the background section of this audit report for more infonnation on operability and footage retention.
[31] If a public safety camera is not connected to the network, this docs not necessarily mean the camera is broken. For example, there are "mobile" cameras attached to CFD boats and CPD helicopters. These cameras must be activated

to begin broadcasting an image and recording footage. The user department, not OEMC, is responsible for determining when to activate mobile units.

[32] To review cellular camera retention, OIG would have needed to visit the physical location of the camera with OEMC crews to extract the footage. This would have been overly time consuming for both OEMC personnel and OIG staff. In any event, OEMC stated that it is phasing out cellular cameras. We thus decided to exclude cellular cameras from our review of archived footage.

[33] The Local Records Commission of Cook County approved OEMC's 30-day retention schedule. CPD's 15-day retention schedule is documented in CPD Special Order S02-04-01.

[34] As with operability, a public safety camera may be disconnected from the network, and, thus not recording, for a number of reasons. If a camera is not connected to the network, this does not necessarily mean the camera is broken or that OEMC is responsible.

[35] OIG found discrepancies between Motorola and PBC records, including differences between opening and closing dates for single repair tickets, incomplete case descriptions, and inaccurate repair totals. Given these discrepancies, we cannot attest to the reliability of PBC's maintenance records. For more information, see Finding Three below.

Department of Innovation and Technology's (DOIT) Infonnation Security and Technology Policies (ISTP).[36] We also reviewed a list of Security Center user IDs to determine if OEMC limited access to cameras to current City employees. OEMC provided OIG with a list of Security Center user IDs, explaining that Motorola had generated the list.. OEMC did not verify that the vendor had accounted for all users.[37] Therefore, while OIG used this list to assess OEMC's management of account access, we cannot attest to its completeness.

D. Standards

We conducted this audit in accordance with generally accepted Government Auditing Standards issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

E. Authority and Role

The authority to perform this audit is established in the City of Chicago Municipal Code § 2-56-030 which states that OIG has the power and duty to review the programs of City government in order to identify any inefficiencies, waste, and potential for misconduct, and to promote economy, efficiency, effectiveness, and integrity in the administration of City programs and operations.

The role of OIG is to review City operations and make recommendations for improvement.

City management is responsible for establishing and maintaining processes to ensure that City programs operate economically, efficiently, effectively, and with integrity.

For more detail on information security, sec DOIT's "IS and IT Policies" webpage at <http://vvww.cityofchicago.org/citv/en/depts/doit/supp> info/is-and-it-policies.html. For the ISTP, see <http://www.citvofchicago.org/content/dam/citv/depts/doit/supp_info/IS%20and%20IT%20Polices/CoC> IT IS Polic v Set ver RC 05.pdf.

[37] For more information on how OEMC manages access lo Security Center, see "Camera Access" in the background section above.

IV. Findings and Recommendations

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.

DOlT's Information Security and Technology Policies (ISTP) describe the minimum security requirements for City information systems. According to DOIT, all City departments must configure their information systems in a way that complies with the standards set forth in the ISTP. OIG's audit discovered that OEMC's public safety camera access procedures violated the ISTP, and thus prevented OEMC, in some cases, from determining whether a camera was used in an inappropriate manner.

Effective access controls provide "reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals."[38] The access controls described in the ISTP were designed to ensure that only authorized users have access to City IT systems, and that those users receive only the appropriate level of access. Specifically, the ISTP requires departments to comply with several practices designed to promote access security:

- Subsection 7.1.1(b) "Access rights granted to systems must be limited to the minimum access rights necessary for the user to fulfill their responsibilities as determined by their role."
- Subsection 7.2.3(c) "Passwords used on the City's systems and on non-City systems that are authorized for use must... be changed at a minimum every 90 days... be unique for each system, site and/or environment."
- Subsection 7.3.1(a) "... ensure that user registration, modification, and deregistration procedures are implemented for user access rights on all information systems. These procedures must be documented."
- Subsection 7.3.2(b) "Individual or group sharing of usernames and passwords is strictly prohibited."[39]

In addition, the ISTP requires that physical access to IT resources be "tightly controlled."[40]

United States Government Accountability Office, "Federal Information System Controls Audit Manual (FISCAM)," February 2009, 11, accessed April 15, 2016, <http://gao.gov/assets/80/77142.pdf>.

[39] City of Chicago, Department of Innovation and Technology, "Information Security and Technology Policies," 2014, Section 7.0, accessed April 15, 2016, <http://www.citvofchicago.org/content/dam/ci%5e> IT IS Folic v Set ver RC 05.pdf.

[40] Specifically, Section 2.2.2 of the ISTP requires "a process for restricting and monitoring physical access to City facilities must be implemented." Subsection 2.2.2(b) requires "physical access to all non-public areas is tightly controlled. Doors must be secured at all times and only authorized personnel may have access." City of Chicago, Department of Innovation and Technology, "Information Security and Technology Policies," 2014, Policy Number 2.0, accessed April 15, 2016,

During our audit, OIG learned that some individuals accessed the public safety camera network through the Security Center application using group logins and group passwords, and were not required to provide unique identification prior to logging on. We also learned that users were not required to change their passwords on a regular basis. For example, at CPD district stations officers used shared computer terminals to access all of the approximately 27,000 cameras in the federated network. Each district had its own group username and group password login. The usemame for each district reflected the district station number, and each district had a similarly generic password.[41] Officers were not required to sign in or otherwise identify themselves prior to using a computer terminal with access to the public safety cameras. In addition, OEMC stated that Security Center users were not required to change passwords. Group logins make it difficult to identify which individuals accessed the system. The ISTP prohibits group usernames and passwords for City applications, and generally requires passwords to be changed every 90 days. The ISTP also requires strict monitoring of physical access to computer terminals [42]

OEMC recognized that group logins were an issue, and, in the case of CPD, expressed interest in having officers log into the Security Center application with a unique usemame. However, according to OEMC, it had been unable to implement this practice due to software compatibility issues.[43] OEMC also did not believe it could compel end users at CPD, sister agencies, and federal agencies to implement physical controls. However, it is authorized to control and enforce all system permissions and access to the public safety camera network.[44] OEMC also orally communicates expectations for camera usage to new users. According to OEMC, police cadets receive Security Center training and there is a "how to use Security Center" video posted on OEMC's intranet portal. OIG reviewed the training Power Point, but found no information relating to appropriate usage of the public safety camera network. OEMC further stated that it had not created policies or procedures governing Security Center usage for non-public safety users.

Along with password, username, and physical security deficiencies, OIG found that OEMC could not verify that each user had the appropriate level of access, nor could the Office confirm the identities of all persons with access to the public safety camera network. OIG asked OEMC to provide its criteria for determining what level of access to grant a particular user. OEMC responded that it had no documented criteria. Regarding the user lists OEMC used to conduct quarterly access reviews, neither the Office nor Motorola had the technical capacity to electronically generate a report of all existing user IDs. OEMC considered asking the vendor to

<http://www.citvofchicago.org/content/danVcirv/depts/doit/supp> info/IS%20and%201T%20Polices/CoC_lT_IS Polic v Sel ver RC

05.pdf.
[41] As of March 2016, there were 22 police districts and 11,906 sworn officers in CPD.
[42] There are several factors at OEMC and CPD that mitigate the risk of inappropriate access and usage. First, the Security Center application can only be accessed within specific IP ranges and privileged access is limited to a few individuals. Second, entry barriers, such as security desks, prevent unauthorized individuals from gaining access to OEMC headquarters and CPD district stations. Finally, according to OEMC, it would be difficult to hack into the. application, because the network is "closed." OIG did not review the sufficiency of these factors during our audit.
[43] Initially, the Security Center application was not compatible with CPD's e-mail directory. However, in its management response to this finding, OEMC, states that the purchase of an active directory license will resolve compatibility issues and pennit the use of e-mail login credentials.
[44] DOIT confirmed that application managers at the department level are responsible for ensuring that other departments, including sister agencies that use the application, arc in compliance with the ISTP prior to receiving access.

build this functionality into the Security Center application, but, at the time of our audit, it had established no timeframe for completing this task. Instead, OEMC contacted Motorola, and the vendor physically transcribed user names, permission levels, and last-access dates into a spreadsheet. OEMC could not verify that Motorola had accounted for all active users.

OEMC stated that they regarded the City's ISTP as "guidelines," and explained that "specific application of those guidelines has to be viewed through the framework of the first response mission of OEMC and its specific technology requirements." Without robust access controls, however, such as those required by the ISTP, OEMC cannot provide reasonable assurance that the public safety camera network is secure. This creates the possibility of inappropriate access and improper use of public safety cameras. For example, in 2012 OIG investigated an allegation that an individual manipulated a public safety camera to avoid recording a CPD arrest.[4] OIG could not complete the investigation, because OEMC did not maintain camera usage records and thus was not able to trace usage to a specific person. This risk persists for all terminals with group logins because OEMC still cannot identify individual users.[46] Without documented policies and procedures for granting and reviewing access, OEMC cannot demonstrate that only appropriate personnel had access to cameras. Moreover, if the OEMC official who is currently in charge of account approval and revocation leaves the position, there will be no guidelines for future staff to follow. Finally, OEMC acknowledged that it would be possible for a vendor to grant access to one or more individuals without the Office's knowledge, and to neglect to notify OEMC of new users.

Recommendation:

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, 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.

To address the issue of ensuring that outside agencies comply with the City's ISTP, OEMC should require all outside agencies to abide by a user agreement as a condition of Security Center

OIG opened this investigation based on a May 2012 report by WBEZ. The report implied that a user manipulated a POD camera to

avoid capturing police activity during an arrest. Rob Wildebocr, "What a police camera did NOT record," WBEZ, December 21, 2011, accessed April 18, 2016, <https://www.wbez.org/shows/wbez-ncws/what-a->police-camera-did-not-rccord/4af5c84e-0c41-4f4f-b43f-805daa8bc982.

[46] OEMC explained that it cannot detect inappropriate usage in real time, but instead relies on user complaints to detect inappropriate usage. If the Office needs to investigate a complaint, it can trace camera usage back to a specific computer terminal and then ask staff to identify who used the computer at the specific time in question. Yet, akin to the problems OIG encountered, OEMC's ability to investigate inappropriate usage is undermined by its inability to determine with certainty who used a particular terminal at a particular time. While OEMC may be able to discover the identity of a user of a group login within the OEMC facility (because only a few staff have Security Center access), it seems unlikely that OEMC could do this if the use in question occurred at a CPD district. Moreover, common sense dictates that an individual who used a camera for an unauthorized purpose, would not admit to using the particular terminal at the particular time in question. c

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. Finally, 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.

Management Response:

"Based on the preliminary findings of this audit, OEMC, in late 2015, began replacing group logins with unique usernames and passwords for all Security Center users except CPD personnel in the district stations. OEMC agrees that it should strengthen its protocols related to accessing the Public Safety Camera Network ("Camera Network"). Currently, OEMC requires all users to log into the Security Application Center through the use of a unique username and password. The Security Application Center also allows OEMC to generate user logon and logoff audit reports and permission levels via a server queiy.

"To strengthen its protocols related to accessing the Camera Network, OEMC has purchased an active directory license from Genetec. Following some integration with active directory, this license will allow OEMC to be able to require all City of Chicago users of the Security Application Center to login with their active directory E-mail login credentials. This will allow OEMC to maintain an electronic record of every individual who accessed the system, and track what they viewed through the use of the Camera Network. The use of the active directory integration will also require that passwords be changed every (90) ninety days.

"Additionally, OEMC agrees, as an interim measure, to request that all users of group logins create and maintain physical records of the identities of each and every user who accessed the Camera Network, including the date and time of access. OEMC will also request that these records be submitted to the OEMC on a monthly basis.

"OEMC will develop a Memorandum of Understanding (MOU) that all external agencies will be required to agree to before access to the Camera Network is granted or continued. The MOU will outline and demand requirements consistent with the City's ISTP. The MOU will also outline the business reason(s) for granting the privileged access, and state that any agency and/or individual user found not to be in compliance with the terms and conditions of the MOU may have their access denied.

"OEMC will also put into written form, an internal policy that will provide guidance for determining who should be allowed access to the Camera network, the level of access to be granted, and the reasons and process to deny access. "

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 reviewed a sample of the public safety cameras to determine how many were optically operable and how many retained recorded footage for the required amount of time. We found that 2,281, or 85.0%, of 2,683 cameras were operational[47] -meaning that they transmitted a clear image, had pan-tilt-zoom (PTZ) capability, and had the ability to auto -focus- and that 1,984, or 91.1%, of 2,178 cameras stored footage for the required number of days.[48] We based our determination of optical operability and footage retention on criteria provided by OEMC.[49] However, OIG was unable to determine if our test results represented an acceptable level of performance, because OEMC had no documented expectations for what percentage of public safety cameras should be fully functional at any given time.

In response to OIG inquiries, OEMC expressed an informal expectation that at least 95% of public safety cameras connected to the network should be fully functional at any given time. While OEMC stated that it may have communicated this expectation to Motorola, it could not say so with certainty and it was not documented as a formal goal. OIG researched other City of Chicago camera contracts to determine whether they included system performance requirements. We identified three contracts that stipulated "system uptime," or the amount of time the system is fully functional as defined in the contract, as a deliverable. These contracts included two current Chicago Department of Transportation (CDOT) contracts for red light and automated speed enforcement programs as well as an OEMC contract that the Office managed when it ran the City's red light enforcement program. OEMC's contract required 95% of all the cameras in the system to be functional in any consecutive five-day period. In addition, one CDOT contract is more detailed, assigning different requirements to different categories of cameras including one category requiring 85% system -wide functionality in a given month and another requiring 95% functionality during specified hours. OIG also spoke with staff at the Department of Procurement Services, who stated that it is reasonable to include uptime as a metric in camera contracts.

OIG asked OEMC and PBC about incorporating uptime expectations into their vendor management strategies. Both agencies expressed concern regarding the use of uptime, stating that public safety cameras have various dimensions of functionality. For example, a public safety camera might not transmit an image due to a temporary disruption in its wireless signal.

[47] The estimated error rate in the population is based on observing errors in our probability sample of 134 cameras. Because this estimate is based on a probability sample, it is subject to sampling error. A different probability sample could have produced different results. Based on the size of our sample and the method used to select it, we are 95% confident that the error rate in the population is between 9.5% and 21.9%.

[48] As discussed in the Methodology section of this report, we excluded 505 cellular cameras from our review of archived footage. Thus, the population sizes between our operability review and recorded footage review were different. The estimated error rate in the population is based on observing errors in our probability sample of 325 cameras. Because this estimate is based on a probability sample, it is subject to sampling error. A different probability sample could have produced different results. Based on the size of our sample and the method used to select it, we are 95% confident that the error rate in the population is between 6.3%> and 12.3%.
[49] For more information on how we conducted our testing see the Methodology section of this report. For more infonnation on the criteria we used, see Camera Operation and Maintenance in the Background section of this report.

Categorizing this scenario as "functional" or "not functional" would require OEMC to define a threshold for acceptable performance. In addition, PBC reported that OEMC did not incorporate uptime expectations into the Scope of Services for the IGA, and explained that PBC designed the Motorola contract to focus on repairing broken cameras rather than maintaining a functionality threshold. While defining functionality and measuring uptime for public safety cameras may require some deliberation, it is a viable goal. Like public safety cameras, red light and speed cameras have nuanced degrees of optical operability, such as image quality. Nevertheless, the drafters ofthe red light and speed camera contracts were able to define enforceable standards.

Without documented standards for system operational levels, OEMC cannot determine if current performance levels are adequate or benchmark performance over time. And without the ability to assess performance over time, OEMC cannot determine if the system consistently meets the operational needs of end users. For example, in 2015, CPD reported 233 POD-assisted arrests. If CPD wanted to determine whether this number was an acceptable outcome and whether cameras were effective tools in solving crime, it would need reasonable assurance that the system functioned consistently. In addition, without documented system performance metrics, OEMC cannot require a vendor to maintain the system at a specified operational level.

Recommendation:

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 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.

Management Response:

"OEMC currently monitors the performance of its Camera Network via the review of a Daily Defect Report. This report tells OEMC eveiy single camera that is failing to communicate with the headend application, and in need of troubleshooting intervention. However, OEMC agrees that it can strengthen its performance measures, and as such OEMC will develop performance measures that will capture the uptime and overall health of the entire Camera Network. Performance measures will be developed for the three (3) major components that make up the Camera Network, which are headend application availability and storage, network availability, and camera viewing availability. The headend application availability and storage measure will tell OEMC the overall availability of the system for every user; the network availability measure will tell OEMC if major segments of the Camera Network are down; and the camera

viewing availability measure will tell OEMC the percentage of cameras working at any given point in time.

"Additionally, OEMC will engage in active discussions with end-users of our Camera Network, as well as PBC, to determine the need for and feasibility of additional performance measures. "

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.

OEMC relied on PBC, as the contracted project manager, to ensure the expeditious and cost-effective completion of repairs to public safety cameras. PBC, pursuant to the Motorola contract, issued task orders for camera maintenance services. OIG found that PBC received the deliverables required by the current maintenance task order and employed additional methods to evaluate the vendor's performance. However, while PBC stated that these methods were sufficient to evaluate the vendor, OIG found that minor changes could strengthen PBC's vendor oversight.

The current maintenance task order requires the vendor to respond on site to the most serious issues (called "Severity 1") within four hours, to Severity 2 issues within 24 hours, and to Severity 3 issues within 48 hours.[50] Once on site, the vendor is required to complete "feasible" repairs-those that can be completed with spare parts in stock-for Severity 1 issues within 8 hours and for Severity 2 issues within 48 hours.[51] Although there is no financial penalty related to response time, the vendor's failure to meet the Severity 1 or Severity 2 repair time results in a $500.00 or $250.00 credit, respectively, per occurrence. PBC used weekly phone calls, an open case spreadsheet, and e-mails sent by the responding technician to evaluate the vendor's compliance with the service levels. According to PBC, the vendor has yet to default on the service level for a feasible repair, and, thus, has not been liable for the financial penalty.

In addition to the response time and repair time service levels, the task order enumerates several deliverables that Motorola is required to provide.[52] OIG found that PBC received the required deliverables and used them to evaluate the vendor's performance. For example, Motorola satisfied the "quarterly reports" and "quarterly spares report" deliverables by "providing PBC with a quarterly repair report. PBC used the information in the quarterly reports to review repair and maintenance issues with the vendor. Beyond the requirements of the task order, PBC employed additional techniques to monitor the vendor's performance. According to PBC staff, project managers review invoices for cost reasonableness, verify the vendor's explanations for prolonged repairs,[53] and conduct field audits of vendor repairs when possible.

OIG reviewed PBC's documents to ensure the documents were accurate, to ensure the vendor had met the service levels, and to measure the timeliness of repairs. OIG's assessment of the open case spreadsheet revealed nine repairs where the vendor appeared to have exceeded the applicable repair timeframe. The documents that PBC provided did not record a timestamp to specifically measure the amount of time it took the vendor to respond to issues nor did they

" The task order defines a severity level one issue as a "major issue that results in an unusable system, subsystem, product, or critical features from the user's perspective." A severity level two issue is a "moderate issue that limits a Customer's nonnal use of the system, sub-system, product, or major non-critical features from a Customer's perspective." A severity level three issue is a "minor issue that docs not preclude use of the system, sub-system, product, or critical features from a Customer's perspective." See Appendix C for a description ofthe service level. [1] See Appendix C for details.

[52] See Appendix C for a list of deliverables.

[53] PBC provided examples of what it deems to be valid reasons for delays in making repairs: the need to dig the street up to get access to a power cable; the need to use a barge to access a malfunctioning camera located near a body of water; and the need to secure permission from a sister agency to access a camera.

demonstrate how PBC determined whether the relevant repair was feasible. PBC also informed OIG that it treats eight hours as the equivalent of one day, but it has not formally documented this interpretation of the standard. Upon request, PBC produced e-mails and explanations demonstrating the vendor had not defaulted in any ofthe nine cases. OIG's review of a Motorola quarterly report found that while it met the requirements expressed in the task order, it miscalculated total repairs. Finally, OEMC and PBC both expressed the expectation that, under ordinary circumstances, a camera should be repaired within five days after a malfunction is discovered. However, PBC stated that it does not calculate average repair time or conduct any other analysis of Motorola's repair times. OIG also found that repairs for 255, or 77%, of 333 cameras classified as Severity 3 took longer than the informal goal of five days.[54]

PBC explained that it does not record a timestamp for "response time on site" or document whether a repair was feasible because it feels that its phone calls with the vendor adequately evaluate these aspects. Regarding the interpretation of the repair time standard, PBC explained that eight hours constitute one work day for a laborer, but also stated that Motorola should be held to the language in the task order. When OIG pointed out the miscalculation in the quarterly report, PBC stated that it manually creates its own internal tracking spreadsheet, and that it had not reconciled the data with the vendor's report to test the data's accuracy. When OIG asked PBC why it did not hold Motorola to deadlines for repairing cameras, PBC stated that there are numerous, valid reasons why a repair job might exceed the preferred five days, and, furthermore, that its IGA with OEMC does not require specific repair timelines.

The IGA requires PBC to "enforce the terms and conditions of the Program Agreement and avail itself ofthe rights and remedies in the Program Agreement and all other agreements pertaining to the Program, consistent with the requirements thereof in order to protect the best interests of the City and PBC." Interviews revealed that OEMC relied on PBC's expertise to ensure that all repairs and installations are completed correctly. In furtherance of these responsibilities, PBC demonstrated that Motorola has yet to default on a service level requirement and had provided all required deliverables. PBC believes that the deliverables, in conjunction with its additional oversight techniques, provide sufficient information to evaluate Motorola's performance as a maintenance vendor. While PBC evaluates Motorola's performance as required by the maintenance task order, it could implement minor adjustments to strengthen its oversight practices. These adjustments would allow management to review the vendor's compliance with service levels more easily, to prevent disputes with the vendor over the timeliness for feasible repairs, to assess the number of open and closed repairs in a quarter, and to determine if repairs were conducted in a timely manner. Because OEMC bears the responsibility for managing the public safety camera network, the Office should ensure protection of its assets by monitoring PBC's oversight of the vendor's performance.

Recommendation:

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

[4] OEMC stated that there was an informal expectation that cameras would be repaired in five days. PBC stated that this informal expectation applied to Severity 3 failures. Therefore, OIG limited its analysis of repair time to Severity 3 failures.

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.[55] 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.

Management Response:

"OEMC is currently exploring alternative program management arrangements for the public safety camera network. In the meantime, OEMC will work with PBC to improve contractor oversight.

"The PBC is committed to provide Project Management Services to OEMC PBC will continue to provide vendor oversight on all projects undertaken. PBC will provide the below to ensure vendor oversight:

- *All applicable task orders will specify applicable service level agreements (SLA). If the SLA changes, the PBC commits to denote the change in writing via task order.*
- *PBC will review and provide a written summary of issues / deficiencies related to the Vendor Monthly Report to OEMC This report will be provided no later than 6 weeks after receipt.*
- *PBC will provide monthly report to OEMC that houses the data from repairs. This report can be used by OEMC to produce any metrics the agency sees fit. (i.e. percentile measurements for repair timeliness and assessing vendor performance.)*
- *PBC will have OEMC review and sign a scope verification form to agree to the deliverable and service levels in various agreements that are described in the maintenance task order."*

Given the variability in repair times, mean and median measurements may not accurately describe camera repair data or allow PBC to see which repairs or cameras (if any) are outliers. By breaking the data into tiers, a percentile measurement would allow the Commission both to detect patterns in the data and to set realistic repair timelines, taking into account that unusual circumstances may justify some repair delays. PBC's informal five-day criterion does not take such a nuanced approach to the reality of the repair environment.

V. Appendix A: Location of Public Safety Cameras

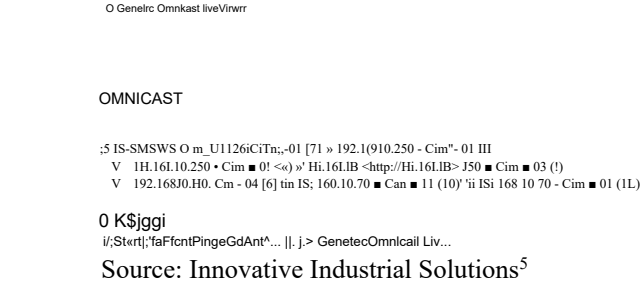
Source: OEMC's inventory of public safety cameras
Page 23 of 26

The map below illustrates the distribution of public safety cameras in Chicago. OIG created the map using ArcGIS software and OEMC's inventory of the approximately 2,700 public safety cameras. Each green dot represents one camera.

OIG File #14-0568
OEMC Public Safety Cameras Audit

VI. Appendix B: Genetec Security Center User View

The image below is an example of the Genetec Security Center application interface. A user can use the directional arrows on the left side of the display to PTZ the camera. Depending on the bandwidth ofthe terminal, a user can view up to four live camera feeds at once.



Source: Innovative Industrial Solutions[5]

"Genetec Omnicast IP Video Sur\'cillance System" Innovative Industrial Solutions, accessed September 23, 2016, hllp://wwvv.i-i-s.nct/?pagc id=833.

VII. Appendix C: Maintenance Task Order Service Levels and Deliverables

The service level and the deliverables enumerated in the current maintenance task order (number 893) are reproduced below. PBC uses the service level and deliverables to evaluate the vendor's performance and determine if the vendor owes any credits to the City.

Task Order 893 PBC/OEMC Camera Infrastructure Program

2016 Maintenance Program

On-Site Response Time Table (Customer's Response Time Classification is designated in the Service Agreement).

Severity Level	Response Time On Site	Off Deferral
Severity 1	Within 4 hours from receipt of Notification 24/7, Monday through Fridays and Holidays. When feasible' repair within 8 hours"	Time provided by Servicer .
Severity 2	Within 24 hours from receipt of Notification Standard Business Day. When feasicle' repair within 48 hours'*	Time provided by Servicer
Severity 3	Within 48 hours from receipt of Notification Standard Business Day	Time provided by Servicer

••"Feasible" repairs are those where spare parts are in-stock and available for immediate deployment into the field. Motorola will be responsible for recommending appropriate spare parts inventor)' levels and regularly reporting on the current inventory levels.

"Failure to meet the specified repair times for severity 1 and severity 2 issues will result in a S500 credit for severity 1 issues and $250 credit for severity 2 issues for each occurrence where the issue was not resolved in the specified repair time, subject lo the above definition ol'a feasible repair.

Source: Task Order 893, page 4

Task Order 893
2013 Maintenance Program

PBC/OEMC Camera Infrastructure Program

DELIVERABLES

- Preventative Maintenance
  - o Provide PBC PM schedule within two weeks of NTP.
  - c Provide checklist with each PM and includes: photos, time on-site and time off-site.
- Network Monitoring
  - o Provide weekly updates/status of network equipment.
- Software Maintenance - Genetec / Vidsys / GIS Mapping
  - o Provide weekly report of system outages (scheduled and non-scheduled). « System Manager
  - o Provide weekly executive reports to PBC/OEMC by Noon on Mondays, o Provide project-wide safety plan within two weeks of NTP o Provide Quarterly reports
- OVS - On-site Support Services
  - o Time sheets on a monthly basis
- OVS - Field Support Services
  - o Time sheets on a monthly basis
- Infrastructure Repairs
  - o Provide root cause analysis on all repairs o Provide Quarterly spares report
- Uptime / Downtime
  - o Provide monthly reports on uptime / downtime

SERVICES NOT INCLUDED UNDER MAINTENANCE OR WARRANTY

Services that are not described in this Task Order are not explicitly included, and will be performed at Motorola's discretion, Change Order to this Task Order, or via a subsequent Task Order.

Optional Services are noted in the pricing table and are not included in the total pricing of this task order.

INVENTORY SPARES

To comply with the agreed-upon Service Levels described in this Task Order, a spares inventory will be required for all applicable

equipment. On a monthly basis, Motorola will review inventory spare stock and make recommendations for replenishment to the PBC. PBC/OEMC is responsible for purchasing all spares.

Source: Task Order 893, page 20

City of Chicago Office of Inspector General

Public Inquiries	Rachel Leven (773) 478-0534 rlevenffljchicaeoinspectoreeneral.ore
To Suggest Ways to Improve City Government	Visit our website: <https://chicaeoinspectoreeneral.ore/get-involved/help-> imorove-citv-government/
To Report Fraud, Waste, and Abuse in City Programs	Call OIG's toll-free hotline 866-IG-TIPLINE (866-448-4754). Talk to an investigator from 8:30 a.m. to 5:00 p.m. Monday-Friday. Or visit our website: <http://chicaeoinspectoreeneral.ore/get-involved/fieht-> wastc-fraud-and-abuse/

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; audits of City programs and

operations; and - reviews of City programs, operations, and policies.

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 the provision of efficient, cost-effective government operations and further to prevent, detect, identify, expose and eliminate waste, inefficiency, misconduct, fraud, corruption, and abuse of public authority and resources.

Authority

The authority to produce reports and recommendations on ways to improve City operations is established in the City of

Chicago Municipal Code § 2-56-030(c), which confers upon the Inspector General the following power and duty:

> *To promote economy, efficiency, effectiveness and integrity in the administration of the programs and operations of the city government by reviewing programs, identifying any inefficiencies, waste and potential for misconduct therein, and recommending to the mayor and the city council policies and methods for the elimination of inefficiencies and waste, and the prevention of misconduct.*