

Poughkeepsie Housing Authority

Procurement and Information Technology Controls

FEBRUARY 2018



OFFICE OF THE NEW YORK STATE COMPTROLLER
Thomas P. DiNapoli, State Comptroller

Contents

- Report Highlights 1**

- Procurement 2**
 - How Should an Authority Procure Goods and Services? 2
 - Quotes Were Not Obtained in Accordance With Authority Policy 2
 - Competition Was Not Solicited For Professional Services. 3
 - The Procurement Policy Was Not Followed 3
 - What Do We Recommend? 4

- Information Technology 5**
 - How Should Authority Assets Be Safeguarded? 5
 - The Board Did Not Adopt Acceptable Use or Breach Notification Policies. 5
 - The Board Did Not Adopt a Disaster Recovery Plan. 6
 - Internet Use Is Not Monitored 6
 - The Server Is Not In a Secured Area 6
 - What Do We Recommend? 7

- Appendix A – Response From Authority Officials 8**

- Appendix B – Audit Methodology and Standards 9**

- Appendix C – Resources and Services. 11**

Report Highlights

Poughkeepsie Housing Authority

Audit Objectives

Determine whether Authority officials procured goods and services in accordance with the procurement policy and applicable statutes.

Determine whether Authority officials ensured that the Information Technology (IT) system was adequately secured and protected against unauthorized use, access and loss.

Key Findings

- During our audit period, Authority officials did not obtain quotes for public works projects totaling \$18,762 and purchases contracts totaling \$10,680 or solicit requests for proposals (RFPs) for professional services totaling \$26,754.
- Authority officials did not adopt comprehensive IT policies or a disaster recovery plan.

In addition, sensitive IT control weaknesses were communicated confidentially to Authority officials.

Key Recommendations

- Ensure that all required quotes are obtained.
- Adopt acceptable use and breach notification policies and a disaster recovery plan.
- Address the IT recommendations communicated confidentially.

Authority officials agreed with our recommendations and indicated they planned to initiate corrective action

Background

The Poughkeepsie Housing Authority (Authority) is located in the City of Poughkeepsie (City) in Dutchess County. The Authority was established in 1952, pursuant to title 34 section 437 of the Public Housing Law, to provide low-rent housing for qualified individuals.

The Authority is governed by a seven member Board of Commissioners (Board). The Mayor appoints five Commissioners and residents elect two Commissioners. The Board Chair is responsible for general supervision of Authority business activities.

The Board appoints an Executive Director, who is responsible for the management of five public housing buildings located throughout the City.

Quick Facts

2016-17 Expenditures	\$5.9 Million
Residents	1,200
Housing Units	359

Audit Period

April 1, 2016 – July 18, 2017

Procurement

How Should an Authority Procure Goods and Services?

General Municipal Law requires the Board to adopt written policies and procedures for the procurement of goods and services that are not subject to competitive bidding requirements in a manner to ensure the prudent and economical use of public money in the best interests of the residents. The Board should establish, implement and monitor such policies to help ensure that the Authority obtains goods and services at competitive prices and to protect against favoritism, extravagance, fraud and corruption.

The Board adopted a procurement policy and procedures that require quotes be obtained for supplies and equipment that are not required to be procured through competitive bidding. The policy requires three quotes (either written or verbal) for purchase contracts from \$2,000 to \$9,999 and public work contracts from \$2,000 to \$34,999. The policy also requires officials to maintain a list of qualified bidders for goods and services, at least annually.

Quotes Were Not Obtained in Accordance With Authority Policy

Authority officials did not adhere to the procurement policy regarding obtaining quotes for purchases and public works. We tested payments made to 15 vendors (12 public works and three purchase contracts) totaling \$82,950, from payments to 108 vendors totaling \$433,500 made during our audit period, to determine whether written or verbal quotes were obtained in accordance with the Authority's policy and found the following discrepancies:

- Payments to four public works contractors totaling approximately \$18,762 were made without seeking quotes.
- Payments for all three purchases totaling \$10,680 were made without seeking quotes.

Figure 1: Procurement Contracts

Type	Description	Total
Public Works	Auto Repair	\$8,249
	Plumbing Repair	\$2,185
	Security Camera Installation	\$8,328
	Total Public Works	\$18,762
Purchases	Appliances	\$5,526
	Rental Countertops	\$3,110
	Road Salt/ice melt	\$2,044
	Total Purchases	\$10,680
Totals		\$29,442

According to the Authority's accountant, officials did not always obtain bids and quotes for services because it is sometimes difficult to find vendors willing to work at Authority properties.

By not properly obtaining quotes in accordance with Authority policy, officials cannot be sure they are obtaining goods and services of the required quantity and quality at competitive prices.

Competition Was Not Solicited For Professional Services

Authority officials did not solicit RFPs as required by policy. We examined payments totaling \$177,654 made to six professional service providers during the audit period to determine whether they were selected through an RFP process. Authority officials did not obtain RFPs for three providers who were paid a total of \$26,754. Two of these providers, who were paid \$7,408, did not have written contracts with the Authority. The Authority's accountant told us that officials chose to retain providers who had previously performed work at the Authority and they did not have written contracts because the providers' bills were for small amounts.

Additionally, Authority officials did not have a current written contract with the painting contractor, who was paid \$99,600 during our audit period. The last painting contract covered 2010 through 2012, and officials did not renew this contract or enter into a new contract since its expiration. Authority officials have also not issued an RFP for this service since 2009. Furthermore, the contractor did not provide the statutorily required workers' compensation policy documentation. As a result, officials included the contractor on the Authority's workers' compensation policy. The Director told us they were soliciting RFPs for the painting service beginning in 2018.

When Authority officials do not seek competition when procuring professional services, they cannot assure residents that they are procuring the most economically beneficial and qualified service providers and that these procurements were not influenced by favoritism. In addition, without adequately written contracts, neither Authority officials nor the provider have a clear way to determine the basis for or entitlement to payment for the work performed.

The Procurement Policy Was Not Followed

Authority officials did not maintain a qualified bidders list as required by the procurement policy. The accountant told us that he did not know the policy required a qualified bidders list.

By not properly seeking full and open competition in all procurement transactions in compliance with policy, Authority officials cannot be sure they are obtaining goods and services of the required quantity and quality at competitive prices.

What Do We Recommend?

Authority Officials should:

1. Ensure all necessary quotes are obtained as required by the Authority's policy for items not required to be competitively bid.
2. Ensure the RFP process is used to select professional services, and maintain proper documentation for future needs.
3. Ensure all professional service providers have a current written contract stipulating services to be performed, amounts to be paid and applicable insurance documentation.
4. Maintain a qualified bidders list for goods and services as prescribed in the procurement policy.

Information Technology

How Should Authority Assets Be Safeguarded?

Computers are an integral part of Authority financial and network systems. An effective process for safeguarding Authority computer assets includes an acceptable computer use policy, which defines the procedures for computer, Internet and email use and holds users accountable for properly using and protecting Authority resources. In addition, New York State Technology Law requires the Authority to establish an information breach notification policy. Such a policy should detail how the Authority would notify individuals whose private information was, or is reasonably believed to have been, acquired by a person without a valid authorization.

Effective internal controls also include adopting a disaster recovery plan to help prevent the loss of computer equipment and data, and provide procedures for recovery in the event of a loss. The plan should include the precautions to be taken to minimize the effects of a disaster so that Authority officials can either maintain or quickly resume mission-critical functions. The plan may also include a focus on disaster prevention.

While using the Internet is a nearly indispensable resource for conducting business, users are susceptible to significant threats from cybercriminals who exploit the vulnerabilities of IT systems to gain unauthorized access to sensitive data. Internet browsing increases the likelihood that users will be exposed to some form of malicious software that may compromise data confidentiality. Authority officials should ensure there is an adequate web filtering process in place to limit vulnerabilities in its IT systems from Internet browsing and ensure the Authority's network is used for appropriate purposes.

Authority officials can reduce the risks to sensitive data and IT assets by monitoring Internet use and using web filtering software to block access to unacceptable websites. In addition, physical security over computerized assets is an important component of overall computer and data security, such as locked doors to prevent unauthorized persons from entering the server room, adequate ventilation and an uninterrupted source of power. If the server room is compromised or there is a power outage, there is an increased security risk to the Authority's IT resources and data, including confidential information.

The Board Did Not Adopt Acceptable Use or Breach Notification Policies

Authority officials do not have a computer use policy that addresses the terms and conditions for acceptable network, Internet and email use. Because the Board did not adopt such a policy to set the standards and expectations for the responsible use of computer resources, there is an increased risk that resources could be misused or that data could be lost or corrupted. In addition, the Board has not

developed and adopted a breach notification policy. Without this policy, Authority officials may not be able to notify individuals in a timely manner in the event that their private information was accessed.

The Board Did Not Adopt a Disaster Recovery Plan

The Board and Authority officials did not develop a disaster recovery plan because they were unaware they needed to prepare for recovery in the event of a loss. Therefore, in the event of a disaster, Authority personnel have no guidelines or plan to follow to prevent the loss of equipment and data or procedures for data recovery. The lack of a disaster recovery plan could lead to the loss of important financial data and serious interruptions to Authority operations, such as not being able to process checks to pay vendors or employees, should a disaster occur.

Internet Use Is Not Monitored

We examined all 12 computers and identified questionable Internet use by Authority employees on seven computers connected to the Authority's network. Authority employees used these computers to visit social networking, email, online banking, shopping, travel, entertainment and blogging websites, and performed other Internet research and browsing of a personal nature, such as how to pass drug tests. We also identified computers that were used to research malware, spyware and other potential security threats while using accounts with administrative privileges.

This occurred because the Board did not adopt an acceptable use policy outlining proper use of Authority computers and there are no web filters. In addition, employees were not provided security awareness training to inform them of the risks of inappropriate Internet use. The IT consultant told us that he is willing to make any changes that Authority officials require from him, but he was never provided with any guidance or requirement. Because these types of websites are commonly used to spread malware, such Internet use unnecessarily exposes the Authority's systems to malware infections.

The Server Is Not In a Secured Area

The Authority's server is not located in a secure area. Instead, it is located in a room without a door in an area accessible to many employees and visitors, leaving the server unsecured. During the audit, we observed that employees usually lock their office doors when at lunch and leave the server room accessible to anyone in the area.

If access to the server is not controlled, the risk increases that unauthorized access to the network could be obtained and the server could be damaged. This

weakness leaves the Authority vulnerable to the manipulation or loss of data with potentially costly consequences.

What Do We Recommend?

The Board should:

5. Adopt an acceptable use policy that defines both acceptable and unacceptable activities when using the Authority's computers, limiting the use of such assets to business purposes.
6. Adopt a breach notification policy that details how the Authority would notify individuals whose private information was, or is reasonably believed to have been, acquired by a person without a valid authorization.
7. Adopt a comprehensive disaster recovery plan that details specific guidelines for the protection of equipment and private essential data against damage, loss or destruction.
8. Ensure all network users receive IT security awareness training and that the training is updated whenever the IT policy is updated, including a discussion of the risks of inappropriate Internet use.
9. Secure the Authority's server room so that only authorized individuals have access.

Appendix A: Response From Authority Officials

(845) 485-8862



Fax: (845) 485-2630

POUGHKEEPSIE

Housing Authority

4 Howard Street
Poughkeepsie, NY 12601

January 31, 2018

Office of the State Comptroller
Division of Local Government and School Accountability
Newburgh Regional Office
33 Airport Center Drive, Suite 103
New Windsor, NY 12553

RE: Poughkeepsie Housing Authority
Procurement and Information Technology Controls
Report of Examination 2017M-222

Dear Chief Examiner Tenneh Blamah,

The Poughkeepsie Housing Authority has reviewed the draft audit report sent to our offices on January 4, 2018. The Board of Commissioners and I appreciate the time and effort your office has invested in supporting the work we do by offering guidance on areas needing improvement such as Procurement and Technology Controls. In general, we agree with the audit and have started working on making changes which includes developing new policies. We will be submitting a corrective action plan within the 90 days of the final report.

Our administration and board recognizes that there is always room for improvement. We will always try to employ the best practices and to continue to develop and train staff. We continue to strive to work at the highest level of professionalism in our field with all the resources that are at our disposal.

Respectfully,

Nancy R. Dotterer
Executive Director

Appendix B: Audit Methodology and Standards

We conducted this audit pursuant to Article V, Section 1 of the State Constitution and the State Comptroller's authority as set forth in Article 3 of the New York State General Municipal Law. To achieve the audit objectives and obtain valid audit evidence, we performed the following audit procedures.

Procurement:

- We interviewed Authority officials to gain an understanding of the Authority's policies and procedures used to procure goods and services.
- We judgmentally selected six professional service providers based on type of service and total amount paid to the provider during the audit period. We reviewed the Board's procurement policy and documentation related to requests for proposals for our sample to assess whether officials sought competition when obtaining these services and determine whether the Board entered into written contracts with these providers.
- We judgmentally selected 15 vendors that were below the bidding threshold based on type of vendor and total amount paid to the vendor, from 108 vendor payments totaling \$433,500 made during the audit period that required quotes based on the Authority's policy. We reviewed bid documents and quotes for our sample to evaluate whether the Board procured goods and services using a competitive method in accordance with Authority policy.

Information Technology:

- We interviewed Authority officials to obtain an understanding of the Authority's IT operations.
- We made inquiries of officials to determine the adopted policies and procedures related to acceptable computer use, data backups, disaster recovery plans, breach notifications, security awareness training and server locations.
- We examined all twelve Authority computers by running audit software and examined specific activities such as user Internet use and web browsing history.

Our audit also examined the adequacy of certain information technology controls. Because of the sensitivity of some of this information, we did not discuss the results in this report, but instead communicated them confidentially to Authority officials.

We conducted this performance audit in accordance with GAGAS (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 our findings and conclusions based on our audit objective.

We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Unless otherwise indicated in this report, samples for testing were selected based on professional judgment, as it was not the intent to project the results onto the entire population. Where applicable, information is presented concerning the value and/or the relevant population size and the sample selected for examination.

Good management practices dictate that the Board has the responsibility to initiate corrective action. As such, the Board should prepare a plan of action that addresses the recommendations in this report and forward the plan to our office within 90 days.

Appendix C: Resources and Services

Regional Office Directory

www.osc.state.ny.us/localgov/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas

www.osc.state.ny.us/localgov/costsavings/index.htm

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems

www.osc.state.ny.us/localgov/fiscalmonitoring/index.htm

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management

www.osc.state.ny.us/localgov/pubs/listacctg.htm#lgmg

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans

www.osc.state.ny.us/localgov/planbudget/index.htm

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders

www.osc.state.ny.us/localgov/lgli/pdf/cybersecurityguide.pdf

Required Reporting – Information and resources for reports and forms that are filed with the Office of the State Comptroller

www.osc.state.ny.us/localgov/finreporting/index.htm

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers

www.osc.state.ny.us/localgov/researchpubs/index.htm

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics

www.osc.state.ny.us/localgov/academy/index.htm

Contact

Office of the New York State Comptroller
Division of Local Government and School Accountability
110 State Street, 12th Floor, Albany, New York 12236

Tel: (518) 474-4037 • Fax: (518) 486-6479 • Email: localgov@osc.state.ny.us

www.osc.state.ny.us/localgov/index.htm

Local Government and School Accountability Help Line: (866) 321-8503

NEWBURGH REGIONAL OFFICE – Tenneh Blamah, Chief Examiner

33 Airport Center Drive, Suite 103 • New Windsor, New York 12553-4725

Tel (845) 567-0858 • Fax (845) 567-0080 • Email: Muni-Newburgh@osc.state.ny.us

Serving: Columbia, Dutchess, Greene, Orange, Putnam, Rockland, Ulster, Westchester counties



Like us on Facebook at facebook.com/nyscomptroller

Follow us on Twitter [@nyscomptroller](https://twitter.com/nyscomptroller)