REPORT OF EXAMINATION | 2019M-224

Hudson Housing Authority

Information Technology

JULY 2020

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

Contents

Report Highlights

Hudson Housing Authority

Audit Objective

Determine whether Authority officials ensured IT systems were adequately secured and protected against unauthorized use, access and loss.

Key Findings

- The Board did not adopt an acceptable use policy.
- Officials did not provide IT security awareness training.
- The Authority did not have adequate online banking agreements.

Sensitive information technology (IT) control weaknesses were communicated confidentially to officials.

Key Recommendations

- Adopt comprehensive IT policies, communicate them to all employees, review and update routinely or when significant changes in the environment occur.
- Create and maintain service level agreements (SLAs) for any IT services provided by third-party vendors.
- Consider requiring employees to sign acknowledgement forms to help ensure they are aware of adopted policies and procedures and understand what is expected of them.

Authority officials agreed with our findings and recommendations and indicated they will take corrective action.

Background

Hudson Housing Authority (Authority) is located in the City of Hudson in Columbia County. The Authority is governed by a seven member Board of Commissioners, five appointed by the City Mayor and two elected by the tenants.

The Board is responsible for hiring an Executive Director who is responsible for the general management, supervision and direction of day-to-day operations.

The Authority provides affordable, quality housing to low-income individuals and families. To provide this service, the Authority collects sensitive personal information. The Authority uses a variety of electronic data and computer resources to manage its daily operations.

Quick Facts	
IT Service Providers	2
Employees	9
2019 Appropriations	$1.09 million
User Accounts[a]	11
Desktop Computers[a]	6

a Identified accounts and computers used for day-to-day operations

Audit Period

July 1, 2017 – July 25, 2019. We extended our audit period forward through September 12, 2019 to review IT systems.

Information Technology

The Authority relies on its IT system to perform a variety of tasks, including providing Internet access, protecting personal, private and sensitive information (PPSI),[1] email communication and maintaining financial records. If the IT system is compromised, the results could range from an inconvenience to a catastrophe and could require extensive effort and resources to evaluate and repair. The Authority pays an IT service provider who offers consulting and support services for product and software acquisitions, network design and computer maintenance.

How Does an Acceptable Use Policy Secure the Authority's IT System?

An acceptable use policy (AUP) describes what constitutes appropriate and inappropriate use of IT resources, along with the board's expectations concerning personal use of IT equipment and user privacy.[2] Monitoring compliance with the AUP involves regularly collecting, reviewing and analyzing system activity for indications of inappropriate or unusual activity and investigating and reporting such activity. The AUP should also include details on how an employee may be disciplined for violations.

Officials should monitor and analyze activities for signs of possible violations and activities that threaten computer security. Internet browsing increases the likelihood that users will be exposed to malware that may compromise data confidentiality, integrity or availability. Officials can reduce the risks to personal, private and sensitive information (PPSI) and IT assets by monitoring Internet usage.

The Board Did Not Adopt an Acceptable Use Policy

The Board did not adopt an acceptable use policy governing appropriate and inappropriate use of Authority IT resources. We examined the web history of six computers used in day-to-day operations and did not identify any significant concerns. However, without an acceptable use policy, the Authority is placing its assets and data at greater risk. Employees may be unaware of potential security threats the Authority is exposed to with inappropriate Internet usage.

Officials told us that they had not considered the importance of implementing such a policy before we began our audit. However, as a result of not having such a policy, employees may unknowingly engage in inappropriate computer use, or officials may not detect inappropriate use, leaving Authority IT assets (and any

1 Personal, private and sensitive information (PPSI) is any information to which unauthorized access, disclosure, modification, destruction or use – or disruption of access or use – could have a severe impact on critical functions, employees, customers, third parties or other individuals or entities.

2 For example, management may reserve the right to examine email, personal file directories, web access and other information stored on computers, at any time and without notice.

PPSI contained on those assets) at a higher risk of exposure to misuse, loss, and fraud.

Why Should the Authority Have a Breach Notification Policy?

New York State Technology Law[3] requires municipalities and other local agencies to have a breach notification policy or local law that requires notification be given to certain individuals in the event of a system security breach, as it relates to private information. The policy should detail how officials would notify individuals whose private information was, or is reasonably believed to have been, acquired without valid authorization.

The disclosure should be made in the most expedient time possible consistent with legitimate needs of law enforcement or any measure necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Private information includes social security numbers, bank account numbers, healthcare information, credit and debit card numbers and driver's license information.

The Board Did Not Adopt a Breach Notification Policy

The Board did not adopt a breach notification policy. Authority officials told us that they were unaware of the legal requirement to adopt a breach notification policy. However, without a breach notification policy, the Authority may not be able to fulfill its legal obligation to notify affected individuals if sensitive information is compromised and to inform those individuals of the need to monitor credit reports and bank activity.

Why Should the Authority Have a Disaster Recovery Plan?

The Board should adopt a disaster recovery plan to describe how Authority officials will deal with potential disasters that affect the IT system. A disaster recovery plan provides a framework for reconstructing vital operations to resume time-sensitive operations and services after a disaster. Disasters could include any sudden, unplanned catastrophic event (e.g., fire, computer virus or inadvertent employee action) that compromises the availability or integrity of the IT system. This is particularly important given the current and growing threat of ransomware attacks that could compromise the network and the availability or integrity of the financial system and any PPSI contained therein.

Typically, a disaster recovery plan includes an analysis of business processes and continuity needs, disaster prevention instructions, specific roles of key individuals

3 New York State Technology Law, Section IT 208

and precautions needed to maintain or quickly resume operations. Additionally, such a plan should include data backup procedures, such as ensuring a backup is stored off-site in case the building is destroyed or inaccessible, and periodic backup testing to ensure backups will function as expected.

Officials Did Not Have a Disaster Recovery Plan

Authority officials did not create a disaster recovery plan to address potential disasters. Consequently, in the event of a disaster, officials have no guidelines or guidance to minimize or prevent the loss of equipment and data. Officials have not identified, documented and prioritized essential systems and data, which increases potential losses, business and systems downtime and the potential overall cost. Officials told us that they were unaware of IT best practices, which include the creation of a disaster recovery plan.

Without a formal written disaster recovery plan, the Authority could lose important financial and other data and suffer serious interruption to operations, such as not being able to pay vendors or employees or determine the status of rental payments receivable.

Why Should Authority Officials Provide IT Security Awareness Training?

To minimize the risk of unauthorized access and misuse or loss of data and PPSI, authority officials should provide periodic IT security awareness training that explains the proper rules of behavior for using the Internet and IT systems and data and communicates related policies and procedures to all employees.

The training should center on emerging trends such as information theft, social engineering attacks[4] and computer viruses and other types of malicious software, all of which may result in PPSI compromise or expose the authority to ransomware attacks. Additionally, authority officials should develop and also communicate written procedures for collecting, storing, classifying, accessing, protecting and disposing of PPSI.

Training programs should be directed at the specific audience (e.g., system users or administrators). The training should also cover key security concepts such as the dangers of Internet browsing and downloading files and programs from the Internet, requirements related to protecting PPSI and how to respond if an information security breach is detected.

4 Social engineering attacks are methods used to deceive users into revealing PPSI and other confidential or sensitive information.

Officials Did Not Provide IT Security Awareness Training

Officials did not provide users with IT security awareness training to help ensure they understand IT security measures and their role in protecting Authority assets. We interviewed all employees during audit testing to determine whether they received or were offered IT security awareness training and found that none of them received (or were offered) such training.

Officials told us that they did not consider the importance of offering such training. However, without IT security awareness training, users may not understand their responsibilities and are more likely to be unaware of a situation that could compromise IT assets. As a result, data and PPSI could be at greater risk for unauthorized access, misuse or loss.

What Should Be Included in an IT Service Provider Contract?

A written agreement between the Authority and its IT service provider provides both parties with a clear understanding of the services expected to be provided and a legal basis for compensation provided for those services. The Board should have a formal written contract with its IT provider that specifies the contract period, services to be provided and basis of compensation for those services.

In addition, to protect the Authority and avoid potential misunderstandings, officials should have a written service level agreement (SLA) between the Authority and its IT consultant that identifies the Authority's needs and expectations and specifies the level of service to be provided by the IT consultant.

An SLA differs from a traditional written contract in that it establishes comprehensive, measureable performance targets so that there is a mutual understanding of the nature and required level of services to be provided. It provides detailed explanations of the services to be performed by identifying the parties to the contract and defining terminology; duration of the agreement; scope and/or subject limitations; service level objectives and performance indicators; roles and responsibilities; nonperformance impact; security and audit procedures; reporting requirements; review, update and approval process; pricing, billing and terms of payment.

Officials Did Not Have Written Contracts or SLAs With IT Service Providers

The Authority did not have SLAs for IT services. The Board did not negotiate written contracts with its IT service providers and officials did not enter into SLAs with these providers to identify the specific services to be provided or the providers responsibilities. Authority officials told us that they did not have SLAs because they had not considered the benefits of having such agreements.

As a result, in the event of any failure in IT controls (such as a breach), by either the Authority or the vendor, the lack of a specific service level agreement can contribute to confusion over who is responsible for the various IT environment aspects, which ultimately puts the Authority's data and computer resources at greater risk for unauthorized access, misuse, or loss. In addition, the Authority may suffer a significant monetary loss and a loss of public trust and confidence.

What Are Effective Online Banking Controls?

Online banking provides a means of direct access to funds held in bank accounts. Users can review current account balances and account information, including recent transactions, and transfer money between bank accounts and to external accounts. Because funds transferred electronically typically involve significant amounts of money, officials must control the processing of its electronic transfers to help prevent unauthorized transfers from occurring. It is essential that officials provide authorization of transfers before they are initiated and establish procedures to ensure that staff are securely accessing banking websites to help reduce the risk of unauthorized transfers from both internal and external sources.

New York State General Municipal Law (GML) allows authorities to disburse or transfer funds in their custody by means of electronic transfers, provided that the governing board has entered into a written agreement with the bank.[5] GML requires that this agreement prescribe the manner in which electronic transfers will be accomplished and identify the names and numbers of bank accounts from which such transfers may be made and the individuals authorized to request transfers.

GML also requires an authority to implement a security procedure that includes verifying that a payment order is for the initiating authority and detecting payment order errors in transmission or content. An employee should not be able to execute an electronic transfer without obtaining authorization from the custodial officer or a deputy.

Authorities should also check with their banks about enabling alerts and other security measures that may be available such as blocking wire transfers to foreign countries, email notifications and requiring the verification of transactions over certain amounts, possibly through callbacks.

Officials Did Not Have Adequate Banking Agreements

Officials used two banks for online banking transactions, which included capabilities such as electronic deposits, internal account transfers and electronic

5 New York State General Municipal Law, Article 2, Sections 5-A and 10

withdrawals. We found that officials did not have an agreement with the banks with which the Authority conducted business. As a result, the Authority did not have an agreement that included the following:

- The manner in which electronic or wire transfers of funds would be accomplished
- The names and the numbers of bank accounts from which electronic or wire transfers may be made
- The individuals authorized to request an electronic or wire transfers
- A procedure (or procedures) for verifying that a payment order is that of the Authority

Officials were unaware they were required to have online banking agreements in accordance with GML. However, without adequate online banking agreements or security controls, officials cannot be assured that funds are adequately safeguarded when performing online bank transactions.

As a result of these weaknesses in controls over the IT system, the Authority is at risk of PPSI compromises, ransomware attacks or inappropriate banking transfers. Some of these weaknesses, when combined, compound these risks. For example, not having a policy to limit Internet use coupled with the lack of training and a contract detailing the security procedures to be provided by service providers could expose the Authority IT system to intrusion attacks. Fortunately, these weaknesses can be resolved and IT system security improved with minimal cost.

What Do We Recommend?

The Board should:

1. Adopt comprehensive IT policies that address acceptable use and communicate all adopted IT policies to officials and employees. Review and update IT policies routinely (at least once per year) or when significant changes occur in the IT environment to keep them in line with changes in technology and communicate all adopted IT policies to officials and personnel.
2. Adopt comprehensive IT policies including a breach notification policy.
3. Consider requiring employees to sign acknowledgement forms to help ensure they are aware of adopted policies and procedures and understand what is expected of them.

Authority officials should:

4. Develop and test a disaster recovery plan that identifies key personnel and test the plan to ensure it works as intended.
5. Ensure that employees receive formal IT security awareness training on an on-going basis that reflects current risk identified by the IT community.
6. Create and maintain SLAs for any IT services provided by IT service providers to ensure the understanding of all services being provided and the roles and responsibilities of all parties is defined and agreed upon.
7. Ensure that sufficient written banking agreements that address online banking with each bank are in accordance with GML, and that those who perform online banking transactions are familiar with its content.

Appendix A: Response From Authority Officials

HUDSON HOUSING AUTHORITY
41 North Second Street, Hudson, NY 12534 HUD NY61-1
Ph (518) 828-5415 Fax (518) 828-2591
**Proud, Progressive, Concern*

June 25, 2020

Lisa Reynolds
Office of the State Comptroller
Chief Examiner
Local Government and School Accountability
110 State Street
Albany New York 12236

Dear Ms. Reynolds,

Thank you for the friendly reminder regarding the housing authority's response to the draft audit report. I have read the draft report and submit no objections to the State's findings or recommendations. Please let this letter serve as my response that the housing authority will institute the recommendations of the State on or before December 31, 2020.

Sincerely,

Timothy M. Mattice
Executive Director
Hudson Housing Authority

cc:
Randel Martin, Board President
Rebecca Wolff, Board Member
Robert Davis, Board Member
Marie Balle, Board Member
Edrick Brown, Board Member
Tricia Mayo, Administrative Assistant

Appendix B: Audit Methodology and Standards

We conducted this audit pursuant to the State Comptroller's authority as set forth in Article X, Section 5 of the State Constitution. To achieve the audit objective and obtain valid audit evidence, our audit procedures included the following:

- We reviewed Board minutes for resolutions concerning IT matters and reviewed written Board policies to determine the number and scope of policies officially adopted.
- We interviewed Authority officials and employees to obtain an understanding of IT operations.
- We reviewed Authority records for any IT-related policies and procedures.
- We performed a walk-through throughout the Authority to identify any weaknesses in the physical security controls over IT systems and devices and to obtain an understanding of the system's and their functionalities.
- We ran a specialized shared folders audit script on each of the six Authority computers that were used for day-to-day operations. We analyzed the report generated to identify any folders that could potentially contain PPSI. We then determined who had access to those folders and inquired with officials to determine whether that access was necessary.
- We reviewed Authority computers and inquired with employees to determine who had access to PPSI.
- We interviewed Authority employees to determine what safeguards were in place to protect sensitive data and financial assets.
- We reviewed web history reports for the six Authority computers, used in day-to-day operations, to determine whether they were used to access websites that could put the network at risk.
- We examined the six Authority computers and the accounts used to access them for day-to-day operations to identify weaknesses in user account management, password management and access controls.
- We ran a specialized audit script on the six Authority computers used in day-to-day operations to identify internally accessible services.

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 objective.

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 size of the relevant population 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 written corrective action plan (CAP) that addresses the recommendations in this report and forward the plan to our office within 90 days.

For more information on preparing and filing your CAP, please refer to our brochure, *Responding to an OSC Audit Report*, which you received with the draft audit report. We encourage the Board to make the CAP available for public review.

Appendix C: Resources and Services

Regional Office Directory
www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2018-12/regional_directory.pdf

Cost-Saving Ideas – Resources, advice and assistance on cost-saving ideas
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263196&issued=All

Fiscal Stress Monitoring – Resources for local government officials experiencing fiscal problems
www.osc.state.ny.us/local-government/fiscal-monitoring

Local Government Management Guides – Series of publications that include technical information and suggested practices for local government management
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263206&issued=All

Planning and Budgeting Guides – Resources for developing multiyear financial, capital, strategic and other plans
www.osc.state.ny.us/local-government/resources/planning-resources

Protecting Sensitive Data and Other Local Government Assets – A non-technical cybersecurity guide for local government leaders
www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2020-05/cyber-security-guide.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/local-government/required-reporting

Research Reports/Publications – Reports on major policy issues facing local governments and State policy-makers
www.osc.state.ny.us/local-government/publications?title=&body_value=&field_topics_target_id=263211&issued=All

Training – Resources for local government officials on in-person and online training opportunities on a wide range of topics
www.osc.state.ny.us/local-government/academy

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.ny.gov

www.osc.state.ny.us/local-government

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

NEWBURGH REGIONAL OFFICE – Lisa A. Reynolds, 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.ny.gov

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

Like us on Facebook at facebook.com/nyscomptroller
Follow us on Twitter @nyscomptroller