CHA
CHICAGO HOUSING AUTHORITY

ADVISORY #9
Office of the Inspector General
Confidential

TO: Eugene Jones, CEO
James Bebley, Chief Legal Officer
Patricia Rios, Chief Administrative Officer

From: Elissa Rhee-Lee, Inspector General

Date: March 15, 2017

Subject: Recommendation for Employment Action against [redacted]

Facts:

[redacted] is a CHA employee working for the Department of Procurement and Contracts (DPC) as a Procurement Associate. [redacted] has been a CHA employee since January 11, 2016. During the time that [redacted] was under consideration for the CHA position with DPC, [redacted] was the subject of a criminal theft investigation by the Chicago City Colleges Office of the Inspector General (CCC OIG). [redacted] had knowledge of the CCC OIG investigation when she accepted the job offer from CHA in December 2015, just a few days prior to her resignation from CCC on December 24, 2015. The criminal investigation against [redacted] was sustained in early 2016 and subsequently the investigation was referred for prosecution to the Cook County States' Attorney's Office, Public Integrity Unit for review. The CCC also placed [redacted] on a 'do not rehire' list permanently.

The CCC OIG determined that [redacted] engaged in conduct unbecoming of a public employee in violation of the CCC Employee Manual and the Illinois Compiled Statute. Specifically, [redacted] engaged in conduct in 2014 and 2015 prohibited by the Illinois Compiled Statutes in that she committed the offense of theft, contrary to 720ILCS 5/16-1 and Official Misconduct, 720ILCS 5/33-3. The investigation revealed that

Chicago Housing Authority
60 E. Van Buren
12th Floor
Chicago, IL 60605
o 312-742-8500
www.thecha.org

[redacted] failed to process at least $2,980 and failed to deposit at least $3,125 in funds that she received as a result of transactions she completed in her capacity as a Bursar Assistant on behalf of Olive-Harvey College. The funds she misappropriated for her personal benefit included but were not limited to, student exam fees and student transcript request fees.

[redacted] was indicted by the Cook County Grand Jury in the fall of 2016 for theft and official misconduct (offense charged against public employees) under docket number 16-CR-1673601. The theft charges were enhanced because she was a public employee and the theft was against a government agency.

[redacted] withdrew her previous entered plea of not guilty and entered a plea of guilty to a Class 2 felony offense of theft in the Circuit Court of Cook County on January 4, 2017 before Honorable Judge James Linn. [redacted] had 30 days from January 4, 2017 to withdraw her plea of guilty. [redacted] no longer can withdraw her plea. Her sentencing is scheduled for April 4, 2017. It is anticipated that her sentence will include restitution for the money she misappropriated and some length of probation.

How the CHA OIG became aware of [redacted] Investigation:

My office learned about [redacted] last summer when I received a call from John Gasiorowski, the Inspector General for CCC. He inadvertently saw her name on the public website for public employee salaries that is posted annually by the Better Government Association (BGA).

Public and private employers can take disciplinary actions against an employee (including termination) if the criminal conviction relates to an offense involving truth, veracity and integrity even though the crime was not committed against the current employer.

Recommendations:

[redacted] should receive the highest level of employment action with strong consideration of terminating her employment and to be placed on a 'do not rehire' list for the following reasons:

- [redacted] was a public employee who impugned the integrity of public service

- The Class 2 felony conviction involved an offense of dishonesty, lack of integrity, and abuse of trust in the administration of government programs
- [redacted] currently works for a department that is tasked with confidential vendor information and sensitive procurement activities that can be compromised

It is also recommended that the CHA Employee Handbook be updated to require all employees to affirmatively notify CHA HR if he/she has been arrested and/or indicted of a crime. This matter was brought to the OIG's attention by chance only. If CHA required affirmative notification (like many other sister agencies), CHA has a better opportunity of reviewing the nature of the offense and consider what the appropriate action should be to protect the best interest of CHA.

CHA
CHICAGO HOUSING AUTHORITY

ADVISORY #10
Office of the Inspector General
Confidential

TO: Eugene Jones, Chief Executive Officer

CC: Dionna Brookens, Chief Procurement Officer
Kathryn Ludwig, Chief Housing Choice Voucher Officer
Derek Messier, Chief Property Officer
James Bebley, Chief Legal Officer

From: Elissa Rhee-Lee, Inspector General
Ashley Lindemann, Information Analyst

Date: November 6, 2017

Subject: P.O. Box Analytics and Recommendation

Addresses are a critical data field when searching for shell companies, fictitious vendors or identifying potential landlord/tenant collusion. Specifically, previous OIG criminal investigations provide evidence that the use of a post office box (P.O. Box) as one's identified address can be a red flag of potential fraud.

For example, the OIG found that a landlord may use a P.O. Box to conceal his or her relationship with a tenant and reside jointly in the subsidized unit. If a landlord's last name is different than a tenant's and their address reflects a P.O. Box, it is less apparent that the tenant and landlord are related and living in the same unit. The OIG has also seen cases where the landlord used a P.O. Box, which according to the USPS application, was originally registered to the tenant. There are approximately 1,300 CHA landlords who use a P.O. Box[1] as an address.

The use of a P.O. Box by contractors, subcontractors or vendors can also be a warning sign for potential fraud. Although it is common to identify a P.O. Box as one's address, it is less common for that to be the only address on record. For example, a fraudster may submit a phony invoice for consulting services and have a P.O. Box remittance address rather than a street address. Since services are not tangible, it is difficult to verify that the consulting services were rendered and that the company actually exists. A company may also subcontract with

[1] Data pulled from Yardi as of October 2017.

Chicago Housing Authority
60 E. Van Buren
12th Floor
Chicago, IL 60605
o 312-742-8500
www.thecha.org

third-party vendors so that the services are provided, but never pay or make nominal payments to those subcontractors.

Another scheme that the OIG has investigated involved three companies who were doing a significant amount of work for the CHA. It was determined that they were separate entities in name only, shared a P.O. Box address, and were controlled by members of the same extended family. They shared bidding information and worked collaboratively to obtain business with the CHA. There are over 200 active vendors in Yardi and 1,050 vendors in Lawson with a P.O. Box address only.

In sum, the legitimacy of a vendor is decreased when they have no physical, geographical location for their business or operation. Numerous state and federal statutes require a business entity list a physical mailing address. In Illinois, the Limited Liability Act states that neither a P.O. Box nor a c/o address is acceptable as the address of the principal place of business, or the office address of the registered agent.

To enhance accountability and transparency, the OIG recommends that landlords, contractors, subcontractors and vendors provide the CHA with an additional physical address if a P.O. Box is the only address on record. Taking this step will hold business owners accountable, lessen the amount of additional scrutiny needed when verifying a new vendor, and help guard against vendor fraud.

CONFIDENTIAL

Office of the Inspector General
Advisory #11

TO: Eugene Jones, Chief Executive Officer
CC: Kathryn Ludwig, Chief Housing Choice Voucher Officer
Derek Messier, Chief Property Officer

FROM: Elissa Rhee-Lee, Inspector General
Beatriz Martinez, OIG Senior Auditor

DATE: November 29, 2017

SUBJECT: **Lead Inspection Process – HCV and Public Housing**

In April 2017 Regional 5 HUD CHA OIG contacted the OIG to discuss various hot issues related to lead in Housing Authorities. They also advised us that HUD OIG Audit section was or will commence a "massive" audit on this topic. The CHA OIG decided to review the lead testing protocol for Housing Choice Voucher (HCV) and Public Housing. While CHA is compliant with current HUD regulations pertaining to lead testing we anticipate significant changes in the near future.

Housing Choice Voucher (HCV)

Policy

Administrative Plan - HUD requires that all units occupied by families receiving HCV assistance meet HUD's Housing Quality Standards (HQS) and permits the Public Housing Agency (PHA) to establish additional requirements. The use of the term Housing Quality Standards (HQS) in this plan refers to the combination of both HUD and PHA-established requirements. HQS inspections are required before the Housing Assistance Payments (HAP) Contract is signed and at least annually during the term of the contract.

Operations

The Chicago Housing Authority (CHA) performs HCV inspections by following the HQS Inspections (visual only) by:

- CVR contracts out the inspection process
  - 3rd party vendor (Naro)
    - Regular Inspectors – Certified
    - QC Inspectors – Certified
- CHA HCV QC Inspectors – Certified (NMA)

Reporting for HCV Operations

HCV sends (on a quarterly basis) the Chicago Department of Public Health (CDPH) HCV addresses with children under the age of 6. The Illinois Department of Public Health report to the CDPH cases where children under the age of 6 tested positive for lead. The City of Chicago will then inspect the residence of those children with lead. If the address for a failed inspection matches the CHA HCV list, a "Match Address" report is sent to HCV. HCV will mail a letter to the landlord demanding to "reduce the lead-based paint hazard". (Attachment 1)

Housing Choice Voucher (continued)

Families with child under 6 years as of 4/18/17

- 8,581

Total HCV Families 47,167

Reported fail inspection from CDPH (source: HCV Program Integrity)

1Q2016 – 36 3Q2016 – 15 1Q2017 – 12

Risk

- CHA's current HQS Inspection process is not capturing all lead violations.
- CDPH delay in notifying CHA, which may reach up to 6 months, leaving families exposed to possible lead poison
- House families in a toxic hazardous environment that can lead to permanent and/or long-term harm.

Recommendations

- CHA should require HCV landlords to pass a lead risk assessment inspection for all occupied units in the HCV portfolio.
- The inspection should be conducted by a third party expert and QC by HCV.

Public Housing (PH)

Policy

Admissions and Continued Occupancy Policy (ACOP) - Annual inspections will be conducted for all units. Residents will be notified at least 48 hours in advance. The CHA shall inspect the condition of the dwelling unit, the equipment within, and any areas assigned to the resident for upkeep. The CHA will use all inspections to assess the resident's compliance with housekeeping standards and overall care of the dwelling unit and equipment in accordance with the Lease. The CHA will provide the resident with a written statement regarding dwelling unit conditions, and the CHA shall request work orders for all items found to be in disrepair.

Operations

UPCS Inspections (random and visual only)

- 3rd party vendor (The Inspection Group, Inc.)
- QC performed by CHA portfolio quality control teams
  - CHA portfolio team members are required to be certified in UPCS inspection

Families with child under 6 years as of 4/18/17

- 2,053

Total PH portfolio

- Traditional Families: 8,969-56%
- Senior Families: 7,049-44%

Risk

Housing families in a toxic hazardous environment that can suffer permanent and/or long-term harm.

Recommendations

- Test, for lead, CHA properties that have not been totally rehabbed prior to 1978.
- Ensure that CHA has passed a lead inspection for each unit.

CONFIDENTIAL

Office of the Inspector General
Advisory #12

TO: Eugene Jones, Jr., Chief Executive Officer;
Jose Alvarez, Chief of Staff;
Patricia Rios, Chief Administrative Officer

FROM: Elissa Rhee-Lee, Inspector General
DATE: December 7, 2017
SUBJECT: Security Recommendations for Master Keys

The Chicago Housing Authority (CHA)'s General Services Department is responsible for the control and security of the master keys at CHA headquarters, 60 East Van Buren, Chicago, IL. As such, General Services maintained two sets of master keys for all CHA offices and storerooms at that location.

Recently, it was reported to the Office of Inspector General (OIG) that both sets of master keys were missing from the General Services offices. The OIG conducted an investigation into the matter and reviewed the key-control process. It was discovered that appropriate policies and procedures which governed the control and security of the CHA master keys did not exist, nor was there appropriate protocol in place for those times when master key control is compromised.

As a result of the above, the OIG recommends that the following controls be immediately enacted:

- The CEO will designate the Chief Administrative Officer for developing appropriate policies and procedures which govern the control of the CHA's ***master keys***.
- The day-to-day operations will remain with the Deputy Chief of Fleet and Facilities. The Chief Administrative Officer has the ultimate oversight of the CHA's ***master keys.***
- The CEO or designee will approve the issuance of any ***master keys***. When *master keys* are issued, the receiver will sign a receipt documenting this transaction. The receipt will be maintained by the Chief Administrative Officer.

- The CEO or designee will approve the issuance of any ***single-floor master keys***. Once a *single-floor master key* is issued, the employee will sign a receipt documenting this transaction. The receipt will be maintained by the Chief Administrative Officer.

- Upon separation from the CHA, any individual in possession of *master keys* must return those keys before any final benefits are paid.

- All *master keys* must be maintained in a secure location. Locking them in a desk is not considered secure. A lock box or a small safe should be considered for storage.

- The Chief Administrative Officer will approve a policy and procedure similar to Section 2.5(b) of CHA's Fleet Policy to ensure accountability and proper control of all *master keys* that have been issued.

- Any individual who maintains a set of *master keys,* and is on leave, should designate someone to maintain the *master keys* while they are gone. This transfer should be documented and the assigned individual should maintain the usage log.

- Upon conference with the Chief Administrative Officer, it was decided that one set of *master keys* be maintained by General Services.

CONFIDENTIAL

Office of the Inspector General
Advisory #13

TO: Eugene Jones, Jr., Chief Executive Officer;
Jose Alvarez, Chief of Staff;
Patricia Rios, Chief Administrative Officer

FROM: Elissa Rhee-Lee, Inspector General
DATE: December 7, 2017
SUBJECT: Security Recommendations for Identification Badges

Chicago Housing Authority (CHA)'s central office located at 60 East Van Buren, Chicago, IL, utilizes card reader technology for physical access control, through the use of identification badges (ID badge) and badge readers. CHA employees are issued a building ID badge upon hire, which provides access to the elevator bank for the 2nd through 16th floors of the building. Employees are also issued a CHA identity badge which provides access to various floors, rooms and offices on all CHA floors.

Certain sections of CHA office space, such as the Executive Offices, the Office of the Inspector General (OIG), and Human Resources, are not accessible to all CHA employees due to the nature of the department's functions (i.e. independent OIG, sensitive and confidential documents contained therein, etc.). However, a limited number of CHA employees have been provided Master Access, which grants access to all restricted areas in CHA office space.

In order to gain access to a secured area an employee is required to place their ID badge in front of the badge reader. Once access is granted, information about that transaction is stored for later retrieval; reports can be generated showing the date/time the card was used to enter the controlled access point. It should be noted, however, that badge access is not required when departing a secure area.

Based on the above, the OIG conducted a physical security access audit and found that four CHA Information Technology Services (ITS) employees had Master Access, allowing those users unrestricted access to all areas within the CHA. The OIG audit also found that no rules existed defining the circumstances under which Master Access was granted, or rules regarding the use of that special access.

The audit also found that, per CHA's System Access Request Form, a user is granted access to restricted areas with approval from their department's director, while access to the 12th floor requires approval from the CHA's Chief of Staff. Non-CHA employees are granted access to their work floor only unless otherwise specified by the applicable CHA manager.

Current guidance on ID badges can be found in the ITS Information Security Policy, Section 12.0, Physical Access Controls, which applies to all CHA and CHA-related locations:

- Access to areas must be limited to authorized personnel;
- Access to locations that contain IT equipment must require appropriate identification (e.g. entry access card);
- Visitors must be identified and authorized for entry;
- Unattended equipment must be physically secured (via locking cables, locked cabinets, etc.).

Although it was explained that Master Access was necessary for ITS employees in order for them to address critical ITS issues and provide 24/7 technical support to restricted areas, specific policy in this area should be enhanced to better protect the physical security of restricted access areas.

In order to strengthen current access controls, the OIG recommends that the following be enacted to ensure only authorized personnel are allowed in a designated area, such as the OIG, Executive and Human Resources office space, or any other sensitive areas designated by the Chief Administrative Officer:

- Limit the number of users with Master Access;
- Define the circumstances under which Master Access is granted;
- Establish guidelines for those granted Master Access rules, and rules dictating the use of Master Access;
- Modify CHA's System Access Request Form regarding approval for access to specified restricted areas, with approval authority by the executive and/or Inspector General having control over that restricted space;
- Prior to entering a department's restricted area, notification must be made to the executive and/or Inspector General having control over that restricted space;
- Require Master Access users to document the reasons for unaccompanied entry into restricted space.

These recommendations will not impact the necessity for entry into restricted space in the case of an emergency, or any issue involving the safety and security of CHA employees.

CONFIDENTIAL

Office of the Inspector General
Advisory #14

TO: Eugene Jones, Jr., Chief Executive Officer

CC: Jose Alvarez, Chief of Staff
Patricia Rios, Chief Administrative Officer
James Bebley, Chief Legal Officer
Michael Moran, Chief Financial Officer
Mary Howard, Chief Resident Services Officer
Kathryn Ludwig, Chief Housing Choice Voucher Officer
Derek Messier, Chief Property Officer
Diana Liu, Chief Development and Construction Officer
Michael Gurgone, Chief Investment Officer
Dionna Brookens, Chief Procurement Officer
Allen Faucett, Internal Auditor
Bryan Land, Deputy Chief of IT Officer

FROM: Elissa Rhee-Lee, Inspector General
DATE: December 7, 2017
SUBJECT: Illinois Identity Protection Act

In its normal course of business, the Chicago Housing Authority (CHA) collects Personally-Identifiable Information (PII), such as social security numbers, dates of birth, and addresses, from employees, tenants, landlords, vendors, contractors, and subcontractors. As such, the CHA is responsible for safeguarding and ensuring the security of this sensitive PII in both paper and electronic form, in order to prevent a privacy incident.

Organizational harms brought upon the CHA from unauthorized access of PII may include a loss of public trust, legal liability, theft, fraud, or remediation costs. The consequences may extend much further and include reputation damage, loss of customer trust, employee dissatisfaction, attrition, and clean-up costs following the breach.

The CHA recognizes the need to maintain confidentiality in the numerous IT systems where PII data may reside. Recently, the Office of the Inspector General (OIG) and Internal Audit facilitated a Yardi Working Group with CHA stakeholders to identify potential vulnerabilities in Yardi, and to address the risks it poses to the agency, such as security access controls and the protection of PII.

A review of CHA's confidentiality and security requirements determined that the Information Technology Services (ITS), Information Security Policy (2013), provides a foundation for protecting information collected, transmitted, processed, stored or presented via CHA's systems. The policy is based on standards and best practices defined by HUD and national organizations, as well as being consistent with numerous federal legislative directives.

On June 1, 2010, in an effort to control the collection and use of PII, the State of Illinois enacted the Identity Protection Act (5 ILC 179), which prohibited certain uses of Social Security Numbers (SSN) at public institutions and agencies. The following are specific prohibited activities enumerated in the Identity Protection Act, but which are not included in the ITS Information Security Policy (2013):

1. Publicly posting or displaying a SSN;
2. Printing a SSN on any card required for the individual to access products or services provided by the person or entity;
3. Printing a SSN on materials that are mailed, unless federal law requires the SSN to be on the document to be mailed;
4. Requiring an individual to use his or her SSN when accessing an Internet website;
5. Using a SSN for any purpose other than the purpose for which it was collected.

In addition to the above five prohibitions, the Identity Protection Act directs each agency to draft and approve an identity-protection policy, as well as conduct training for all employees having access to SSN's in the course of performing their duties. The Act also makes it a Class B misdemeanor for any person found guilty of intentionally violating the prohibitions in the Act.

Government agencies are a common target for hackers and identity thieves. Strong defenses diminish the likelihood of any information being compromised. Adequate procedures and controls related to safeguarding PII in the possession of the CHA and its service providers enhance integrity in the agency's information security and lessen the impact of a breach involving PII data.

In order to tighten data privacy and security processes at the CHA, the OIG recommends the following:

1. ITS review the Illinois Identity Protection Act and update the ITS Information Security Policy accordingly;
2. ITS implement the components of the identity-protection policy that are necessary to meet the requirements of the Act;
3. ITS update the Information Security Policy to include the above-referenced prohibited activities;
4. ITS conduct training for all employees having access to SSN's in the course of performing their duties;
5. All Department Chiefs direct their personnel to review the Identity Protection Act and comply with the above-referenced prohibited activities.