2020 Privacy Impact Assessment

ECM Utility Assistance Program Automation

Human Services Department, Seattle City Light, Seattle Public Utilities

03.16.2016

Seattle
Information Technology

Privacy Impact Assessment overview

What is a Privacy Impact Assessment?

A Privacy Impact Assessment ("PIA") is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. It asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

When is a PIA required?

A PIA may be required in two circumstances.

- When a project, technology, or other review has been flagged as having a high privacy risk.
- When a technology is required to complete the Surveillance Impact Report process. This is one deliverable that comprises the report.

How to complete this document?

As department staff complete the document, they should keep the following in mind.

- Responses to questions should be in the text or check boxes only, all other information (questions, descriptions, etc.) should **NOT** be edited by the department staff completing this document.
- All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

1.0 Abstract

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

The objective of the ECM Utility Assistance Program (UAP) Automation project is to implement an online application form and tool that improves customer experience; improves accuracy; decreases processing time by Seattle City Light (SCL), Seattle Public Utilities (SPU), and Human Services Department (HSD); and decreases the turn-around time for customers.

This project will provide an online application process for UAP that will use Oracle's Webcenter Content (WCC) suite, and will interface Oracle's Enterprise Content Management (ECM) system with the Customer Care & Billing (CCB) system and use Oracle's Identity Cloud Service (IDCS) for single sign on for the customer. The goal is to create a consistent process for the customer and create efficiencies for all three City departments.

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

The online application will be collecting sensitive data, including the collection of PII, and more specifically Social Security Number (SSN) to validate income.

2.0 Project / Technology Overview

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed

2.1 Describe the benefits of the project/technology.

This new system will allow efficiency of work through the elimination of some manual work, and the use of one system rather than multiple systems to administer and manage the programs under the Utility Assistance Program. A new singular system will also create increased transparency between City departments.

2.2 Provide any data or research demonstrating anticipated benefits.

This question is not applicable.

2.3 Describe the technology involved.

There are two vendors providing services around implementation and organizational change management for the project: TEAM IM (previously Team Infomatics), and Motive Power.

Technology involved in the project includes:

- Oracle Webcenter Content (WCC)
  - Enterprise Content Management (ECM) for document repository
  - WCC for workflow
- Oracle Identity Cloud Service (IDCS) for single sign on

- Customer Care and Billing System to validate and apply data

2.4 Describe how the project or use of technology relates to the department’s mission.

This project will provide the ability for City departments to process applications faster and provide assistance to customers in need quicker through one system and a more automated process.

2.5 Who will be involved with the deployment and use of the project / technology?

The project deployment, change management, and implementation teams includes:

- Implementation Vendor
- Organizational Change Management Vendor
- IT Project Manager
- IT Business Analyst
- IT Business Systems Analyst
- 2 ECM Developers
- 2 DBA/Middleware Developer
- IDCS Developer
- Network Team
- CCB Developer
- ECM Program Manager
- QA Resource

Designated lines of business within SCL, SPU and HSD will be using this application, with ITD providing ITD Operations and Maintenance (O&M) support.

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities are bound by restrictions specified in the Surveillance Ordinance and Privacy Principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

Access to the application by internal staff will be:

- Defined by the business
- Implemented using defined access permissions provided by the business
- Authenticated and validated through security access rights using Active Directory *(AD)*

Additionally, there will be an audit trail and log of who accesses the application and its data

3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

This question is not applicable.

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.

An annual privacy and security awareness training is required for all employees.

Additional specific training will also be provided by the respective business units.

4.0 Data Collection and Use

Provide information about the policies and practices around the collection and use of the data collected.

4.1 Provide details about what information is being collected from sources other than an individual, including other IT systems, systems of record, commercial data aggregators, publicly available data and/or other city departments.

Aside from the data provided by individual customers, the only other data involved in the project will be pulled in from one IT system, Customer Care and Billing (CCB). Data collected from CCB includes customer name, address, and account status.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

Internal Reps are aware of what data to collect to qualify a customer for their program. Questions on the *application* are easy to understand and ‘help/tips’ will be available within the application to provide additional details and guidance for our customers.

Additionally, if a customer enters the wrong information when submitting an application, a contact phone number and e-mail will be provided so that the information can be corrected, and the application can move forward.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

The project is targeted to be fully deployed and in use by May of 2022.

Departments using the technology are:
Seattle City Light (SCL), Seattle Public Utilities (SPU), and Human Services Department (HSD)

Department doing Operations and Maintenance:
Seattle Information Technology Department (ITD)

4.4 How often will the technology be in operation?

The solution will be available 24 hours, 7 days a week for customers.

4.5 What is the permanence of the installation? Is it installed permanently or temporarily?

Installation is permanent until end of software lifecycle or a replacement is implemented.

4.6 Is a physical object collecting data or images, visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

There will be a page within the application where the customer is required to upload required documents. The page is clearly marked as a document upload page, upload document icon will be visible and instruction text will be present. ‘Help/tip’ tool will also be available to provide additional guidance on how to upload a document.

4.7 How will data that is collected be accessed and by whom?

Collected data will be accessed by our Internal Reps (SCL, HSD, SPU) using their Internal system. Internal Reps are City of Seattle department employees. Internal Reps must first have the right security access/roles to access the system and must authenticate.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols. Please link memorandums of agreement, contracts, etc. that are applicable.

- The application is “on premise” and not in the cloud. ITD will be supporting the application once implemented.
- The Front end of the application uses TEAM IM’s customer front end User Interface (UI), called Modern UI.
- The City also has a contract with the implementation vendor (TEAM IM) and is available for troubleshooting.

4.9 What are acceptable reasons for access to the equipment and/or data collected?

City Departments will have access to the data to assist the public, and provide necessary services.
ITD will need access only for Operations and Maintenance (O&M) support.
The vendor may need access for operational support or to troubleshoot technical issues should they arise.

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) and to provide an audit trail (viewer logging, modification logging, etc.)?

- The data will be encrypted at rest and in transit
- There will be an audit trail and log of who accesses the application and its data
- Additionally, internal department staff/users will have to authenticate in order to be able to access the system and data residing therein
- Finally, licenses must be approved by business

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

The data will be stored in Oracle's Enterprise Content Management (ECM) document repository. Information will only be accessed by those who have approved security roles to access the identified data.

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

City departments are responsible to audit for compliance with legal deletion requirements. Users with the proper security access/role will be able to perform this task.

5.3 What measures will be used to destroy improperly collected data?

Application data and uploaded documents will follow the City's retention schedule requirements. As such, data will not be deleted/removed from the system until the retention period has been reached. Once the retention requirements are met, the business will ensure data is purged securely.

The existing Utility Discount Program Steering Committee and a user group that will be set up will continuously evaluate the application, its effectiveness, and at ways to prevent the collection of unnecessary data and/or removal of fields.

5.4 Which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

Seattle City Light (SCL), Customer Care Division

- Customer Care Officer

Seattle Public Utilities (SPU), Utility Account Services

- Specified Director

HSD Community Services Unit

- Specified Director

City Clerk's Office

- City Records

6.0 Data Sharing and Accuracy

6.1 Which entity or entities inside and external to the City will be data sharing partners?

SCL, SPU and HSD will be using one system as configured by security to access data in the new application.

No data is planned to be shared outside of the City at this time.

6.2 Why is data sharing necessary?

Data is being shared to eliminate redundant work that is currently being done in separate systems and by separate workgroups to get customers assistance.

6.3 Are there any restrictions on non-City data use?

Yes ☐ No ☒

6.3.1 If you answered Yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

The Washington State Public Records Act, and public disclosure response may limit the City's ability to enforce restrictions.

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?

A governance document is in progress to be signed by SCL, SPU and HSD to define the decision making process on data sharing, program roadmap and priority of enhancements after go live.

6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

Customer data will be checked for accuracy with CCB, the source of truth for customer data for COS Utilities. Data not captured in CCB will be manually validated by the Internal Reps assigned to the case.

6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

Customers have the ability to modify information either the system created or they entered previously.

7.0 Legal Obligations, Risks and Compliance

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

This question is not applicable.

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

An annual privacy and security awareness training is required for all employees. Training will also be provided by the respective business units.

7.3 Given the specific data elements collected, describe the privacy risks identified and for each risk, explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Respond here. Please work with the Privacy Team to identify the specific risks and mitigations applicable to this project / technology.

Users of the system must be approved by appropriate management to gain access to the system. Access will be granted by ITD Applications, who will be doing the Operations and Maintenance (O&M) of the system. Based on permissions granted, only certain employees will be able to access certain data where sensitive PII are being collected to validate income. The system allows masking sensitive data based on security roles.

The system is "on premise", and not in the "cloud", and the data will be encrypted in transit and encrypted at rest at the database level.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

None identified.

8.0 Monitoring and Enforcement

8.1 Describe how the project/technology maintains a record of any disclosures outside of the department.

Any disclosures outside of the department will be logged and tracked through the City's Public Disclosure Tracking System, GovQA.

8.2 What auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

- City Auditors are able to conduct an audit at any time
- Security auditing can be conducted at any time by ITD Security and Infrastructure teams.