2019 Privacy Impact Assessment

LobbyGuard

Seattle Police Department

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.

LobbyGuard technology streamlines the check-in process and transitions SPD from a manual paper sign-in/sign-out form to a digital visitor management system. This digital visitor management system is designed to solve major challenges related to the visitor check-in process: speed and security.

Once the sign-in process is complete, the person the visitor is there to see (if that person is in the system), will receive a text and/or email notifying them that a visitor is waiting in the lobby. Staff data, including email and mobile number for texting is also stored in the system to facilitate notification of a visitor. The text and email include the information gathered at the kiosk: First Name, Last Name & Company.

If the person the visitor is there to see is not in the system for the visitor to choose, the officer at the lobby will manually reach out to that person, if possible, to notify them of their visitor. A business process is in place to get that person in the system for future visitors, if desired by SPD.

When staff is notified of a visitor, a badge is printed behind the counter and held by the office in the lobby until the staff arrives to receive their visitor. The badge is given to the staff for the visitor to wear. When the visit is over, the visitor is escorted back to the kiosk and instructed to scan their badge at the kiosk to check-out. The badge is kept by the visitor for disposition.

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

A PIA is necessary to address possible concerns from the public that SPD is collecting personal data, including that from a visitor's driver's license. As a convenience to a visitor, this system has the ability to scan a visitor's driver's license to pull in the user's first and last name, so that a visitor does not need to type their first and last name. The system is configured to only pull in the visitors first and last name from a license scan. This saves the visitor time by reducing the amount of typing required to meet the sign-in/out requirements of access to the SPD security facility.

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.

A digital visitor management system is designed to solve the following major challenges related to the visitor check-in process: speed and security. A sign-in/out process is mandated by SPD policy and CJIS regulatory requirement.

2.2 Provide any data or research demonstrating anticipated benefits.

Speed

The paper check in book process doesn't provide visibility into SPD visitor trends and causes congestion at the receiving desk. Using a self-registration kiosk at the entrance provides a streamlined way to manage visitor entry while keeping the reception area clear and moving quickly. In a matter of seconds, visitors can scan their driver's license or other ID, or enter details into the kiosk to register their visit relieving the burden on desk officer and providing an improved experience for your visitors. Pre-registration allows staff to schedule their upcoming visitors to expedite the check in process.

Security

A digital visitor system improves security by providing a digital record of visitors on-site. The first step in making sure everyone on your premises is safe in an emergency is knowing exactly who's on your premises. With a visitor management system, SPD will have this information available and reports are available to show who is and is not onsite. Printed badges let staff easily recognize visitors and verify they are in the correct area.

With using a digital visitor management system SPD will be collecting and storing details of visitors for a limited period. Because of this SPD will need to gain consent from the individual to do so. This can be achieved by ensuring that the individual reads and understands the privacy policy and by moving forward in the process and receiving a badge they are acknowledging that they agree with the privacy policy and conditions of storage and give consent for their data to be stored in the system.

2.3 Describe the technology involved.

LobbyGuard is a SaaS application, touchscreen all-in-one computer hooked directly to the internet (not connected to the SPD or SEA domains).

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

This system assists SPD to support quality public safety by delivering professional police services. Using a paper sign in process is neither professional, secure or acceptable. Visitors would often have to wait for an extended amount of time for the person to come down. With this system the person being visited receives an email and a text message on their department phone.

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

There currently is no standard for visitation management. This system was installed and is maintained by SPD staff. Designated Seattle IT staff are also involved in supporting and maintaining the system.

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.

APRS (Audit, Policy & Research Section) users who are responsible for the lobby at SPD headquarters, have been trained in the use of the system to make configuration updates. The application is not currently subject to formal change control, but APRS staff does not make changes without consulting with Seattle IT first. Seattle IT staff has access necessary to support APRS staff.

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

Criminal Justice Information Systems compliance requires SPD to log all visitors to SPD's physical locations. Prior to the use of this system, compliance was achieved through a paper sign in, this technology allows for SPD to adhere to CJIS compliance requirements with the added benefits defined in 2.2.

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.

A formal communication was sent from the Chief Operating Officer to SPD staff in HQ providing proper sign-in process guidelines, protocols and requirements for use of the new system.

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.

No data other than the visitor's First name, Last name, and optionally Company are being collected. The system date and time stamps the transaction. Data is stored at rest as an electronic version of a paper sign in/out sheet. No other information is being collected from other systems.

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

The system is configured to only require and/or collect visitors First name and Last name. All configuration changes are audited/logged by the system.

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 technology is used by SPD HQ visitors and designated SPD staff. The technology is already deployed.

4.4 How often will the technology be in operation?

8-5 Monday through Friday, the hours that the SPD lobby is open to the public.

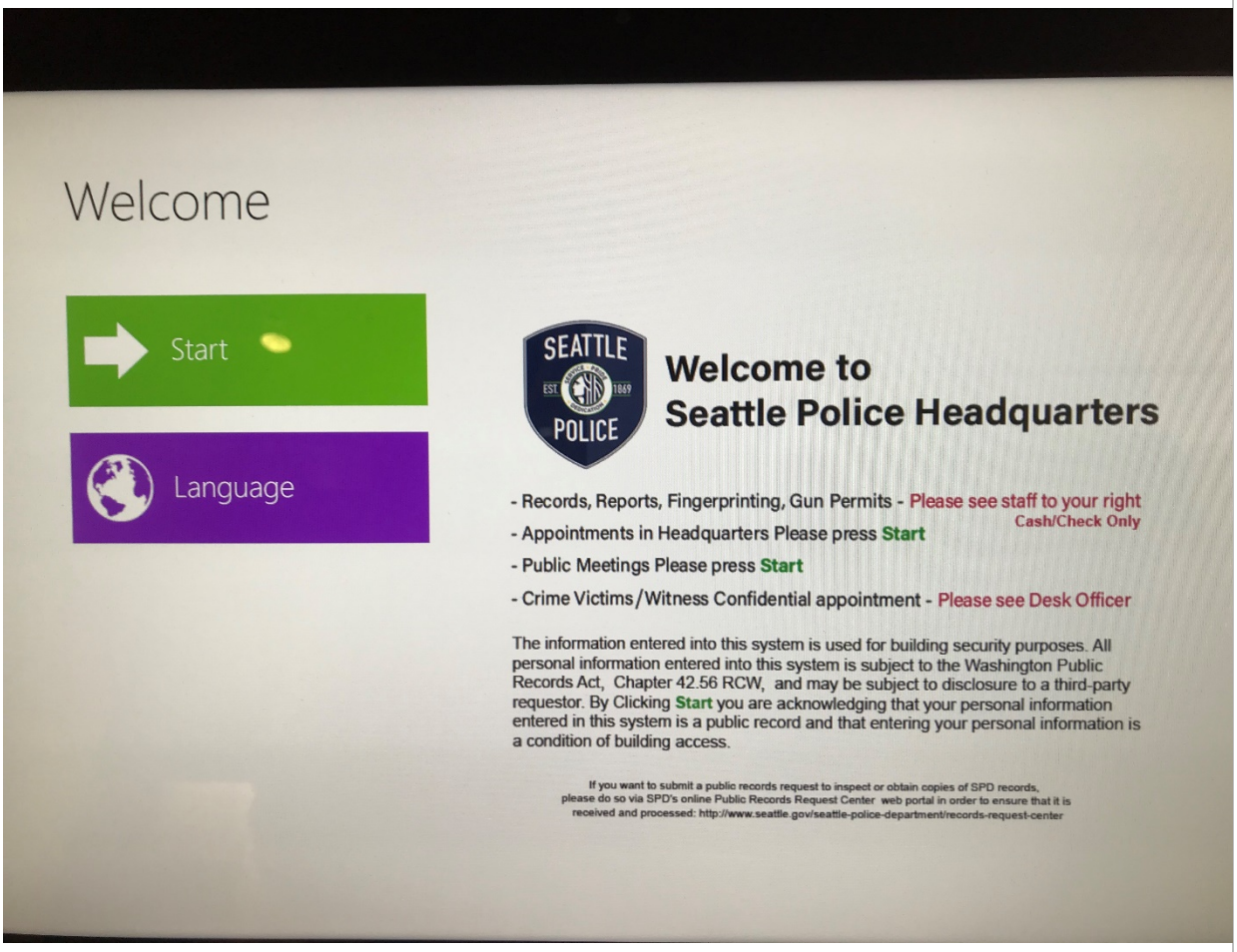
4.5 What is the permanence of the installation? Is it installed permanently or temporarily?

LobbyGuard is a permanent solution.

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?

Visitor's First name, Last name and Company (optional) are the only information collected.

SPD gains consent from the individual to do so. Prior to data collection, the visitor is presented with the following language:



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

Data is sent to staff identified by the system as able to receive visitors via email and optionally text, notifying them that their visitor has arrived.

All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy

12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

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.

Access to the system is limited only to trained APRS staff, authorized SPD administrators, and authorized Seattle City IT administrators.

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

Data can be accessed for public disclosure requests or during a facility emergency to see who is in the building.

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.)?

Data is protected by SSL certificates on the SaaS solution.

Individuals can only access the system via unique login credentials and all activity in the system is logged and can be audited.

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

The content below can be found in the LobbyGuard Statement on Data Security (https://kb.lobbyguard.com/hc/en-us/articles/224371627-LobbyGuard-Statement-on-Data-Security).

"Data Transmission and Secure Storage Transmission of all data to and from the LobbyGuard Kiosk to the customer database is via SSL (secure socket layer). Data at rest is secured via Microsoft Transparent Data Encryption (TDE) utilizing a 256-bit data encryption algorithm. For more information on Microsoft TDE visit **https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption**".

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

Systems keep logs of access and action. The Office of Inspector General may audit for compliance at any time.

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

All information must be gathered and recorded in a manner that is consistent with SPD Policy 6.060, such that it does not reasonably infringe upon "individual rights, liberties, and freedoms guaranteed by the Constitution of the United States and the State of Washington, including freedom of speech,

press, association, and assembly; liberty of conscience the exercise of religion; the right to petition government for redress of grievances; and the right to privacy."

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

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

SPD APRS are responsible for ensuring compliance with retention requirements. The Office of the Inspector General (OIG) can audit, review, and ensure compliance at any time.

6.0 Data Sharing and Accuracy

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

Data obtained from the system may be shared outside SPD with the other agencies, entities, or individuals within legal guidelines or as required by law.

Data may be shared with outside entities in connection with criminal prosecutions:

- Seattle City Attorney's Office
- King County Prosecuting Attorney's Office
- King County Department of Public Defense
- Private Defense Attorneys
- Seattle Municipal Court
- King County Superior Court
- Similar entities where prosecution is in Federal or other State jurisdictions

Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Discrete pieces of data collected by the parking enforcement systems may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayor's Directive, dated February 6, 2018.

SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the parking enforcement systems.

6.2 Why is data sharing necessary?

Data sharing may be necessary for SPD to fulfill its mission as a law enforcement agency and to comply with legal requirements.

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.

Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.

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?

Research agreements must meet the standards reflected in SPD Policy 12.055. Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

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

Accuracy is not checked. Visitors are responsible to ensure the data entered meets their expectation of accuracy.

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

Individuals may request records pursuant to the PRA, and individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

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?

SPD already collects visitors First name and Last name with a physical sign-in process. This system uses a computer instead of a piece of paper.

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

System support staff are required to complete mandatory privacy and security awareness training.

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.

Per SPD Policy 16.170, all users are restricted from accessing the data, except as it relates to a specific criminal investigation. Appropriate SPD personnel can access the data (assuming it is within the 90-day retention period) as it relates to the active investigation.

Any activity by a user to access this information is logged and auditable. Washington State's Public Records Act requires release of collected data, however, making it possible for members of the public to make those identification connections on their own if they have access to the information necessary to do so.

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?

The system includes an option to scan a visitor's driver's license for the convenience of not having to type their first and last name. While the data is mandatory for entry into the SPD secured facility, the visitor has the option to manually enter their first and last name, or us their driver's license. The system does not clearly indicate that no other driver's license information is being gathered, stored or used for purpose other than the visitation process.

8.0 Monitoring and Enforcement

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

Per SPD Policy 12.080, the Crime Records Unit is responsible to receive and record all requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies." Any requests for disclosure are logged by SPD's Crime Records Unit or Legal Unit, as appropriate. Any action taken, and data released subsequently, is then tracked through the request log. Responses to Public Disclosure Requests, including responsive records provided to a requestor, are retained in SPD's GovQA system for two years after the request is completed.

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.

Self-audits are not performed, however, the Office of the Inspector General (OIG) can conduct an audit at any time.

Appendix A

Lobbyguard Artifiact

LobbyGuard
Statement on Data S

Policy Artifiact

Lobby Guard
Visitation Process at