POWERFUL TECHNOLOGY SOLUTIONS
FOR THE CITY AND PUBLIC WE SERVE

City of Seattle Privacy Impact Assessment

VOLUNTEER MANAGEMENT SYSTEM PROJECT

Owner: Office of Immigrant and Refugee Affairs

Date: 4/4/2017

CONTENTS

PURPOSE OF PIA

A Privacy Impact Assessment is designed to outline the anticipated privacy impacts from a City project/program or project/program update that collects, manages, retains or shares personal information from the public. The PIA will provide project/program details that will be used to determine how privacy impacts may be mitigated or reduced in accordance with the City of Seattle Privacy Principles and Privacy Statement.

ABSTRACT

Please provide a brief abstract. *The abstract is the single paragraph that will be used to describe the project and* ***will be published on the Privacy Program website.*** *It should be a minimum of three sentences and a maximum of four, and use the following format:*

- *The first sentence should include the name of the project, technology, pilot, or project/program (hereinafter referred to as "project/program").*
- *The second sentence should be a brief description of the project/program and its function.*
- *The third sentence should explain the reason the project/program is being created or updated and why the PIA is required. This sentence should include the reasons that caused the project/program to be identified as a "privacy sensitive system" in the Privacy Intake Form, such as the project/program requiring personal information, or the technology being considered privacy sensitive.*

As directed by the Mayor's Office, the Office of Immigrant and Refugee Affairs (OIRA) is striving to naturalize over 80,000 legal permanent residents (Green Card holders) living in Seattle by launching the New Citizen Campaign (NCC). This comprehensive outreach and education project makes citizenship assistance more accessible to larger numbers of eligible Seattle residents through partnerships with community-based organizations and other City departments.

Crucial to the success of NCC is our engagement with and management of the hundreds of volunteers staffing citizenship application assistance workshops and clinics. Managing hundreds of volunteer registrations and assigning them to volunteer shifts via Survey Monkey and Excel has proven overwhelmingly burdensome for OIRA's limited staff; and a professional volunteer management system is vital to our ability to operate future citizenship events. The software purchased for the volunteer management system will be CERVIS.

PROJECT/PROGRAM OVERVIEW

Please provide an overview of the project/program. *The overview provides the context and background necessary to understand the project/program's purpose and mission and the justification for operating a privacy sensitive project/program. Include the following:*

- *Describe the purpose of the system, technology, pilot or project/program; the name of the department that owns or is funding the project/program and how it the project/program relates to the department's mission;*
- *Describe how the project/program collects and uses personal information, including a typical transaction that details the life cycle from collection to disposal of the information;*

- *Describe any routine information sharing conducted by the project/program both within City of Seattle departments and with external partners. Describe how such external sharing is designed with the original collection of the information.*
- *Identify any major potential privacy risks identified and briefly discuss overall privacy impact of the project/program on individuals*
- *Identify the technology used and provide a brief description of how it collects information for the project/program.*

Purpose

NCC events require large numbers of skilled and unskilled volunteers maneuvering a logistically complex environment. Detailed planning and volunteer placement are crucial to the success of these events.

The organized coordination of volunteers, including volunteer interpreters who speak up to 40 different languages and legal professionals who specialize in fee waiver assistance, is critical to New Citizen Campaign's ability to assist these populations.

The CERVIS volunteer management system will:

- Allow volunteers to self-register via the website.
- Allow the OIRA team administrators create skill- and time-specific volunteer opportunities for volunteers to register.
- Cap the number of available registrations for each opportunity as specified by the OIRA team administrators, and create a waitlist or denial message for anyone attempting to register over that cap.
- Email automated messages to registered volunteers.
- Allow email messaging to specified groups of volunteers and to the entire volunteer pool as needed.
- Send reminders via SMS.
- Allow volunteers to opt out of their assigned shift via the website.
- Track day-of volunteer attendance.
- Allow the OIRA administrators to change volunteer roles/shifts manually as needed.
- Allow for notes or tagging of volunteer profiles by the administrators.
- Report on total, or by individual, participation and volunteer hours
- Track volunteer completion of training and verification of professional credentials.
- Securely store volunteer data.
- Make volunteer opportunities public
- Make available volunteer information, shift schedules, and event locations to registered volunteers only

Use of personal information

The CERVIS system will collect the following personally identifiable information, though not all the information is required:

- Full name
- Company or firm
- ZIP code
- E-mail address

- Phone number
- Emergency contact
- Languages spoken other than English
- Experiences (attorney, paralegal, etc.)
    - Attorney-related fields: AILA member, criminal experience, years of immigration experience, number of naturalization cases handled
    - Law students-related fields: current year in law school, immigration experience
    - Interpretation experience
    - Past citizenship and AILA workshops
- Liability waivers specific to volunteer type
- Food allergies

Data Sharing

CERVIS will not use or share the data collected. All customer data remains the sole property of the City and CERVIS does not use customer data for any purposes other than providing service to their customer. Additionally:

- All CERVIS employee access to customer data is logged and audited
- Password complexity and duration are completely customizable within the CERVIS application
- Customer can implement IP address restrictions for access to administrative functions
- System includes bot detection and anti-bot functionality

Technology

The CERVIS volunteer system is a SaaS system. (http://www.cervistech.com/)
The proposed CERVIS contract includes unlimited online customer service, maintenance, and system upgrades.

- There is an annual subscription for the software. You can have as many administrators as needed and there is no cost per person. The system can also have an unlimited number of volunteers.
- The City will have one CERVIS instance, and it will not be shared with other instances used by other entities.

CERVIS can easily export and import data, to and from most of the Donor Management and CRM solutions. CERVIS uses industry standard data file formats for importing and exporting data to ensure maximum compatibility with the systems most used. For more advanced, direct system-to-system integration, CERVIS offers an enhanced capability Web Services API for custom integration.

CERVIS integrates into most organization's websites using iframes

NOTIFICATION

1. ***How does the project/program provide notice about the information that is being collected?*** *Our Privacy Principles and Statement require that we provide notice to the public when we collect personal information, whenever possible.*
    - *Describe how notice will be provided to the individuals whose information is collected by this project/program and how it is adequate.*

- *If notice is not provided, explain why not. (For certain law enforcement or other project/programs, notice may not be appropriate.)*
- *Discuss how the notice provided corresponds to the purpose of the project/program and the stated uses of the information collected.*

Information will be used only for volunteering purposes, and for no other purpose. All data collected and stored is subject to WA Public Disclosure laws.

2. ***What opportunities are available for individuals to consent to the use of their information, decline to provide information, or opt out of the project/program?*** *Describe how an individual may provide consent for specific uses or whether consent is given to cover all uses (current or potential) of his/her information. If specific consent is permitted or required, how does the individual consent to each use? If notice is provided explain how an individual may exercise the right to consent to particular uses or decline to provide information describe the process. If this is not an option, explain why not. Note: An example of a reason to not provide an opt-out would be that the data is encrypted and therefore unlikely available to identify an individual in the event of a data breach.*

   Volunteers opt-in to register and sign-up for volunteer activities. The only required fields are: first name, last name, and email address. All other data fields are voluntarily provided and are used only to match volunteer skills and experience with an event. Volunteers can modify or delete their data and/or account at any time. Schedule B, Section 1.4 of the Service Agreement addresses issues of security breach. Service Level Indicators and other operational monitoring policies in place to ensure errors can be detected and responded to in a timely and proactive manner are detailed in "Section 4 - Availability" of the Service Agreement.

COLLECTION

3. ***Identify the information, including personal information, that the project/program collects, uses, disseminates, or maintains.*** *Explain how the data collection ties with the purpose of the underlying mission of the department.*

   The data listed below will be collected to support volunteer OIRA activities and events. Volunteers are only required to provide the following information: first name, last name, and email address. All other data fields are voluntarily provided and are used only to match volunteer skills and experience with an event. Volunteers can modify or delete their data or account at any time.

Data fields: Volunteer Registration
First name
Last name
Company or firm
ZIP code
Email address
Phone number
Emergency contact
Other than English, languages spoken (pre-populated list we want to generate)
What experience do you have? (Attorney vs. paralegal vs. other roles) *

Attorneys: AILA member
Attorneys: Criminal experience*
Attorneys: Years of immigration experience
Attorneys: # of Naturalization cases handled
Law students: Current year of law school
Law students: Immigration experience
Interpretation experience
Experience: Past citizenship and AILA workshops
Experience: Other
Liability waivers (specific to volunteer type)
Food allergies
T-shirt size

Data fields: Event-specific
Shift availability
Volunteer type
Comfort with standing for most of the shift
How did you hear about event?
Availability for pre-help
Availability for post-event help

4. ***Is information being collected from sources other than an individual, including other IT systems, systems of records, commercial data aggregators, publicly available data and/or other departments?*** *State the source(s) and explain why information from sources other than the individual is required.*

   No other systems or sources are used.

USE

5. ***Describe how and why the project/program uses the information that is collected****. List each use (internal and external to the department) of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used.*

   The CERVIS volunteer management system will:

   - Allow volunteers to self-register via the website.
   - Allow the OIRA team administrators create skill- and time-specific volunteer opportunities for volunteers to register.
   - Cap the number of available registrations for each opportunity as specified by the OIRA team administrators, and create a waitlist or denial message for anyone attempting to register over that cap.
   - Email automated messages to registered volunteers.

- Allow email messaging to specified groups of volunteers and to the entire volunteer pool as needed.
- Send reminders via SMS.
- Allow volunteers to opt out of their assigned shift via the website.
- Track day-of volunteer attendance.
- Allow the OIRA administrators to change volunteer roles/shifts manually as needed.
- Allow for notes or tagging of volunteer profiles by the administrators.
- Report on total, or by individual, participation and volunteer hours
- Track volunteer completion of training and verification of professional credentials.
- Make volunteer opportunities public
- Make available volunteer information, shift schedules, and event locations to registered volunteers only.

6. ***Does the project/program use technology to:***
   a. ***Conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly or***
   b. ***Create new information such as a score, analysis, or report?***

If so, state how the City of Seattle plans to use such results. Some project/programs perform complex analytical tasks resulting in other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Explain what will be done with the newly derived information. Will the results be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data?

No analysis will be used to discover or locate a predictive pattern or an anomaly. No new information will be created for a score.

7. ***How does the project/program ensure appropriate use of the information that is collected?*** *Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.*

The volunteers will have a unique ID and password. They can change their passwords at any time. The City administrative users will implement IP address restrictions for access to administrative functions. These passwords are customizable in both complexity and duration. All CERVIS employee access to customer data is logged and audited.

RETENTION

8. ***Does the project/program follow the City records retention standard for the information it collects?*** *Departments are responsible for ensuring information collected is only retained for the period required by law. City departments are further responsible for reviewing and auditing their compliance with this process. For more information, please see the internal retention schedule, here, and records retention ordinance, here.*

In addition, please provide answers to the following questions:

- *How does it dispose of the information stored at the appropriate interval?*

- *What is your audit process for ensuring the timely and appropriate disposal of information?*

The Mayor's naturalization initiative is completed at the end of 2018. Upon completion of the Services, CERVIS is contractually obligated to bring together and deliver to the City all Data and Confidential Information, at which time OIRA and/or the Mayor's Office will determine City-appropriate means of disposal. Contractually, CERVIS agrees to require all Authorized Persons using the Data and Confidential Information to comply with the provision. They also agree to document the methods used to destroy the Data and Confidential Information, and provide certification to the City when all the Data and Confidential Information is destroyed. Additionally, the volunteers can delete any or all their own information at their discretion.

SHARING

9. ***Are there other departments or agencies with assigned roles and responsibilities regarding the information that is collected?*** *Identify and list the name(s) of any departments or agencies with which the information is shared and how ownership and management of the data will be handled.*

   Data will be used by OIRA to manage their volunteer and event scheduling and for no other purpose. Contractually, CERVIS shall acquire no rights to Data and Confidential Information. CERVIS shall not, without the prior written approval in each instance, disclose Data and Confidential Information to any third party nor use Data and Confidential Information for any purpose, except as provided in this contract. They agree to not make any copies or duplicates of any Data and Confidential Information except as the City may otherwise explicitly request.

10. ***Does the project/program place limitations on data sharing?***
    Describe any limitations that may be placed on external agencies further sharing the information provided by the City of Seattle. In some instances, the external agency may have a duty to share the information, for example through the information sharing environment.

    All data remains the sole property of OIRA; CERVIS does not use customer data for any purposes beyond providing service to them.

11. ***What procedures are in place to determine which users may access the information and how does the project/program determine who has access?*** *Describe the process and authorization by which an individual receives access to the information held by the project/program, both electronic and paper based records. Identify users from other departments who may have access to the project/program information and under what roles these individuals have such access. Describe the different roles in general terms that have been created that permit access to such project/program information. Specifically, if remote access to the system is allowed or external storage or communication devices interact with the system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two-factor authentication).*

    The volunteers will have a unique ID and password and can change their passwords at any time. The City administrative users will implement IP address restrictions for access to administrative functions. These passwords are customizable in both complexity and duration. All CERVIS employee access to customer data is logged and audited. In addition, all volunteer data is protected behind Database firewalls and is encrypted while at rest using 256bit AES encryption on both operational systems and in backup storage. Volunteer data selected as "Sensitive Data" is encrypted with an additional layer of 256bit AES encryption within the database. All data is encrypted while in motion via 128bit SSL encryption.

12. ***How does the project/program review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies?*** *Please describe the process for reviewing and updating data sharing agreements.*

    Data sharing is not planned at this time. If changes are made to this policy, we will alert privacy for review of MOUs.

LEGAL OBLIGATIONS AND COMPLIANCE

13. ***Are there any specific legal authorities and/or agreements that permit and define the collection of information by the project/program in question?***
    - *List all statutory and regulatory authority that pertains to or governs the information collected by the project/program, including the authority to collect the information listed in question.*
    - *If you are relying on another department and/or agency to manage the legal or compliance authority of the information that is collected, please list those departments and authorities.*

    CERVIS will be bound by a contractual Service Agreement that includes specific language related to their management of security and confidentiality, data use, data security and security breach. The agreement also addresses data ownership, licensing, and restrictions to stored information. The documented CERVIS Security Policies include language addressing physical, network, system, application, and data security, data privacy, and system redundancy.

14. ***How is data accuracy ensured?*** *Explain how the project/program checks the accuracy of the information. If a commercial data aggregator is involved describe the levels of accuracy required by the contract. If the project/program does not check for accuracy, please explain why. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project/program.*

    Both volunteers and attendees can access, modify, and/or delete their information from their individual accounts.

15. ***What are the procedures that allow individuals to access their information?***
    Describe any procedures or regulations the department has in place that allow access to information collected by the system or project/program and/or to an accounting of disclosures of that information.

    Both volunteers and attendees can access, modify, and/or delete their information from their individual accounts.

16. ***What procedures, if any, are in place to allow an individual to correct inaccurate or erroneous information?*** *Discuss the procedures for individuals to address possibly inaccurate or erroneous information. If none exist, please state why.*

    Both volunteers and attendees can access, modify, and/or delete their information from their individual accounts.

17. ***Is the system compliant with all appropriate City of Seattle and other appropriate regulations and requirements?*** *Please provide details about reviews and other means of ensuring systems and project/program compliance.*

    The system is compliant with all appropriate City of Seattle and other regulations and requirements.

18. ***Has a system security plan been completed for the information system(s) supporting the project/program?*** *Please provide details about how the information and system are secured against unauthorized access.*

    The CERVIS solution is a SaaS, cloud-based solution. Below is CERVIS' security information:

    The privacy, security, and availability of your critical information is Priority #1 at CERVIS Technologies. CERVIS has been designed from the ground up with security in mind.

    Physical Security

    - CERVIS houses and operates all operational servers that store or process customer data in redundant SOC 2 (Type II) data centers in Dallas TX, Seattle, WA, San Jose, CA and Washington DC.
    - Data centers are located in facilities with controlled access and 24-hour security
    - No server room doors are public-facing
    - Server rooms are staffed 24/7
    - Un-marked entry and exit doors
    - Digital security video surveillance
    - Biometric security systems
    - Server room access strictly limited to datacenter employees and escorted contractors or visitors
    - Barcode-only identification on hardware; no customer markings of any type on the servers themselves
    - Fire detection and suppression systems, including dry pipe, fire extinguishers, smoke and fire alarms.
    - Backup power, including UPS and Generators
    - Power Distribution Units (PDU) and electrical panels
    - Heating and cooling (HVAC) mechanisms exist, such as CRAC units, and chillers, to monitor and control temperature and humidity
    - Data centers are maintained with adequate lighting and are free of clutter.

    Network Security

- All systems are protected behind network firewalls that limit both inbound and outbound traffic to the minimum needed access for system operation.
- All systems are protected and monitored by network layer Intrusion Prevention Systems.
- All system-to-system back-end traffic is encrypted and transmitted within private VLANs

Data Security

- All customer data is protected behind Database firewalls
- All customer data is encrypted while at rest using 256bit AES encryption on both operational systems and in backup storage.
- Customer selected "Sensitive Data" is encrypted with an additional layer of 256bit AES encryption within the database
- All customer data is encrypted while in motion via 128bit SSL encryption.

System Security

- All systems are protected and monitored by host layer Intrusion Prevention Systems.
- All systems are protected behind host layer firewalls that limit both inbound and outbound traffic to the minimum needed access for system operation.
- All systems are protected with Anti-Virus and Anti-Malware software which is updated daily
- All operating system, application server, database server, and web server patches and system updates are applied as quickly as possible depending on the severity of vulnerability being addressed.

Application Security

- External network and application level vulnerability tests are conducted daily by an external 3rd party.
- Internal System level vulnerability assessments are conducted monthly.
- Automated web application security assessments are conducted by a third party against CERVIS daily.
- Manual web application security assessments are conducted twice yearly.

Data Privacy

- All customer data remains the sole property of the customer and CERVIS does not use customer data for any purposes other than providing service to the customer
- All CERVIS employee access to customer data is logged and audited
- Password complexity and duration are completely customizable within the CERVIS application
- Customer can implement IP address restrictions for access to administrative functions
- System includes bot detection and anti-bot functionality

System Redundancy

- All data centers provide redundant electrical power, equipment cooling systems and backbone internet connectivity.
- CERVIS databases are stored on redundant drives configured within state-of-the-art dedicated servers.
- All customer data is encrypted, backed up, and stored at a secure offsite location two times per day.

- CERVIS databases are configured with mirror replication so all information in the database is copied (instantly and securely), up to the last committed transaction, to one of our fail-over data centers.
- In the unlikely event that we experience the loss of our primary data center, CERVIS will instantly fail-over to a secondary data center and continue to remain fully operational.

----

19. ***How is the project/program mitigating privacy risk? G****iven the specific data elements collected, discuss 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.*

    Immigration status, country of birth, citizenship, or native language is not asked for in the volunteer registration process.

MONITORING AND ENFORCEMENT

20. ***Describe how the project/program maintains a record of any disclosures outside of the department.*** *A project/program may keep a paper or electronic record of the date, nature, and purpose of each disclosure, and name and address of the individual or agency to whom the disclosure is made. If the project/program keeps a record, list what information is retained as part of the accounting requirement. A separate system does not need to be created to meet the accounting requirement, but the project/program must be able to recreate the information noted above to demonstrate compliance. If the project/program does not, explain why not.*

    Data will be used by OIRA to manage their volunteer and event scheduling and for no other purpose. Contractually, CERVIS shall acquire no rights to Data and Confidential Information. CERVIS shall not, without the prior written approval in each instance, disclose Data and Confidential Information to any third party nor use Data and Confidential Information for any purpose, except as provided in this contract. They agree not to make or permit to be made any copies or duplicates of any Data and Confidential Information except as the City may otherwise expressly request.

21. ***Have access controls been implemented and are audit logs are regularly reviewed to ensure appropriate sharing outside of the department?*** *Is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies? Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.*

    Data will be used by OIRA to manage their volunteer and event scheduling and for no other purpose. Contractually, CERVIS shall acquire no rights to Data and Confidential Information. CERVIS shall not, without the prior written approval in each instance, disclose Data and Confidential Information to any third party nor use Data and Confidential Information for any purpose, except as provided in this contract. They agree not to make or permit to be made any copies or duplicates of any Data and Confidential Information except as the City may otherwise expressly request. The volunteers will have a unique ID and password. They can change their passwords at any time. The City administrative users will implement IP address restrictions for access to administrative functions. These passwords are customizable in both complexity and duration. All CERVIS employee access to customer data is logged and audited. In addition: All volunteer data is protected behind Database firewalls and is encrypted while at rest using 256bit AES encryption on both operational systems and in backup storage. Volunteer data that is selected as "Sensitive Data" is encrypted with an additional layer of 256bit AES encryption within the database. All data is encrypted while in motion via 128bit SSL encryption.

22. ***How does the project/program ensure that the information is used in accordance with stated practices of the project/program?*** *What auditing measures are in place to safeguard the information and policies that pertain to them? Explain whether the project/program conducts self-audits, third party audits or reviews.?*

    OIRA will collect and provide the following for audit and tracking of program data management practices: Event Schedules, Volunteer Registration Reports.

23. ***Describe what privacy training is provided to users either generally or specifically relevant to the project/program.*** *City of Seattle offers privacy and security training. Each project/program may offer training specific to the project/program, which touches on information handling procedures and sensitivity of information. Discuss how individuals who have access to personal information are trained to handle it appropriately. Explain what controls are in place to ensure that users of the system have completed training relevant to the project/program.*

    Staff will be trained on the CERVIS system.

24. ***Is there any aspect of the project/program that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?*** *Examples might include a push of information out to individuals that is unexpected and appears to be intrusive, or an engagement with a third party to use information derived from the data collected that is not explained in the initial notification.*

    Immigration status, country of birth, citizenship, or native language is not asked for in the volunteer registration process. The Program Manager has stated it would be difficult to connect immigration status to language.