# Court Services and Offender Supervision Agency (CSOSA)

## Check In System
## Privacy Impact Assessment

**CONTROLLED UNCLASSIFIED INFORMATION**

**August 2017**

**Community Supervision Services**
**Court Services and Offender Supervision Agency for the District of Columbia**
633 Indiana Avenue, NW, Washington, DC 20004

## **Overview of the Check In System**

The Check -In System is a system used at the Court Services and Offender Supervision Agency's (CSOSA) Martin Luther King, Jr. community supervision site (MLK) for clients reporting to MLK, CSOSA employees located at the MLK site. Clients will enter their names into the system to sign in. When a sign-in is complete, a Community Supervision Officer (CSO) or other designated staff person is electronically notified of the client's arrival. The Check-In System functions as an electronic sign-in sheet, providing attendance information.

## 1. Description of the System

1.1. Describe the system, including the system name, system, acronym, and a brief description of the major functions.

*The Check-In system is operated through an IPAD and will be mounted at the reception location. The client types in his/her first and last name and selects the CSO that they are there to see or the activity, group that they are scheduled to attend. The client's name will then appear on the CSO's computer. There is a person physically located at the reception's area that will direct them and provide guidance.*

*The client types his/her (First and Last) in an IPAD that is secured and locked to this specific application. The client's name will appear on the screen of the CSOSA staff person that the client is visiting or group that they are attend.*

1.2. Describe the purpose for which the personally identifiable information (PII) is collected, used, maintained, or shared.

*The purpose of the system is to establish an electronic check in system of client attendance for reporting, drug testing, program attendance, treatment evaluations, global positioning system (GPS) installations and other related supervision activities. The check in system will replace the manual, paper sign in process that has been used. The check in system allows the agency to capture reporting trends that will help the agency to better manage the programmatic flow within the facility. The first and last name of the client is the only identifier used. The client will type his/her name into the IPAD provided and the system will send an alert to the staff assigned. The system will also be used to generate a list of participants for classes, or group sessions.*

1.3. Is this a new system or one that is currently in operation?

*This is a new system.*

1.4. Is this privacy impact assessment (PIA) new, or is it updating a previous version?
If this is an update, please include the publication date of the original.

*This is a new PIA.*

1.5. Is the system operated by the agency, by a contractor, or both?

*Contractors will not be involved in the design and maintenance of this system. The system is designed, owned and operated by CSOSA.*

## 2. Legal Authorities and Other Requirements[1]

2.1. What specific legal authorities and/or agreements permit and regulate the collection, and use of the data by the system?[2]

- *E-Government Act of 2002*
- *Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems*
- *National Institute of Standards and Technology (NIST) Special Publication (SP) 800- 122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
- *OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*
- *OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information*

2.2. System of Records Notice (SORN) Requirement: Is the information in this system retrieved by a name or a personal identifier? If so, this system will need to be covered by a Privacy Act SORN.[3]

*Yes, this application lists the staff names that are stationed at the MLK site. This application is used at the MLK site only. The application notifies the CSOSA staff of the client name and the check-in date and time.*

2.3. Records Management Requirement: Does a records retention schedule, approved by National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.[4]

*Yes. General Records Schedule 18, Item 17.b: Visitor Control Files. Registers or logs used to record the names of outside contractors, service personnel, visitors, employees admitted to areas, and reports on automobiles and passengers. Destroy 2 years after final entry or 2 years after date of document, as appropriate.*

[1] If you are unsure of your legal authority, please contact CSOSA's Senior Agency Official for Privacy.

[2] Legal authorities are statutes, executive orders, federal regulations, and/or Memorandum of Understandings. Include the citation/reference of the legal authority.

[3] System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by CSOSA. Verify if there is an existing SORN for the system.

[4] If you are unsure of the records retention schedule, please contact CSOSA's Records Management Officer.

*https://www.archives.gov/files/records-mgmt/grs/grs.18.pdf.*

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timeliness in the records disposition schedule?

*Yes. The PII contained in the system is disposed of in accordance with General Records Schedule 18, Item 17.b: Visitor Control Files. The retention is 2 years after final entry. A report will be generated annually to identify and delete PII that has met its retention period.*

2.5. Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.).

*CSOSA does not yet have an electronic data records management system that would potentially provide automatic purging and other records management capabilities. These are handled manually. A periodic report will be generated to identify any records that have met the retention schedule and they can then be deleted from the database.*

## 3. Characterization and Use of Information

### Collection

3.1. Select the specific personal information data elements (e.g. name, email, address, phone number, date of birth, social security number, etc.) that the system collects, uses, disseminates, or maintains.

*The application houses the list of staff first and last names and their team assignment. Only the staff stationed at the MLK site. The clients type in their first their first and last names and the application collects the names at that point.*

| | | | | | |
|---|---|---|---|---|---|
| **Identifying Numbers** | | | | | |
| Social Security | | Alien Registration | | Financial Account | |
| Taxpayer ID | | Driver's License | | Financial Transaction | |
| Employee ID | | Passport | | Patient ID | |
| File/case ID | | Credit Card | | | |
| Other identifying numbers (please specify): | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| Work-related data | | | | | |
| Occupation | | Telephone number | | Salary | |
| Job title | | Email address | | Work history | |
| Work address | | Business associates | | | |
| Other work-related data (specify): | | | | | |

| General Personal Data | | | | | |
|---|---|---|---|---|---|
| Name | ✖ | Date of birth | | Religion | |
| Maiden Name | | Place of birth | | Financial Info | |
| Alias | | Home address | | Medical Info | |
| Gender | | Telephone Number | | Military Services | |
| Age | | Email Address | | Physical characteristics | |
| Race/Ethnicity | | Education | | Mother's maiden bame | |
| Other general personal data (please specify): | | | | | |

| Distinguishing features/Biometrics | | | | | |
|---|---|---|---|---|---|
| Fingerprints | | Photos | | DNA profiles | |
| Palm prints | | Scars, marks, tattoos | | Retina/iris scans | |
| Voice recording/signatures | | Vascular scan | | Dental profile | |
| Other distinguishing features/biometrics (specify): | | | | | |

| System admin/audit data | | | | | |
|---|---|---|---|---|---|
| User ID | | Date/time of access | | ID files accessed | |
| IP address | | Queries run | | Contents of files | |

3.2. Indicate the sources of the information in the system (e.g., individual, another agency, commercial sources, etc.) and how the information collected from stated sources (paper form, webpage, database, etc.).[5]

| Directly from individual about whom the information pertains | | | | | |
|---|---|---|---|---|---|
| In person | ✖ | Hard copy: mail/fax | | Online | |
| Telephone | | Email | | | |
| Other (specify): | | | | | |

| Government sources | | | | | |
|---|---|---|---|---|---|
| Within the Component | | Other CSOSA components | | Other federal entities | |
| State, local, tribal | | Foreign | | | |
| Other (specify): | | | | | |

| Non-government sources | | | | | |
|---|---|---|---|---|---|
| Members of the public | | Public media, internet | | Private sector | |
| Commercial data brokers | | | | | |
| Other (specify): | | | | | |

3.3. Where will the PII be stored in the system?

*The PII is stored in the system application database in a computer housed in the agency's secured computer room.*

[5] Examples include form filling, account verification, etc.

3.4. Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exists in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.).

*Risk is a function of threats, vulnerabilities, likelihood, controls in place, and impact. Threats to confidentiality may include intentional or unintentional unauthorized disclosure of the first and last names of the individuals who have entered their names into the system for check-in purposes. The choice was made to collect the first and last name, and no other information to be collected because there is no need for any other information to make staff aware of the individual's presence for an appointment.*

**Purpose and Use of the System**

3.5. Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

*The purpose of collecting the PII is to identify the client to the CSOSA staff notifying them of the client's arrival; generate a sign in sheet for the group, training or activity that the client participates in at the MLK site. The PII collected is proof of attendance.*

3.6. Select why the information in the system is being collected, maintained, or disseminated.

| **Purpose** | | | |
|---|---|---|---|
| For criminal law enforcement activities | | For civil enforcement activities | |
| For intelligence activities | | For administrative matters | |
| To conduct analysis concerning subjects of investigative or other interest | | To promote information sharing initiatives | |
| To conduct analysis to identify previously unknown areas of note, concern, or pattern | | For administering human resources programs | |
| For litigation | | | |
| Other (specify): ***See Section 1 subsection 1.2*** | | | |

**Social Security Numbers**[6]

3.7. Does they system collect Social Security Numbers? If so, explain the purpose of its collection, type of use, and any disclosures.[7]

*No.*

3.8. Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

*N/A*

## 4. Notice

4.1. How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

*A posted paper notice will be placed within eyesight of the kiosk and of the individual entering his or her name for check-in if/until the same notice can be made available on the iPad/Kiosk prior to entering the client's name into the interface*

4.2. Provide the text of the notice, including where it can be found, or the link to the webpage where notice is posted.

*"Please enter your first and last name and choose the appropriate reason for your visit. The information entered will be used to advise appropriate CSOSA staff of your presence and purpose for presence at this facility and in accordance with your supervision requirements. For more information related to CSOSA's privacy policy, please visit www.csosa.gov.*

4.3. What opportunities are available for individuals to consent to uses, decline to provide information, or opt-out of this system/project?

*A client can refuse to input his/her name. If a client does not understand how to use the system, with the client's permission, the staff person at the reception's desk can input the client's name for him/her. If the client declines the use of the check-in system, the staff person at the receptionist will ask the client his/her name and notify, via phone or email, the appropriate staff person that the client has arrived.*

[6] In order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by the law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

[7] In accordance with OMB Regulations, please note if the system collects SSN, the PIA will require a signature by the Assistant Secretary or equivalent.

## 5. Information Sharing

### Internal

5.1. How do agency personnel gain access to the system and the PII (e.g., users, managers, system administrators, developers, contractors, etc)?

*Designated CSOSA staff, Community Supervision Officers, and Vocational Training staff located at the Martin Luther King, Jr. community supervision site are to complete a computer access form. A separate login and password are required for this system. Staff are required to be cleared by the Office of Security; have management approval; and adhere to all agency network access policy.*

5.2. Will information be shared internally with other CSOSA program offices and/or components, if so, which ones?

*Community Supervision Services (CSS) and Community Justice Programs management staff at Martin Luther King, Jr. community supervision site will determine who has access to the system and the PII.*

5.3. What information will be shared and with whom?

*The information will not be shared with anyone or any entity outside of CSOSA unless as required by law. The information may be shared within CSOSA for case management, research and evaluation, human resources performance management, and Information Technology (IT) support and troubleshooting purposes.*

5.4. How will the information be shared?[8]

*The information may be shared electronically by internal email, secure internal database connection (e.g., internal security policy controlled), secure extract remaining within CSOSA network (e.g., password protected spreadsheet).*

5.5. What is the purpose of sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

*The information may be shared within CSOSA for case management, research and evaluation, human resources performance management, and IT support and troubleshooting purposes. Yes.*

5.6. Describe controls that the program offices and/or components have put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information.

[8] Examples, include but is not limited to, case-by-case, direct access, e-mail, etc.

*CSOSA has policies in place to oversees network access to all agency systems. Policy*
*CSOSA IT Security Policy PS2036*
*OIT Operating/Management Instructions*
*Personal Identification Information (PII) and Social Security Number (SSN) Usage Review and Reduction MI2059*
*Instruction for Personally Identifiable Information (PII) Data Extracts for CSOSA Business and Mission Critical Systems MI2062*
*Breach Notification Standards and Procedures for CSOSA Business and Mission Critical Systems MI2058*
*Personal Identification Information (PII) and Social Security Number (SSN) Usage Review and Reduction MI2059*
*Access Controls OI OIT-2014-01-1*
*Personnel Security Controls OI OIT-2014-13-1*

5.7. Is the access to the PII being monitored, tracked or recorded?

*All systems are subject to operational and security network monitoring for issue, errors, etc.*

**External**

5.8. Will the information contained in the system be shared with external entities (e.g. another federal agency, District of Columbia agency, etc.)?

*No.*

5.9. What information will be shared and with whom?

*N/A*

5.10. What is the purpose of sharing the specified information with the specified external entity? Does this purpose align with the stated purpose in Question 1.2 above?

*N/A*

5.11. How is the information accessed and used by the external entity?

*N/A*

5.12. What controls are in place to minimize risk and protect the data?

*N / A*

5.13. Is the external information sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

*N/A*

## 6. Consent and Redress

6.1. How will individuals be notified if there are any changes regarding how their information is being collected, maintained, or disseminated by the system?

*Through a posted notice, the client will understand that the system is used to inform appropriate staff that they are present to see their Community Supervision Officer and/or to attend classes and groups activities.*

6.2. What are the procedures that will allow individuals to access their own information?

*The only information that is "their own" is their first and last name. The individuals will not have access to the information electronically, as this is not a system that maintains any account or other information. The client may request a printout of their first and last name.*

6.3. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

*The system only collects clients first and last names. Clients may alert staff of name changes the assigned CSO will alert the agency's Office of Information Technology to make the change in the check in system.*

6.4. How does the project notify individuals about the procedures for correcting their information?

*N/A*

6.5. How will individuals have the opportunity to consent or dissent to particular uses of the information?

*The posted notice will explain that to advise CSOSA staff of their presence for a meeting or appointment, they are to enter their name in the Kiosk. It is then implied by entering their first and last name that they have consented.*

6.6. How will the agency provide notice to individuals that their PII information may be shared with other agencies or entities (both internal and external)?

N/A

## 7. Information Security and Safeguards[9]

7.1. Does the component office work with their Chief Information Officer (CIO) to build privacy and security into the system and build privacy extension to the extent feasible?

*Yes.*

7.2. Do contractors have access to the system?

*No.*

7.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

*CSOSA IT Security policy on least privilege governs this control. The policy requires that access and levels of access control to systems and information will only be granted to the extent necessary to operate or maintain a system, commensurate with a staff member's job requirements and duties.*

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

*All CSOSA users of the system must first have network access. This access is granted after completing the security clearance process. Users must complete a Computer Access form which must be signed by the manager and Access to the system. Elevated privilege requires signature, management and security. CSOSA personnel, systems, and processes comply with National Institute of Standards and Technology (NIST) 800-53 controls which include administrative, technical and physical controls. These controls are in place to ensure integrity, availability, accuracy and relevancy of the data and to mitigate privacy risks.*

7.5. Is an Authority to Operate (ATO) required? Has one been granted?

*No, other than the Commercial Off The Shelf (COTS) application, all components server, endpoints, configurations) are part of the CSOSA Enterprise System which has an existing ATO.*

7.6. Is the system able to provide an accounting of disclosures?

*No.*

7.7. What controls are in place to prevent the misuse (e.g., browsing) of data by authorized

[9] If you are unsure which safeguards will apply, please consult with CSOSA's Information Security Officer.

users who have access to the data?

*CSOSA IT Security Policy.*

7.8. Is there a way to identify unauthorized users? If so, what controls are in place to prevent a data breach?

*Yes, CSOSA IT and IT Security offices have multiple tools to identify unauthorized users.*

7.9. Does the agency provide annual security and privacy training for agency employees and contractors?

*Yes.*

7.10. Who is responsible for assuring safeguards for PII in the system?

*The Agency's Senior Agency Official for Privacy (SAOP) has agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirement and managing privacy risks. Many of the requirements established by law and mandated by the Office of Management and Budget to protect the rights of individuals whose PII is collected, maintained or shared on the system are shared with the Agency's Office of Information Technology's Chief Information Officer and the Agency's Chief Information Security Officer.*

7.11. How will owners of the PII be harmed if privacy data is unlawfully disclosed?

*Owners of the PII would be minimally harmed. The Check-In system captures only the first and last names, time checked in, intended program to attend or the CSOSA staff member who the client is scheduled to meet.*

7.12. If contractors have access to the system, has the agency provided the contractor, who works on the system, a confidentiality agreement or a Non-Disclosure Agreement (NDA)?

*N/A. There are no contractors involved.*

7.13. What other IT security measures has the agency implemented to protect PII in the system?

*CSOSA IT Security Policy, CSOSA IT Security annual assessments and audits, and IT Security tools.*

## 8. Auditing and Accountability

8.1. How does the system owner ensure that the information is used in accordance with the stated practices in this PIA?

*CSOSA requires staff to follow and adhere to agency policy, including those stated in section 5.6.*

8.2. What are the privacy risks associated with this system and how are those risks mitigated?

*Risk is compromise to confidentiality of first and last name associated with attendance at CSOSA. All CSOSA users of the system must first have network access. CSOSA personnel, systems, and processes comply with National Institute of Standards and Technology (NIST) 800-53 controls for which include administrative, technical and physical controls. These controls are in place to ensure integrity, availability, accuracy and relevancy of the data and to mitigate privacy risks.*

## 9. Data Quality and Integrity

9.1. How will the information that the agency collects be verified for accuracy and completeness when it is entered into the system?

*Once the client checks into the system, the assigned person receives a notification. It is the responsibility of the assigned person (e.g., CSO, group facilitator, Illegal Substance Collection Unit designee) to verify the accuracy of the PII using photos and other information in the agency's Supervision and Management Automated Record Tracking System (SMART).*

9.2. Are there any privacy risks for individuals whose information is collected or used by the project that relate to data quality and integrity? If so, how will CSOSA mitigate these risks?

*No.*

## 10. Privacy Policy and Statement

10.1. Has the agency provided a privacy statement or policy for this system and is it provided to all individuals whose PII is collected, maintained or stored?

*Yes, all clients will be advised the Agency’s privacy statement by notice at the iPad kiosk.*

10.2. Is the privacy policy publicly viewable? If so where?

*Yes. The agency's privacy policy is located on the agency's website at www.csosa.gov.*

## Authorizing Signatures

This Privacy Impact Assessment has been conducted by Community Supervision Services and has been reviewed by Mahala Dar, the Senior Agency Privacy Official, for accuracy.

Frank Lu

System Owner Name (Please Print)

10/2/2017

X Frank Lu

Frank Lu
Service Development Director
Signed by: FENG LU

System Owner Signature Date

Mahala Dar

Chief Privacy Officer Name (Please Print)

/S/ September 7, 2017

Chief Privacy Officer Signature Date

SHEILA STOKES

General Counsel (Please Print)

Sheila

General Counsel Signature 10/12/2017

Date