Court Services and Offender Supervision Agency (CSOSA)

Sex Offender Registry for the District of Columbia (SOR)
Privacy Impact Assessment

CONTROLLED UNCLASSIFIED INFORMATION

April 26, 2023

Office of Community Supervision and Intervention Services
Court Services and Offender Supervision Agency
300 Indiana Avenue, NW, Washington, DC 20004

POINTS OF CONTACT for Sex Offender Registry

Program Office Point of Contact: **Name: Kaitlin Forsha** **Title: Branch Chief** **Office: CSOSA Sex Offender Registration** **Phone: 202-585-7314 Room 872** **Bldg./Room: 633 Indiana Ave., 8th Floor** **Email: Kaitlin.Forsha@csosa.gov**	**System Owner Point of Contact:** **Name: Frank Lu** **Title: Service Development Director** **Office: OIT** **Phone: 202-585-7902** **Bldg./Room: 800 North Capitol St** **Email: frank.lu@csosa.gov**
Privacy Program Manager: **Name:** **Office:** **Phone:** **Bldg./Room:** **Email:**	**Senior Agency Official for Privacy:** **Name: Shelia Stokes** **Office: Office of the General Counsel** **Phone: 202-220-5797** **Bldg./Room: 800 N. Capitol Street, NW** **Email: Office of the General Counsel**

THIS PAGE IS FOR INTERNAL ROUTING PURPOSES AND DOCUMENTATION OF APPROVALS. UPON FINAL APPROVAL, COMPONENTS SHOULD REMOVE THIS PAGE PRIOR TO PUBLICATION OF THE PIA.

Overview of Sex Offender Registry for the District of Columbia (SOR)

The Court Services and Offender Supervision Agency (CSOSA) core mission is to effectively supervise adults under our jurisdiction, to enhance public safety, reduce recidivism, support the fair administration of justice, and promote accountability, inclusion and success through the implementation of evidence-based practices in close collaboration with our criminal justice partners and the community.

The Sex Offender Registration Act (SORA) of 1999 ("the Act," D.C. Law 13–137, D.C. Official Code § 22–4001 *et seq.*) delegates the responsibility for the design, development, enhancement, and maintenance of the Sex Offender Registry (SOR) for the District of Columbia (DC) to CSOSA. CSOSA is responsible for operating SOR (the electronic application), all electronic interfaces of SOR data to other systems, as well as the processes, procedures, and authorized staff members for working with offenders required to register, including collecting, maintaining, and updating data in SOR. The Sex Offender Unit at the Metropolitan Police Department (MPD) also has a role in collecting, maintaining, and updating specific pieces of data in SOR.

The SOR is currently in operation and this new Privacy Impact Assessment (PIA) is necessary to provide information regarding the SOR and the collection and use of Personally Identifiable Information (PII).

1. Description of the System

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

System Name: Sex Offender Registry for the District of Columbia (DC).
System Acronym: SOR
Brief description of major functions: The SOR system provides the user interface, database, document management and electronic interfaces required to collect, manage, maintain and share required information on convicted sex offenders who reside, are employed, and/or attend school in DC and are required to register.

SOR (electronic system) is operated, supported, and maintained by CSOSA. Information on offenders in SOR is taken from original source documents as much as possible. CSOSA and MPD staff members collect, enter and maintain sex offender information in the system (personal, offense, registration, supervision, physical description and photos, residence, employment, school, vehicles, driver's license, and fingerprints). The vast majority of data in SOR is manually entered. CSOSA electronically interfaces the National Crime Information Center (NCIC) number from NCIC/National Sex Offender Registry (NSOR) (NCIC is the system of record);

the confirmation of a valid DC address from the Office of the Chief Technology Officer (OCTO) Government Information System (GIS) for the City of DC (the source system for addresses, Police Serving Area (PSA), latitude and longitude); and, if the offender is also under supervision at CSOSA, the assigned supervision officer and the officer's supervisor from CSOSA's Supervision & Management Automated Record Tracking (SMART) system. SMART is the system of record for supervision information. The information on offenders who transfer in from another jurisdiction/state is also confirmed against the source documents.

Data collected and maintained in the SOR system is limited to information required by law and regulations (to include information required for electronic interfaces). Information that is posted to the DC and National Sex Offender Public websites is limited to the information approved in DC law and regulations.

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

The collection and use of PII is necessary for CSOSA to carry out the legal requirements and mission of the SOR for DC, which include:

- Proper identification of a sex offender within DC, including the sharing of relevant data with other law enforcement partners and systems that support the administration of justice within DC;
- Data exchanges with mandatory national systems such as NCIC/NSOR and National Sex Offender Public Website (NSOPW);
- Periodic verification of the addresses at which the sex offender lives, resides, works, and/or attends school, and information about the appearance of the sex offender (e.g., height, weight, eye color, hair color, and other physical descriptors);
- Reporting of any changes of address and any other changes in registration information (including changes in appearance);
- Data exchanges with other jurisdictions if the sex offender is moving into DC, resides, works or attends school in another jurisdiction concurrent with DC (multi-jurisdiction registration required); and/or notification that an offender is leaving the DC jurisdiction and relocating to another jurisdiction;
- Complying with the requirements of the DC Sex Offender Registration Act (SORA), DC Municipal Regulations (DCMR) and Code of Federal Regulations (CFR) relevant to sex offender registration in DC, and any procedures, requirements, rules, or regulations promulgated under SORA, DCMR and CFR relevant to sex offender registration in DC.

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

No. This system is currently in operation.

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

This PIA is new.

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

The system is operated by CSOSA (the agency). The system is supported and maintained by CSOSA human and technical resources (hardware, software, code, network, servers, and interfaces). CSOSA and MPD staff members collect, enter and maintain sex offender information in the system. All staff members who enter and maintain data are employees of CSOSA or MPD. The CSOSA staff members who maintain the SOR application and database are employees. There are contractor staff members on the CSOSA Infrastructure and CSOSA Information Security Teams who do have access to the servers and the network, however they do not add or update data, only monitor and maintain the servers and operating systems.

2. Legal Authorities and Other Requirements

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

The main legal authorities for sex offender registration are:

- Sex Offender Registration Act of 1999, D.C. Law 13–137, **D.C. Official Code § 22–4001 *et seq.*** Sex Offender Registration and Notification Act (SORNA),Title 1 of the Adam Walsh Child Protection and Safety Act of 2006, 34 U.S.C. § 20901 *et. seq*.

CSOSA execution of sex offender registration functions is authorized by:

- Section 166(a) of the Consolidated Appropriations Act, 2000 (Pub. L. 106–113, sec. 166(a), 113 Stat. 1530; D.C. Official Code § 24–133(c)(5))
- Further authorized by the Sex Offender Registration Act (SORA) of 1999 (D.C. Law 13–137, D.C. Official Code § 22–4001 *et seq.*).
- Chapter 4 of Title 6A, District of Columbia Municipal Regulations (6A DCMR 400 *et. seq.*).
- Code of Federal Regulations, Title 28, Part 811, Sex Offender Registration, 28 CFR § 811.1 *et. seq.*

System to system interfaces are governed by the authorities listed above, operating manuals, and/or Memorandums of Understanding between CSOSA and the other organization. Because the system to system interfaces are to share SOR data with other systems, system interfaces are built in compliance with the operating manuals and guidance provided by the receiving agency (i.e., MPD, Federal Bureau of Investigations (FBI), Department of Justice (DOJ)).

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.

Information in SOR is retrieved by a name and personal/unique identifiers, which require the system to be covered under a Privacy Act System of Records Notice (SORN). The SORN is published at 67 FR 51, CSOSA-18. https://www.govinfo.gov/content/pkg/FR-2002-03-15/pdf/02-6092.pdf

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.

Yes, an approved NARA records retention schedule exists for the records contained in SOR. The approved schedule and records disposition number is DAA-0562-2013-0022.

Offenders Classification A – Cutoff when case is closed (upon offender's death, reversal, vacation of pardon). Destroy 6 months after cutoff.

Offenders Classification B and C – Cutoff when case is closed (upon expiration of offender's supervision, or 10 years after the offender is placed on supervision, whichever is later, or upon reversal, vacation or pardon).

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

When authorized by the CSOSA Sex Offender Registration Unit, system records are "logically deleted" by staff members in the CSOSA Office of Information Technology (OIT) (can be viewed and/or recovered by a database administrator) due to the identification of a duplicate record, or a mistake in data entry.

Sex offender records closed in the system due to completion of the period of registration, death, a determination that the offender is not required to register, reversal of the conviction or other similar situation remain in the SOR database in a closed status as required by the records retention schedule. Paper files associated with these offender records are separated from paper files of active offender records and kept in a specific area in the secured file room. CSOSA executes manual procedures to dispose of records in a timely manner, in accordance with the records disposition schedule.

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 of appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.).

Potential threats to privacy as a result of the collection and use of information, and controls that CSOSA has put into place to ensure that the information is handled, retained and disposed of appropriately are:

- Collection of inaccurate information: The CSOSA Sex Offender Registration Unit uses original documents (e.g., documents completed by the offender, Sentencing documentation from the Courts, documents from other jurisdictions, written classification determinations from the CSOSA Office of General Counsel (OGC), etc.) as the source for entering, maintaining and updating information in SOR. A minimum amount of data is electronically captured in SOR from the designated/approved system of record at NCIC (sends assigned NCIC #), OCTO (data is open source to provide DC addresses), or CSOSA (for case assignment).
- Mistakes in data entry: The CSOSA Sex Offender Registration Unit has a system of second party checks that require another staff member use the original documents to review and confirm the data was correctly entered and/or updated in SOR. The CSOSA Sex Offender Registration Unit is also required to perform continuous NCIC data validations to confirm the information in SOR matches the information in NCIC/NSOR. Staff members in the MPD Special Investigations Branch are required to approve information to be posted to the DC Sex Offender Public Website (DC SOPW), including updates to offender information.
- Exposure of PII to unauthorized persons:
    - The CSOSA Sex Offender Registration Unit maintains paper records (the source documents), which are required to be secured in an employee's desk or in the unit's secured file room when not in use. Access to the secured file room is granted only to certain agency staff via their agency-issued badge. During the NCIC Audit (every 3 years), the paper files are pulled and used during the audit. The unit's fax machine is housed within the file room so documents that are faxed to CSOSA are secured until staff are able to retrieve them. Reports are limited and are normally used on-line (only) by authorized, authenticated staff members for planning or preparing management/statistical reports that do not contain PII or offender level details.
    - Staff Training: Staff members at CSOSA are required to complete Records Management, Privacy Awareness, Ethics, and Information Security Awareness training on a periodic basis. This training reinforces the need to protect all information, including PII, from unauthorized access or misuse.
- Collection of extraneous information: The PII collected in SOR is limited to what has been authorized in law, regulations (SORA, DCMR, CFR) and policy. The law and regulations were continuously reviewed during system design and development to verify that the proposed PII was only collected in accordance with law and regulations.
- Vulnerabilities in system access and exchanges: CSOSA employs Federal Government standard/approved technical controls to ensure data is protected while stored and exchanged in the SOR. CSOSA manages internal access by assigning roles based on need; enforcing password strength requirements; authenticating access; logging access at the application, database and server levels; and use of firewall rules to limit data exchanges to approved systems.

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.

Identifying Numbers					
Social Security	X	File/Case ID		Financial Account	
Taxpayer ID		Driver's License	X	Financial Transaction	
Employee ID		Credit Card			
Other identifying numbers (please specify): CSOSA ID, PDID, DCDC, FBI #, NCIC #					

General Personal Data					
Name	X	Date of Birth	X	Religion	
Maiden Name		Place of Birth	X	Financial Information	
Alias	X	Home Address	X	Medical Information	
Gender	X	Telephone Number	X	Military Service	
Age		Email address		Physical Characteristics	X
Race/Ethnicity	X	Education	X		
Other general personal data (specify): For Place of Birth – SOR currently captures and saves Country of Birth. Education, as in highest level achieved, is not tracked in SOR. School information for offenders attending school is tracked in SOR (Name of school, address, start date, end date, and point of contact name and phone number). There is no field in SOR that indicates the offender has a GED, BA, BS, MBA, etc.					

Work-related Data					
Occupation	X	Telephone number	X	Salary	
Job title	X	Email address		Work history	
Work address	X	Business associates	X		
Other work-related data (please specify): In SOR for employment: SOR captures whether employed or not employed; whether the employment is primary, secondary, or non-paid/volunteer; start date; end date; organization name and address; whether the organization is a school; the position; and point of contact name and phone number.					

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

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	
IP address	X	Queries run		Contents of files	X
Other system admin/audit data (please specify):					

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

Directly from individual about whom the information pertains					
In person	X	Hard copy: mail/fax	X	Online	X
Telephone	X	Email	X		
Other (please specify): Any information provided via email is confirmed against some type of source documentation (e.g., attachment to the email, hard copy documents already on file, or documents from other Jurisdictions). Authorized staff members do use other government agency systems, for example NCIC/NSOR, for review and validation of collected and shared information.					

Government Sources					
Within the Component	X	Other CSOSA components	X	Other federal entities	X
State, local, tribal	X	Foreign			
Other (please specify):					

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

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

Once saved, the non-PII and PII data is stored in the SOR database which runs on a separate server on-premise in the agency's data center. No data is "stored" (meaning saved) in the application.

Documents may contain additional PII. Initially, documents are scanned in and stored in file folders on a secured shared drive. A C# console app, which is used as a pass-through application only, retrieves the documents and copies them to the same server as the SOR database where they are stored. This C# App does not save any data. The SOR application has a user interface that allows authorized, authenticated users to view the scanned documents.

Initially, photos (head and upper body) are uploaded to file folders on a secured shared drive. An app retrieves the photos and copies them to the same server as the SOR database where they are stored. The SOR application has a user interface that allows authorized, authenticated users to view the photos.

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 exist 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.).

The potential threats to privacy that exist in light of the information collected, and the choices that CSOSA made in regards to the type or quantity of information collected are:

- Collection of extraneous information or extraneous PII: Data collected and maintained in the SOR system, including PII, is limited to the data authorized by law and regulations, or required to execute mandatory data exchanges. Information that is posted to Sex Offender Public Websites is covered by law and regulations. When a request to collect new/additional information is made, the request is reviewed against the law and regulations, reviewed as to whether the information is necessary to register an offender (e.g., substance abuse information that is needed to successfully supervise an offender on probation/parole/supervised release is not needed to register an offender), and forwarded to OGC for final review before any system development action is initiated.

The potential threats to privacy that exist in light of sources from which information is collected, and the choices that CSOSA made in regards to the sources of information are:

- Inaccurate or incomplete information from the offender: Sex offenders are required to provide complete and accurate information with his/her signature as verification that the information being provided is accurate. The quarterly/annual verification process requires the sex offender to appear in person at the CSOSA Sex Offender Registration Unit and confirm and/or update the information.
- Incorrect information from MPD: MPD staff members are responsible to verify, update and maintain data in less than 15 fields in SOR. These are fields where MPD staff members would have the information and/or the best access to the information: Police Servicing Area, victim, whether a warrant has been issued, and aliases known to MPD.
- Incorrect information from other Jurisdictions: CSOSA requires the source documents from other Jurisdictions so that all information can be verified, and OGC can determine the correct DC SOR Classification (A, B, C) for the offender.

- Extraneous information interfaced in from other systems: Minimal data is electronically interfaced into SOR from other systems. Those systems are the System of Record for the information being interfaced in. CSOSA electronically interfaces in the National Crime Information Center (NCIC) number from NCIC/National Sex Offender Registry (NSOR); the confirmation of a valid DC address (address only) from the OCTO GIS for the City of DC; and, if the offender is also under supervision at CSOSA, the assigned supervision officer and the officer's supervisor from CSOSA's SMART system.
- Collection of information required solely for matching offender information in local and national sex offender databases: The identifiers are limited to those that best serve the purpose for matching data between systems (Social Security Number, FBI Number, NCIC Number), or as required by law and/or regulation.

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.

Staff members at CSOSA and MPD use the information in SOR to achieve the purpose in the response to Question 1.2:

- Review, update and maintain the information in SOR to properly identify a sex offender during the registration and quarterly/annual verification processes (to confirm that the offender is who he/she says he/she is and is the person who is presenting him/herself for registration, information update, and/or verification).
- Review and update the information in SOR to properly identify a sex offender who is not in compliance with the sex offender registration requirements so that the offender can be correctly identified/found and steps taken to bring the offender into compliance.
- Review the information in SOR to maintain awareness of the location and presence of registered sex offenders in the community, and to provide authorized information to the public as to registered sex offenders that live, work and/or attend school in and around their communities.
- Collect and use the information in SOR to meet legal requirements, rules, or regulations as promulgated under the DC SORA, DCMR and CFR relevant to sex offender registration in DC.

The SOR interfaces/exchanges offender information, including some PII, in order to:

- Correctly match offender information in the SOR system with information on the same person in other local and national systems as required by law (MPD, SORNA Exchange Portal, NSOPW, NCIC/NSOR).
- Notify other jurisdictions if the sex offender resides, works or attends school in another jurisdiction in addition to DC (multi-jurisdiction registration required); and/or notification that an offender is leaving the DC jurisdiction and relocating

to another jurisdiction; and/or to notify another jurisdiction that the offender has relocated to DC and has registered, or has not registered or reported by the expected date.

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

Purpose			
For criminal law enforcement activities	X	For civil enforcement activities	
For Intelligence activities		For administrative matters	X
To conduct analysis concerning subjects of investigative or other interest	X	To promote information sharing initiatives	X
To conduct analysis to identify previously unknown areas of note, concern, or pattern		For administering human resources programs	
For litigation			
Other purpose (please specify):			

Social Security Numbers

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

Yes, the system captures and maintains social security numbers. Code of Federal Regulations, 28 C.F.R. § 811.7 details the SSN requirement and the information obtained during initial registration. Due to the purpose of the system (see response to Question 1.2), which includes data sharing with local and national systems as required by law (MPD, SORNA Exchange Portal, NSOPW, NCIC/NSOR), as well as making information concerning sex offenders available to other law enforcement and governmental agencies as appropriate (often done in support of locating or gaining compliance from non-compliant sex offenders), it was determined that SSN is a key universal identifier to validate that data on a sex offender is being correctly matched with data on the same sex offender in other systems maintained by other jurisdictions and nationally (U.S. Marshal Service, National Center for Missing and Exploited Children), or assist with locating non-compliant offenders. Other identifiers, such as PDID or CSOSA internal ID numbers, are not known or used by other Jurisdictions or at a national level.

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

No alternatives were considered in the collection of SSN because of the need for a universal identifier to correctly match data on the same sex offender in other systems, or assist with locating non-compliant offenders.

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.

The Privacy Act Statement is included on forms that are extracted from the system for offenders to complete as well. The SOR system does not notify sex offenders about the collection of PII because sex offenders do not have direct or indirect access to the SOR (system). However, offenders are notified of the collection of data as part of the initial registration process. Any notifications in the SOR system are for authorized, authenticated CSOSA and MPD staff member use. A Privacy Act Statement is added to the front screen of SOR to remind authorized users of information being in a system of record.

CSOSA staff members who collect and maintain the information in SOR provide notice to the individuals about the information being collected through the use of forms and other documents:

- At Initial Registration:
  - As part of the initial registration process, the CSOSA staff members are required to provide the text of the District of Columbia Sex Offender Registration Act and the Rules for implementation of the Act (6A DCMR Chapter 4, 6A DCMR 400 *et. seq.*) to the sex offender. The sex offender signs the Initial Registration form indicating that these have been provided/received. These documents explain the offender's duties and responsibilities, the role of MPD, the role of CSOSA, and the responsibilities of CSOSA regarding sex offender registration.
  - The Initial Registration form allows the offender to review the information collected (Offense, Home, Work and School Addresses, Motor Vehicles, Date of Birth, and Driver's License) and entered in SOR for initial registration. The offender must sign the form verifying the information is correct. That same form contains language as to the duties and responsibilities of the sex offer to report/update (1) changes of home, work or school addresses, (2) any change in motor vehicle information, or (3) any significant changes in physical appearance to CSOSA within three (3) days of the change, as well as the requirement for quarterly or annual verification of information.
- At Quarterly/Annual Verifications:
  - Depending on the offender's Classification, the offender is required to report in person quarterly or annually to the CSOSA Sex Offender Registration Unit. The Verification form (paper form) is used to collect information from the offender regarding home, work or school addresses, vehicles owned, and driver's license information. The form is manually

completed by the offender. The offender must sign the form verifying the information is correct. That same form contains language as to the duties and responsibilities of the sex offender to report/update: (1) changes of home, work or school addresses, (2) any change in motor vehicle information, or (3) any significant changes in physical appearance to CSOSA within three (3) days of the change, as well as the requirement for quarterly or annual verification of information.

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

Authority: National Capital Revitalization and Self-Government Improvement Act of 1997, Pub. L. 105–33, sections 11231–11234 and sections 11271–11280 as amended by the District of Columbia Appropriations Act, 2000, and the District of Columbia Sex Offender Registration Act of 1999, 24 DC Code Sections 1117–1137.

Purpose: Pursuant to delegation by Congress, the Court Services and Offender Supervision Agency will exercise the powers and functions for the District of Columbia relating to sex offender registration as provided in the District of Columbia Sex Offender Registration Act of 1999.

Routine Use: Information may be disclosed for any of the Routine Uses listed below:

A. Disclosure may be made to a congressional office or DC City Council member when the member or staff requests this information on behalf of, and at the request of, the individual who is the subject of record.

B. Information may be disclosed to any civil or criminal law enforcement agency, whether Federal, state, or local or foreign, which requires information relevant to a civil or criminal investigation.

C. To any source from which information is requested in the course of an agency investigation, to the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation and to identify the type of information requested.

D. To the appropriate Federal, state, local, foreign or other public authority responsible for investigating, prosecuting, enforcing or implementing a statute, rule, regulation, or order where CSOSA becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.

E. To provide information source for contract or treatment facilities who provide services to offenders under CSOSA supervision to the extent necessary to accomplish their assigned duties.

F. To provide information relating to DC defendants to Federal, local and state courts, court personnel, pretrial, parole and/or probation officials to the extent necessary to accomplish their assigned duties.

G. To provide information to Federal, state and local law enforcement agencies responsible for monitoring, enforcing and/or implementing a Federal, state or local statute or regulation related to sex offenders.

H. A record may be disclosed to the National Archives and RecordsAdministration for use in records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

I. For Litigation: To disclose information to the Department of Justice for the purpose of representing CSOSA, or its components or employees, pending or potential litigation to which the record is pertinent.

J. For Judicial/Administrative Proceedings: To disclose information to another Federal agency, a court, grand jury, or a party in litigation before a court or administrative proceeding being conducted by a Federal agency, when the Federal Government is a party to the judicial or administrative proceeding.

K. For Data Breach and Mitigation Response:

- To provide information to appropriate agencies, entities, and persons when (1) the CSOSA suspects or has confirmed that there has been a breach of the system of records; (2) the CSOSA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the CSOSA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the CSOSA's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

- To provide information to another Federal agency or Federal entity, when CSOSA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach, or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

Disclosures: Disclosure of information by a convicted sex offender who is required to register is mandatory. Failure to comply with any provision of the Sex Offender Registration Act is a criminal offense punishable by a fine of not more than $1,000, or imprisonment for not more than 180 days, or both. Failure to comply where there is a prior conviction in any other jurisdiction for failing to comply with the requirements of a sex offender registration program, is punishable by a fine of not more than $25,000, or imprisonment of not more than 5 years, or both.

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

At initial registration, for offenders convicted in another jurisdiction, if the offender believes the registration classification determination is inaccurate, the CSOSA Sex Offender Registration Unit staff member will provide the registrant with the case number of the sex offense conviction and instructions for contacting the sentencing Court to address the concerns regarding sentencing conviction.

At initial registration, if the registrant has a concern with registering in DC, they are given the packet to challenge and seek Judicial Review with the D. C. Superior Court and, if an attorney is needed, the Public Defender Service's contact information. The individual must follow the dispute resolution procedures in District of Columbia Superior Court, set forth in the DC Code. Any information already entered in SOR will be marked as "Pending – Judicial Review" and be held until the DC Superior Court has made a final determination, or the waiting period (30 days) has expired. Depending on the outcome, the information in SOR will be updated to reflect any changes to the registration information (e.g., classification, duration of registration period, mark the case as closed if the offender is found not required to register).

Once it has been determined the individual must register as a sex offender, there are no opportunities for the offender to decline to provide information, or opt out of SOR. Sex offenders complete registration and verification paperwork themselves to ensure the accuracy of the reported information, and that they understand the duties and responsibilities of a registered sex offender. For sex offenders who are unable to read or write, a CSOSA Sex Offender Registration Unit staff member will complete the paperwork for them and verbally review the information for accuracy. Offenders sign the forms to document that information is complete and accurate, and to confirm his/her understanding of the duties and responsibilities of a sex offender specifically for updating address, vehicle and appearance information.

The penalties for not complying with the duties and responsibilities of sex offender registration are severe. Those penalties are listed on both the Initial Registration Form and Verification Form. At the time of quarterly/annual verification, the offender is required by law and regulation to provide the information, as well as reconfirm his/her understanding of his/her duties and responsibilities regarding maintaining/updating changes of home, work or school addresses; any change in motor vehicle information; and/or any significant changes in physical appearance, as well as the quarterly/annual verification process.

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.)?

CSOSA requires that CSOSA and MPD staff members who need to gain access to the SOR system submit a CSOSA computer access form. That form is reviewed by a CSOSA staff member who is responsible for system access. Once approved, the staff member creates a ticket for the CSOSA Customer Support group to create the network account (username and password). Once the network account is created, if the individual requires access to SOR, a separate ticket with the specific SOR network access group is created. Once the individual's username is added to the approved SOR network access group, the individual has access to the SOR system.

There are 3 distinct network access groups for the SOR System:

- SORU - this network access group provides data entry, update and limited delete access to the information in SOR, including the PII. Staff assigned to the CSOSA Sex Offender Registration Unit, and their direct supervisors are assigned to this network access group.
- MPD - this network access group provides limited data entry and update access to the information in SOR. This group has read only access to the remainder of the information in SOR, including the PII. MPD staff members assigned to the MPD Special Investigations Branch are assigned to this network access group. There is a general Memorandum of Understanding (MOU) regarding data sharing between CSOSA and MPD. SOR data is specifically referenced on the MOU on page 5, item 13.
- CSO – this network access group provides read only access to the information in SOR, including the PII. Supervision staff, their supervisors, and other management level staff at CSOSA are assigned to this network access group.

The SOR System Administrators, Database Administrators and Developers are the same staff member at CSOSA. This person has local administrator rights to the servers in order to install the application, install the database software and database, make changes to the application code, manage the interfaces, configure the software, and troubleshoot problems and issues. A limited number of data changes are performed directly in the database by this staff member. The CSOSA Project Manager for SOR has access to the application and data through the admin network access group. The Project Manager serves as a control point to assist with troubleshooting and fixing issues, approving changes to the application and database, testing, and documentation.

The CSOSA Infrastructure and Information Security Teams have admin rights to all servers, including the servers that the SOR system runs on, to perform backups, troubleshoot network issues, bring servers off and on-line, ensure security controls are working properly, and perform other tasks.

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

Yes, information is shared internally with other CSOSA program offices and/or components:

- Information is shared by CSOSA Sex Offender Registration Unit staff members with:
  - The Office of General Counsel (OGC).
  - If the sex offender is supervised by CSOSA, with the supervision officer (as needed) and that supervision officer's supervisors. Most supervision officers have view (no data entry) access to SOR.
  - The Office of Information Technology (OIT).
  - CSOSA executives and the Office of the Director.
- Information is shared by OIT staff members with:
  - The Office of Financial Management 2 times per year. This is statistical level information (not offender specific).
- Internal system access is authorized for:
  - Information in the SOR database is accessed by a server belonging to the CSOSA Office of Research and Evaluation (ORE) for data collection/ analysis purposes.

5.3. What information will be shared and with whom?

The CSOSA Sex Offender Registration Unit staff members share information in accordance with the following:

- The Office of General Counsel (OGC): Arrest and sentencing documentation is shared electronically via a secure email encryption. OGC is required to review the arrest and sentencing documents from other jurisdictions in order to determine if the offender is required by law to register in DC and, if so, to classify the offender for registration (A, B or C). CSOSA Sex Offender Registration Unit staff members share legal documents with the OGC on convictions in DC for classification and review purposes. OGC may also be consulted for a variety of matters related to an offender's registration requirements and all relevant documents would be provided to assist OGC in making required determinations.
- If the sex offender is supervised by CSOSA, then information is shared with

the supervision officer (as needed), and that supervision officer's supervisors. Most supervision officers have view (no data entry) access to SOR. Documentation, such as sentencing, forms, and notarized letters related to the case are shared with the supervision officer. Arrest and sentencing documents, as well as registration and other legal paperwork, may be shared to ensure close accountability of each offender.

- The Office of Information Technology: CSOSA Sex Offender Registration Unit staff members share information on system and data issues and errors with OIT staff members. Sometimes it is a general error message (e.g., An Error has Occurred). Other times it is offender specific information that is shared in order to troubleshoot and resolve a data error (e.g., cannot update the end date of a particular address). The goal is speedy resolution of the issue so that CSOSA Sex Offender Registration Unit staff members can continue to enter, update and maintain accurate sex offender registration information.
- As a part of performance management/measurement, the CSOSA Sex Offender Registration Unit provides statistical and performance-related information to management, including the CSOSA Office of the Director. This data is not offender specific. This includes number of offenders by Registration Status, number of offenders who completed their verifications, number of non-compliant offenders, and number of violation reports submitted to MPD. When needed, details of unique cases/offenders that management should be aware of are shared.

The OIT staff members share the following information:

- Provide annual statistical level information (total number of registrants, total number of new registrants sent to MPD) to the Office of Financial Management 2 times per year. This information does not contain any PII or offender specific details.

Internal system access is authorized for:

- Information in the SOR database is accessed by a server belonging to the CSOSA Office of Research and Evaluation (ORE). While the server in ORE has access to the entire SOR database, current access is situational in response to inquiries from CSOSA management and executive staff members, including the CSOSA Office of the Director. Future plans for the sharing of the information include statistical information on CSOSA's execution of the duties and responsibilities of SOR, and comparison of data in SOR to SMART for consistency of data maintained in both systems (e.g., address information) and to assist with the identification of offenders who have unmet registration obligations.

5.4. How will the information be shared?

All files/information that are shared by staff members are shared electronically via secured email, or in person.

ORE Staff connect to the SOR back end database with read-only access accounts. ORE does not have copies of this database and does not save any PII data. Data is only used in aggregate format. At this time ORE staff have not been tasked with creating reports or inquiries for any SOR data.

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 purpose of sharing the information listed in the response to Question 5.3 is to obtain necessary guidance (e.g., Classification) and resolve issues impacting the effective and efficient update and maintenance of accurate and complete information on registered sex offenders in SOR, including immediate entry, update and maintenance of address, appearance, vehicle and other registration information. If the information in SOR is not complete, up-to-date or accurate, CSOSA cannot deliver on the purpose stated in the response to Question 1.2. Accurate and complete information is required for proper identification of a sex offender; successful data exchanges with mandatory local and national systems; and complying with the requirements of the DC Sex Offender Registration Act (SORA), DC Municipal Regulations (DCMR) and Code of Federal Regulations (CFR) relevant to sex offender registration in DC.

Yes this purpose aligns with the purpose stated in question 1.2.

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.

CSOSA has a number of controls in place in order to prevent threats to privacy in connection with internal disclosure of information:

- Established policies and procedures: CSOSA has a number of policy statements on information technology security; safeguarding sensitive, unclassified information; records management; standards of employee conduct, and sex offender registration. These are supported by associated operating instructions which provide implementation and operational details. CSOSA staff members are expected to review the relevant policies and procedures. CSOSA staff members are informed when a new policy statement or operating instruction is posted, or an updated version is available.
- Training: Staff members at CSOSA are required to complete Records Management, Privacy Awareness, Ethics, and Information Security Awareness training on a periodic basis. This training reinforces the process around disclosure of information.
- Limit what is disclosed: CSOSA limits what is disclosed to the information that is authorized by law and regulations by limiting the information captured in SOR to what is authorized by law and regulations or necessary for the mandatory data exchanges.
- Conduct various reviews: Information in SOR is subject to reviews (i.e., second

party checks, NCIC data validations, approval by MPD) to ensure information is accurate and complete when disclosed as allowed by law and regulations.

- Minimize access to paper records: The CSOSA Sex Offender Registration Unit maintains paper records secured in an employee's desk or in the unit's secured file room. Access to the secured file room is granted only to certain agency staff via their agency-issued badge. The unit's fax machine is housed within the file room so documents that are faxed to CSOSA are secured until staff are able to retrieve them.
- Internal system access by ORE is a server to server database link between 2 CSOSA servers that are in the same data center and on the same network.

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

Yes. All access to the SOR system and the data within the system is monitored, tracked and recorded:

- The SOR system captures audit trail information at the record level. Every table in the database includes fields for created by (specific user), created date, updated by (specific user) and updated date.
- All SOR authorized users are made aware that accessing the SOR system constitutes agreement to be monitored through a warning that displays when he/she logs into the SOR system.
- System logs are a critical component of managing authorized and unauthorized access to the SOR system. The application (IIS) logs monitor accessing of the SOR application, the database logs monitor accessing of the SOR database and data, and server logs contain events used to monitor accessing of the operating system and other components on the servers. The logs are reviewed manually on a periodic basis.

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.)?

Yes. The information is shared with external entities.

5.9. What information will be shared and with whom?

CSOSA electronically (system to system interfaces) shares SOR data with a number of external entities as required by law and regulation, or for validation of information before saving the information in SOR:

- OCTO Master Address Repository System (MARS)/GIS: The OCTO MARS is the main authority for addresses in DC. All DC addresses entered into SOR (address only – Street Number, Street Name, City, State, Zip – not considered PII) are sent for validation through the OCTO MARS system before being saved.
- MPD: The MPD information technology staff members have direct read-only access to the SOR database to pull data through database views. Information that

is shared includes: Name, aliases, sex, race, date of birth, physical description (height, weight, hair color, eye color, scars, markings, tattoos), identification numbers, registration offense information, sentence information, addresses and phone numbers, and vehicle information.

- DC SOPW: The DC SOPW is managed by the DC Government. This site is open to the public to find information on Class A and Class B offenders that live, work, and/or go to school in DC. Information that is shared includes: Police District, Police Servicing Area, whether an offender is wanted, name, residence address (number rounded to "block" information), work address (number rounded to "block" information), school address (number rounded to "block" information), date of birth, age, physical description (height, weight, hair color, eye color, scars, markings, tattoos), offense(s) of conviction, date of conviction, case number, place of conviction, class of offense (A or B) (if multiple, highest class of offense), age of victim, "Was Victim a Stranger", date of registration and date of last (latest) verification.
- DOJ – SORNA Exchange Portal: The SORNA Exchange Portal was established to allow participating jurisdictions to exchange information on registered sex offenders that are moving in to and out of a Jurisdiction. The portal is open to registered, validated users. Information that is shared includes: assigned to jurisdiction, date of departure, date to report, reason for notification, date sent (date the notification was transmitted to the SORNA Exchange Portal), staff contact name, staff contact phone, staff contact email, offender name (full), addresses (residence, work, school), and optionally, photo, physical description (height, weight, hair color, eye color, scars, markings, tattoos), aliases, date of birth, and/or registration offense(s).
- DOJ – NSOPW: The NSOPW is managed by DOJ. This site is open to the public to find information on registered sex offenders. Information that is shared includes: offender name, offender age, aliases, residence address (number rounded to "block" information), work address (number rounded to "block" information), and school address (number rounded to "block" information). The NSOPW provides a link to the DC SOPW if additional information is desired (please see the DC SOPW description above).
- FBI – NCIC/NSOR: Users of NCIC/NSOR are approved by the FBI and consist of staff members in law enforcement roles and capacities throughout the United States. Information that is shared includes: offender status, offender full name, sex, race, date of birth, physical description (height, weight, hair color, eye color, scars, markings, tattoos), FBI number, social security number(s), registration offense, conviction date, date registered, end of registration date, residence address, residence or cell telephone number, and aliases. Actions are also taken to update information, and remove information from NSOR that is no longer active/valid.

CSOSA Sex Offender Registration Unit staff members share limited SOR data with external entities as part of law enforcement activities and inquiries, such as trying to locate an offender who is non-compliant or has absconded. Such external entities include the U.S. Marshal Service, National Center for Missing and Exploited Children, and other jurisdictions. Sharing may be in person, via secured email, or via secured fax.

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?

The purposes of sharing the information with MPD, DOJ and the FBI through the interfaces listed in section 5.9 directly support and align with the stated purpose in the response to Question 1.2:

- Meet legal requirements: The sharing of data is mandated in the various laws and regulations promulgated under SORA, DCMR and CFR relevant to sex offender registration in DC.
- Support the execution of law enforcement actions and activities at the local, state and national levels by providing proper identification of and current information about sex offenders who live, work, and/or go to school in DC.
- Provide information to the public regarding registered sex offenders in their community by enabling searches for sex offender registration information at the local and national level through the DC SOPW and the NSOPW.
- Tracking of offenders who are required to register within the DC jurisdiction, and outside of the DC jurisdiction due to residing, working or going to school in multiple jurisdictions (a common occurrence in DC), and offenders who are relocating through sharing of information in the SORNA Exchange Portal.

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

The information shared by the SOR system is accessed and used:

- OCTO MARS/GIS: The SOR application makes a call via the internet to the OCTO MARS system. Only address information (Street Number, Street Name, City, State, Zip – not considered PII) is provided. OCTO MARS returns an indication if the address is validated, the PSA, and the latitude and longitude coordinates. The information is saved to the SOR database at the time the residence, employment or school is saved. CSOSA Sex Offender Registration staff members can save a DC address that does not validate. Staff members at OCTO will take action to try and confirm the address, offer alternative verified addresses, research the address, or report that the address is invalid and needs to be updated.
- Metropolitan Police Department (MPD): The MPD information technology staff members have direct read only access to the SOR database to pull data through database views. MPD interfaces the information into MPD systems that support MPD staff members and officers. MPD uses the data in the execution of its mission of law enforcement, public education, protecting the citizens of and visitors to DC, and preserving the Nation's Capital city.
- DC SOPW: MPD provides some of the information they pull from the SOR database to OCTO for the DC SOPW. OCTO provides the web site, the search capability and ability to view offender addresses and locations via a map of DC. CSOSA provides information through a "More Details" link that links to a server at CSOSA with a copy of relevant data from the SOR database. The CSOSA

server provides the information on the offender in a format specified by MPD entitled "Metropolitan Police Department Sex Offender Information Bulletin". The public has access to the DC SOPW through https://mpdc.dc.gov and clicking on the Sex Offender Registry link under Services. The public may use the information to obtain knowledge about registered sex offenders that live, work and/or attend school in the community.

- DOJ – SORNA Exchange Portal: Information from SOR that applies to other jurisdictions is uploaded by CSOSA to the SORNA Exchange Portal on a daily basis. Computer logic at the portal makes the transactions available to the appropriate jurisdiction. Approved users of the portal are given a username and password for logging into the portal. The information in the SORNA Exchange Portal is used by the participating jurisdictions to track sex offenders who are entering the jurisdiction to verify the offenders appear for registration confirmation, assist with tracking offenders who are leaving the Jurisdiction, and confirm the offenders report to the new jurisdiction as required. CSOSA also downloads information for the DC jurisdiction from the portal on a daily basis. The CSOSA Sex Offender Registration Unit staff members review the information and take appropriate action (e.g., update the location of an offender with multi-jurisdiction registration, prepare for an offender who is transferring into the DC jurisdiction, and confirmation that offenders have registered).
- DOJ – NSOPW: Information from CSOSA for the NSOPW is sent via secure file transfer protocol on a daily basis. Computer logic at the NSOPW makes the information available through the NSOPW web site. The public can access the NSOPW through https://www.nsopw.gov. The public may use the information to obtain knowledge about registered sex offenders that live, work and/or attend school in the community.
- FBI – NCIC/NSOR: CSOSA provides information to NCIC through coded transactions that are sent multiple times per day. Computer logic at NCIC processes the transactions to the databases at the FBI. Access to NSOR is managed by the FBI. Approved users can access information on registered sex offenders in support of law enforcement inquiries and actions.

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

For the electronic interfaces, CSOSA has several technical controls in place to minimize risk including strong passwords, restricted firewall rules, and use of encryption in transit and at rest. Transparent data encryption (TDE) has been applied to our SOR Database; this encryption is known as encrypting data at rest. Data exchanged is limited to the minimum amount of data necessary to successfully add, update and maintain records. Information data available through public websites is limited to the data authorized to be shared in the law and regulations.

CSOSA Sex Offender Registration Unit staff members manually share limited SOR data with external entities as part of law enforcement activities. Controls that are in place to minimize risk include sharing data via secured email, or via secured fax. Other controls include training for staff members on information security, privacy, and records management. Manual sharing of information is limited to specific law enforcement purposes (e.g., finding offenders who are non-compliant with quarterly or annual verification, information on offenders who may have absconded, etc.).

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?

System-to-system interfaces are governed by the authorities listed in Section 2, operating manuals, and/or Memoranda of Understanding between CSOSA and the other organization. Because the system to system interfaces are to share SOR data with other systems, system interfaces are built in compliance with the operating manuals and guidance provided by the receiving agency (i.e., MPD, FBI, DOJ).

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?

When changes as to how information is being collected, maintained or disseminated are implemented, CSOSA will update the required policy, procedures and forms to reflect the changes. Offenders will be notified in writing, via updates to the language on the forms, and CSOSA Sex Offender Registration Unit staff members will review the changes with the offender at their next in person visit – either initial registration, quarterly/annual verification, or an intermittent in person visit due to a change in address, vehicle or personal appearance information.

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

Individual sex offenders do not have access to the SOR system. However, there are several ways an offender can view the information that has been entered in SOR:

- Office forms: Sex offenders are provided a copy of the Initial Registration form which has the information in SOR at the time of initial registration printed on the form. If another copy is needed, it will be provided. Sex offenders also receive copies of each verification form completed by the offender at the quarterly/annual verification, or during an intermittent in person visit due to a change in address, vehicle or personal appearance information (all in person updates).
- As the DC SOPW is a public website, sex offenders may log into this site and review information, including their own. The information available on the website includes the major information in SOR: name, aliases, sex, race, date of birth, physical description, identification numbers, registration offense information, sentence information, addresses and phone numbers, and vehicle information The web site includes cautionary language that unlawful use of information on the site to threaten, intimidate, harass, or injure a registered sex

offender will not be tolerated and will be prosecuted to the full extent of the law.

- As the NSOPW is a public website, sex offenders may log into this site and review information, including their own. There is a link from the NSOPW that allows the offender to view the information on the DC SOPW.

Under the provisions of the Privacy Act and Freedom of Information Act (FOIA), individuals may request searches of appropriate applications to determine if any records have been added that may pertain to them. This is accomplished by sending a written request directly to:

Court Services & Offender Supervision Agency
Office of the General Counsel
800 North Capitol Street, N.W., Suite 7217
Washington, DC 20002
ATTN: FOIA/Privacy Act Request

By facsimile at:
(202) 442-1963
ATTN: FOIA OFFICER

Please see the Privacy Act regulations set forth in 49 C.F.R. Part 10 for more information on how to submit a request. While no specific form is required, individuals may obtain forms for this purpose from the CSOSA internet site, https://www.csosa.gov/foia/

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

CSOSA has procedures that allow an individual to discuss and highlight inaccurate or erroneous information:

- At initial registration, for offenders convicted in another jurisdiction, if the offender believes the registration classification determination is inaccurate, the CSOSA Sex Offender Registration Unit staff member will provide the registrant with the case number of the sex offense conviction and instructions for contacting the sentencing Court to address the concerns regarding sentencing conviction.
- At initial registration, if the registrant has a concern with registering in DC, he/she is given the packet to challenge and seek Judicial Review with the DC Superior Court and, if an attorney is needed, the Public Defender Office's information. The individual must follow the procedures set forth in D.C. Code § 22–4004 Dispute resolution procedures in the Superior Court, which is a process between the individual, and the DC Superior Court. Any information already entered in SOR will be marked as "Pending – Judicial Review" and be held until the DC Superior Court has made a final determination, or the waiting period (30 days) has expired. Depending on the outcome, the information in SOR will be updated to

reflect any changes to the registration information (e.g., classification, duration of registration period, mark the case as closed if the offender is found not required to register).

- If an individual believes that information related to them in SOR is inaccurate, either through review of forms outlined in the response to Question 4.1, or data viewed through the DC SOPW or NSOPW, the individual can address his/her concerns with the CSOSA Sex Offender Registration Unit by reporting to the Unit and updating the required paperwork. The staff members are in the best position to review the issue with the offender and either correct the inaccurate/erroneous information, or determine to whom the issue needs to be elevated to, in order for it to be resolved.

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

Individuals are notified about the procedures for correcting their information via this PIA, by the copy of the SORA and DCMR received at initial registration (documents detail the process of initial registration Judicial Review), and by the staff members in the CSOSA Sex Offender Registration Unit.

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

Once it has been determined that the individual must register as a sex offender, there are no opportunities for the offender to consent or dissent to uses of the information that are in the law and regulations. The penalties for not complying with the duties and responsibilities of sex offender registration are severe. Those penalties are listed on both the Initial Registration Form and Verification Form. At the time of quarterly/annual verification, the offender is required by law and regulation to provide the information, as well as reconfirm his/her understanding of his/her duties and responsibilities regarding maintaining/updating changes of home, work or school addresses, any change in motor vehicle information, and/or any significant changes in physical appearance, as well as the quarterly/annual verification process.

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)?

As part of the initial registration process, the CSOSA staff members are required to provide the District of Columbia Sex Offender Registration Act and the Rules for implementation of the Act (6A DCMR 400 *et. seq*) to the sex offender. The sex offender signs the Initial Registration form indicating that these have been provided/received. These documents explain the information that will be shared with other agencies and the public. Both documents allow CSOSA to take action so that "information concerning sex offenders is promptly provided or made available to other law enforcement and governmental agencies as appropriate."

7. Information Security and Safeguards

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, the component office works with the CIO and OIT to build privacy and security into SOR. Every request to add new fields and information to SOR is routed to CSOSA OIT for additional review, approval and implementation. The OIT will review the request with CSOSA OGC and as needed, MPD, to confirm the addition is within the scope of the law, regulations, and the Privacy Act.

7.2. Do contractors have access to the system?

Yes, contractors have indirect access to SOR. There are contractors in CSOSA working on the CSOSA Infrastructure and CSOSA Information Security Teams who do have access to the servers and the network. All staff members who enter and maintain data are employees of CSOSA or MPD. The staff members who maintain the SOR application and database are employees of CSOSA.

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

There are procedures in place to determine which users may access the information. Users are selected by their respective management personnel for the positions on the CSOSA Sex Offender Registration Unit and MPD Special Investigations Branch. A CSOSA Computer Access form, signed by the user's supervisor, must be submitted for edit/update access to SOR. Based on CSOSA-implemented user roles, responsibilities, and need to know, a user is granted access to the appropriate network access group.

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

The administrative safeguards in place to protect the information in SOR include:

- The SOR system captures audit trail information. Every table in the database includes fields for created by, created date, updated by and updated date.
- All CSOSA and MPD staff members who are authorized users of SOR are made aware that accessing the SOR system constitutes agreement to be monitored through a warning that displays when the user logs into SOR.
- System logs are a critical component of managing authorized and unauthorized access to the SOR system. The application (IIS) logs monitor accessing of the SOR application, the database logs monitor accessing of the SOR data and database, and server logs contain events used to monitor accessing of the operating system and other components on the servers. The logs are reviewed manually on a periodic basis. The logs provide the data needed to verify that

authorized users are accessing the system, and to search for and identify any unauthorized accesses to the system.
- The SOR database is backed up on a daily basis. The backup capability at CSOSA is centralized and managed by CSOSA OIT. The backup schedule and plan includes storage of backups on-site at CSOSA, and off-site.
- Security and other audits of the SOR system (e.g. review of the SOR System Security Plan, annual FISMA audit, annual financial audit) are completed as scheduled by CSOSA OIT and CSOSA Office of Management and Administration.

The technical safeguards in place to protect the information in SOR include:

- All equipment and components for the SOR system run on the CSOSA network and are located behind a firewall or multiple firewalls.
- The SOR application is web-based and available on CSOSA's internal network. All workstation access to the SOR application server is protected by a Certificate which encrypts information between the workstation and the SOR application server.
- The physical database on the SOR database server is protected, along with the data in the database.
- Access to the data by authorized MPD and CSOSA staff members is controlled by network access groups. Each time an authorized staff member logs onto the SOR system, his/her username and password are verified by the network directory as being a successful match before access to the SOR system is given.

The physical safeguards in place to protect the information in SOR include:

- Access to CSOSA office spaces (not lobbies) is controlled by badges and key cards. All CSOSA offices have security guards and scanners located in the lobby which control the access for those individuals who do not have key cards.
- Only CSOSA issued workstations are connected to CSOSA's network.
- CSOSA does support remote access for CSOSA staff members. MPD staff members with access to SOR access SOR remotely. Extra authentication in the form of a PIN and code from a token is required to authenticate to the network. A CSOSA VPN is available to individuals with CSOSA issued devices.
- If working remotely, once a staff member has successfully authenticated to the network, access to SOR requires that the user re-enter their username and password.
- The servers running the SOR application, housing the SOR database, and housing the servers used in the data exchange processes are located in CSOSA's data center.
- Access to CSOSA's data center is limited to specific individuals who are authorized to maintain the servers, and controlled by CSOSA issued badges. All other individuals who need to be in CSOSA's data center for any reason (contractors, outside support personnel, etc.) are escorted the entire time they are

in CSOSA's data center.

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

Yes, an ATO is required. The current ATO was signed on 5/13/2020.

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

The SOR system is able to provide an accounting of disclosures defined as follows:

- Changes to data in the database: The SOR system captures audit trail (changes to the data) information. Every table in the database includes fields for created by, created date, updated by and updated date. The database administrator can identify who created the data and when, and who last modified the data and when.
- Access to the application: System logs are a critical component of managing access to the SOR system. The application (IIS) logs monitor accessing of the SOR application, the database logs monitor accessing of the SOR data and database, and server logs contain events used to monitor accessing of the operating system and other components on the servers. The logs are reviewed manually on a periodic basis. The logs provide the data needed to verify that authorized users are accessing the system, and to search for and identify any unauthorized accesses to the system.
- Access and running of Reports: The SOR system has a limited number of statistical, operational and data integrity reports available for authorized, authenticated users of SOR. The logs also track who accessed and ran one or more reports.
- Interface execution status: For most of the system interfaces, the SOR system provides some type of audit trail as to whether the interface ran successfully, or encountered errors. If errors are found, the errors are investigated, the information is fixed, and the interface picks up the corrected data when it runs the next time. For the interfaces with MPD and the DC SOPW, user feedback is required in order to identify that the interfaces did not execute as scheduled. In those cases, MPD, OCTO and CSOSA work closely to find the error, fix the issues, and restore the information to the DC SOPW.

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

The controls that CSOSA has in place to prevent the misuse of data by authorized, authenticated users are procedural guidance. Misuse of the information by CSOSA staff members carries significant penalties, including termination. The CSOSA Office of Professional Responsibility is authorized to investigate any alleged misuse of data by CSOSA staff members.

Staff members at CSOSA are required to complete Records Management, Privacy Awareness, Ethics, and Information Security Awareness training on a periodic basis.

This training reinforces the need to protect all information, including PII, from authorized access or misuse. The penalties for misuse are reviewed as part of this training.

There are limitations to the use of the data through the DC SOPW and the Metropolitan Police Department Sex Offender Information Bulletin. The restrictions for the use of the data, as well as the penalties for misuse, are posted on the website and are included in the text of the Bulletin each time the Bulletin is generated.

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

Yes, CSOSA has system logs that are used to identify unauthorized users/unauthorized access. The system logs are a critical component of managing access to the SOR system. The application (IIS) logs monitor accessing of the SOR application, the database logs monitor accessing of the SOR data and database, and server logs contain events used to monitor accessing of the operating system and other components on the servers. The logs are reviewed manually on a periodic basis. The logs provide the data needed to verify that authorized users are accessing the system, and to search for and identify any unauthorized accesses to the system.

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

Yes, the agency does provide annual security and privacy training for agency employees and contractors. CSOSA staff members, including government personnel and contractors, are required to take annual security awareness and privacy training offered by CSOSA. This allows staff members to understand how privacy impacts their role and retain knowledge of how to properly and securely protect information in situations where they may use PII in the course of performing their duties.

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

All authorized users of SOR, staff in the Office of Information Technology, MPD staff in the MPD Special Investigations Branch, and staff who work on the interfacing systems, are responsible for assuring the correct use of the information and safeguarding of PII.

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

SOR is different in that collection and disclosure of specific PII is authorized in the law and regulations that govern Sex Offender Registration in DC, and at the national level. If PII is unlawfully disclosed, the impact would be low because much of the PII collected in SOR is publicly available.

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)?

All contractors who work in OIT Infrastructure and OIT Information Security have gone through the same background investigation process as federal employees prior to starting work at CSOSA. Contractors have a separate computer access form for gaining access to a system that must be signed by the Contracting Officer's Representative (a federal employee). Contractors are held to the same security and privacy requirements as federal employees. Non-Disclosure Agreements are in process for the contractors who work in OIT Infrastructure and OIT Information Security.

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

The relevant IT security measures have been documented in this PIA.

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?

The system owner has a number of tools he/she can use to ensure the information is used in accordance with the stated practices in this PIA:

- Review of policies and procedures: The system owner can review CSOSA policies and procedures regarding sex offender registration and verify they are aligned with the stated practices in this PIA. If discrepancies are found, the system owner can request actions be taken to align the documents.
- Spot checks of offender files: The system owner can review the paper files of registered sex offenders to verify they are aligned with the stated practices in this PIA (e.g. initial registration form is signed, etc.).
- Review of FBI Audit results: The system owner can review the results of the audit performed by the FBI regarding NCIC/NSOR. As this is the most complex system to system interface, the audit results are an indication of the overall health and robustness the of the data exchanges.
- Review of the DC SOPW and NSOPW: The system owner can view sex offender records through these public websites and confirm the displayed information is in accordance with the stated practices in this PIA.
- Requests for vulnerability scan results and logs: The system owner can request to see the results of vulnerability scans. The system owner can also request a review of the application, database and server logs to check for authorized and possible unauthorized access.
- Accreditation process: The system owner can review the results of the Accreditation which document the system security controls and how the system assessed against each control.

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

The privacy risks associated with SOR are the same as the threats to privacy associated with SOR as outlined in the responses to Question 2.5 and Question 3.4:

- Collection of inaccurate information: This is mitigated by the use of source documents for collecting and entering the information. Sex offenders are required to provide complete and accurate information with his/her signature as verification that the information being provided is accurate.
- Mistakes in data entry: This is mitigated by the various reviews completed (e.g., second party checks, NCIC validation, and MPD validation of data prior to it being displayed on the DC SOPW).
- Exposure of PII to unauthorized persons: This is mitigated by requiring paper records to be secured in an employee's desk or in the unit's secured file room when not in use, and housing the unit's fax machine is housed within the secured file room. Staff members at CSOSA are required to complete Records Management, Privacy Awareness, Ethics, and Information Security Awareness training on a periodic basis.
- Collection of extraneous information: This is mitigated by limiting the PII collected in SOR to what has been authorized in law and regulations (SORA, DCMR, CFR) or by OGC. Collection of information required solely for matching offender information in local and national sex offender databases is limited to those identifiers that best serve the purpose for matching data between systems, or as required by law and/or regulation.
- Vulnerabilities in system access and exchanges: This is mitigated by employing Federal Government standard/approved technical controls to ensure data is protected while stored and exchanged in the SOR system of records.
- Extraneous information interfaced in from other systems: This is mitigated by electronically interfacing minimal data into SOR from Systems of Record.

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?

CSOSA has a number of ways to verify that the information entered into SOR is accurate and complete:

- The SOR system has validations built into the application that enforce known data standards, such as length for SSN, number of digits for a phone number, requiring numbers for a date of birth, and similar standards. The application makes extensive use of drop down values and radio buttons to ensure consistency in how the information is captured and entered.
- The CSOSA Sex Offender Registration Unit has a system of second party checks that require another staff member use the original documents to review and confirm the data was correctly entered and/or updated in SOR.
- The CSOSA Sex Offender Registration Unit is also required to perform

continuous NCIC data validations to confirm the information in SOR matches the information in NCIC/NSOR.

- Staff members in the MPD Special Investigations Branch review and approve the records in SOR of all offenders who qualify to appear on the DC SOPW. MPD staff members must approve the offender as “Web OK” before the offender’s data will appear on the DC SOPW. MPD staff members also review any changes or updates to those records.
- Information on an offender is not sent to the NSOPW until it has been approved by MPD for the DC SOPW.
- Every three years, the FBI conducts an audit of the information in SOR versus the information in NCIC/NSOR (selected random sampling). Differences are discussed. Audit findings document the major issues and CSOSA is required to address the findings.

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?

There are no additional privacy risks other than what has already been identified in this PIA.

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.

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

Yes, the privacy policy is provided at https://www.csosa.gov/privacy-policy.

Authorizing Signatures

This Privacy Impact Assessment has been conducted by Kathleen French and Kaitlin Forsha and has been reviewed by SHEILA STOKES Digitally signed by SHEILA STOKES Date: 2023.05.02 10:39:32 -04'00'________, the Senior Agency Privacy Official, for accuracy.

_Frank Lu__________________________
System Owner Name (Please Print)

FENG LU Digitally signed by FENG LU Date: 2023.04.27 07:50:59 -04'00'

System Owner Signature Date

_Sheila Stokes_______________________
Senior Agency Official for Privacy (Print)

SHEILA STOKES Digitally signed by SHEILA STOKES Date: 2023.05.02 10:37:22 -04'00'

Senior Agency Official for Privacy Signature Date

____
General Counsel (Print)

SHEILA STOKES Digitally signed by SHEILA STOKES Date: 2023.05.02 10:37:57 -04'00'

General Counsel Signature Date