# Court Services and Offender Supervision Agency (CSOSA)

## The Supervision & Management Automated Record Tracking (SMART 21) Privacy Impact Assessment

**CONTROLLED UNCLASSIFIED INFORMATION**

**_____, 2022**

**SMART 21/Office of Information and Technology**
**Court Services and Offender Supervision Agency**
633 Indiana Avenue, NW, Washington, DC 20004

# POINTS OF CONTACT for SMART 21

| **Program Office Point of Contact:** | **System Owner Point of Contact** |
|---|---|
| **Name:** | **Name:** Frank Lu |
| **Title:** | **Title:** Service Development Director |
| **Office:** | **Office:** OIT |
| **Phone:** | **Phone:** 202-585-7902 |
| **Bldg./Room** | **Bldg./Room** 800 North Capitol St NW |
| **Email:** | **Email:** frank.lu@csosa.gov |
| **Privacy Program Manager:** | **Senior Agency Official for Privacy:** |
| **Name:** | **Name:** |
| **Office:** | **Office:** |
| **Phone:** | **Phone:** |
| **Bldg./Room** | **Bldg./Room** |
| **Email:** | **Email:** |

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 SMART 21

The Supervision & Management Automated Record Tracking (SMART 21) is a case management system used by the Court Services and Offender Supervision Agency (CSOSA) for the District of Columbia's agency personnel to enter, update, and maintain information on the 10,000+ offenders under supervised release, probation, parole, deferred sentencing agreement and civil protection order in the city of DC.

The purpose of this new Privacy Impact Assessment (PIA) is to address privacy risks associated with the collection, storing, dissemination, and disposal 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.

SMART 21 is a custom developed case management system used to enter, update, and maintain information on the 10,000+ offenders under supervised release, probation, parole, deferred sentencing agreement and civil protection order in the city of DC.

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

The collection and use of the PII is necessary for CSOSA to carry out its legal requirements and mission for the District of Columbia (DC) which include:

- Proper identification of an offender including photos and distinguishing features such as height, weight, hair color, eye color, and other physical identification.
- Various identifying numbers required for matching offender information and various fields required for sharing of relevant data with other law enforcement partners and systems such as the National Crime Information Center (NCIC)/Supervised Release system, and JUSTIS (Criminal Justice Coordinating Council (CJCC) portal for information on arrests, defendants, offenders, and those being released from prison). There are over 25 manual and automated interfaces in and out of SMART 21 to support data exchanges to systems internal to CSOSA and external at the local and national levels.
- Execution of the terms and conditions of supervision (releasing authority ordered as well as CSOSA imposed) including visits to home addresses, places of employment, drug testing, drug and alcohol treatment, GPS monitoring, treatment for mental health issues, treatment for sex offenders, and information on disabilities and health concerns as those impact the need for and accessibility to services.

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

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 is a new PIA.

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

The system is 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]

National Capital Revitalization and Self-Government Improvement Act of 1997, Pub. L. 105-33, D.C. Official Code § 24-133

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]

SMART 21 allows user information to be retrieved by a personal identifier which is detailed in the System of Records Notice (SORN) published in the Federal Register. The Privacy Act System of Records Notice for is CSOSA-11, Dated 3/15/2002, 67 FR 11816, Document number 02-6092. The SORN can be viewed here: https://www.federalregister.gov/d/02-6092/p-317

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]

The NARA schedule number is DAA-0562-2013-0011. The Disposition instructions state the records should be destroyed 20 years after case is closed or 5 years after an offender's death.

[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.

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

All information in SMART 21 is saved in the database indefinitely and will be disposed of in accordance with the NARA schedule and procedures.

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.).

Threats to privacy would be through compromise of the data in the database, or compromise of data through one of the system data exchanges. CSOSA uses a number of controls: splitting of roles involved with granting user access, strong passwords, https, Activity Directory Groups, transparent data encryption, encrypted data exchanges, and IP specific firewall rules to name just some of the controls in place to ensure that from a database and data exchange operations standpoint, the information is handled, retained, managed and disposed of appropriately.

CSOSA requires employees to complete mandatory IT Security & Privacy Awareness, Records Management and Ethics training in accordance with Federal regulations, all which have sections on the proper handling, retention and disposition of offender information, including personally identifiable information.

## 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 | **X** | Financial Account | |
| Taxpayer ID | | Driver's License | **X** | Financial Transaction | |
| Employee ID | **X** | Credit Card | | | |

Other identifying numbers (please specify):

Offenders:

- Police Dept ID (PDID) – DC Metropolitan Police Department (MPD)
- Bureau of Prisons (BOP) Tracking
- Federal Bureau of Investigations (FBI) Number
- Federal Registry (FEDREG) Number
- Dept of Corrections (DCDC) Number
- VISA

- Immigration Naturalization
- Interstate Compact
- NCIC Number
- Passport
- State ID
- Vehicle Tag Number

| **General Personal Data** | | | | | |
|---|---|---|---|---|---|
| Name | **X** | Date of Birth | **X** | Religion | |
| Maiden Name | | Place of Birth | **X** | Financial Information | **X** |
| Alias | **X** | Home Address | **X** | Medical Information | **X** |
| Gender | **X** | Telephone Number | **X** | Military Service | **X** |
| Age | **X** | Email address | **X** | Physical Characteristics | **X** |
| Race/Ethnicity | **X** | Education | **X** | | |

Other general personal data (specify):

- Information on mental health assessments and progress on recommended treatment is tracked.
- Information on substance abuse assessments and progress on recommended treatment is tracked.
- Information on sex offender assessments and progress on recommended treatment is tracked.
- Information on domestic violence intervention orientation and progress on recommended treatment is tracked.

| **Work-related Data** | | | | | |
|---|---|---|---|---|---|
| Occupation | **X** | Telephone number | **X** | Salary | **X** |
| Job title | **X** | Email address | **X** | Work history | **X** |
| Work address | **X** | Business associates | **X** | | |

Other work-related data (please specify):
For Offenders: Business Associate information is limited to the Supervisor Name and Phone number for the offender. SMART 21 maintains a history of employment and unemployment information.

| **Distinguishing Features/Biometrics** | | | | | |
|---|---|---|---|---|---|
| Fingerprints | | Photos | **X** | DNA profiles | |
| Palm prints | | Scars, marks, tattoos | **X** | Retina/iris scans | |
| Video recording/signatures | **X** | Vascular scan | | Dental profile | |

Other distinguishing features/biometrics (please specify):
For Offenders: SMART 21 stores multiple photos to allow staff to view how an offender's physical appearance has changed over time. Scars, Marks and Tattoo information is found on the same page as the Physical Description information.

| **System admin/audit data** | | | | | |
|---|---|---|---|---|---|
| User ID | **X** | Date/time of access | **X** | ID files accessed | **X** |

| | | | | | |
|---|---|---|---|---|---|
| IP address | X | Queries run | X | Contents of files | X |
| Other system admin/audit data (please specify):<br>System admin/audit data is collected on users of SMART 21 (federal employees and contractors) , not offenders. The purpose of collecting this information is for troubleshooting problems (e.g., enables OIT to view error logs to see where a particular transaction is failing), and to respond to requests from the Office of Personnel Responsibility. Log files are maintained at the database, application, system and network levels. | | | | | |

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 (please specify): | | | | | |

| **Government Sources** | | | | | |
|---|---|---|---|---|---|
| Within the Component | X | Other CSOSA components | X | Other federal entities | X |
| State, local, tribal | X | Foreign | | | |
| Other (please specify):<br>Through the interfaces with various systems, SMART 21 is automatically updated with the following:<br>- From NCIC, MPD (through JUSTIS), Maryland and Virginia: Notifications to CSOs and SCSOs of arrests potentially involving offenders under CSOSA supervision.<br>- From Pre-trial Services (sister agency): Results of drug tests.<br>- From NCIC: Law enforcement inquiries and warrants potentially involving offenders under CSOSA Supervision.<br>- GUNStat: This is a manual upload of information on offenders on a particular watch list.<br>- Most Violent Person: This is a manual upload of information on offenders on a particular watch list.<br>- Department of Youth Rehabilitation Services (DYRS): This is a manual upload of information on offenders on that are supervised by CSOSA and DYRS.<br>- Information on GPS bracelets being worn by offenders under CSOSA supervision.<br>- CJCC's JUSTIS: Data from the DC Superior Courts on charges, new charges, and requests for Pre-sentencing Investigations.<br>- From US Parole Commission (USPC): Responses to Alleged Violation Reports submitted by CSOSA on offenders who are non-compliant with the terms of their supervision. | | | | | |

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

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

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

Data is entered, retrieved, viewed, and updated through the application user interface by authorized users (CSOSA staff members and contractors). Once saved, the data is stored in the SMART 21 database, documents are scanned in and then stored in SharePoint. Users are able to retrieve scanned in/stored documents through the Document Library. The documents are scanned in in their entirety and staff members are able to review the entire document. Documents may contain additional personally identifiable information.

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 interfaces are necessary to obtain information from and exchange information with other partner agencies involved in the law enforcement continuum in DC. Automated interfaces reduce the amount of work required by CSOSA staff to enter data into the SMART 21 database that has been previously recorded in other systems, and improve the quality of the data in SMART 21 due to the removal of the potential for human error, typos and record mismatches. Interfaces are generally limited to what is required by the interface to successfully create, maintain and close records, minimizing the potential for loss of data. Each interface has been reviewed and CSOSA has determined the data is critical to the successful supervision of offenders and has secured the necessary interfaces to minimize potential threats to privacy.

Threats to privacy based on the information collected and the sources of information include a compromise of the database, compromising the data in the database, and protecting the information as it is being passed through the interfaces. To mitigate those risks, CSOSA uses a number of controls: splitting of roles involved with granting user access, strong passwords, secure encrypted hyperlinks, transparent data encryption, encrypted data exchanges, and IP specific firewall rules to name just some of the controls in place to ensure that from a database and data exchange operations standpoint, the threats to data compromise or loss are minimized.

**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 system uses the information to assist in the execution of the terms and conditions of supervision (releasing authority ordered as well as CSOSA imposed) including

conducting visits to home addresses as verification that the offender does reside there, conducting visits to places of employment as verification of the offender's employment, to request and provide drug and alcohol treatment, to order and track GPS monitoring, in the treatment for mental health and sex offender related issues, and to be aware of conditions that impact an offender's accessibility to and eligibility for services.

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 | **X** |
| For Intelligence activities | | For administrative matters | |
| 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**[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]

Yes. Social Security Numbers (SSN) are collected and entered by CSOSA staff members when entering data on offenders. Please note, not all offenders have a SSN.

The SSN is used for matching arrest data from Virginia with records on offenders in SMART 21. This is the only use of SSNs for the interfaces. The other interfaces rely on name, date of birth and/or other identifiers to successfully match offender information.

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

No alternatives were considered or selected because collection SSN is required for the purpose of matching arrest data from Virginia.

## 4. Notice

[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.

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.

Notice is not provided prior to the collection of information because offender and case information is entered into the system, or acquired by the system from other law enforcement and criminal justice systems.

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:** 5 U.S.C. 301, Department Regulations; 5 U.S.C. 6122, Flexible Schedules; E.O. 10450, Security Requirements for Government Employees; and E.O. 9397* (SSN), as amended.

**Purpose:** Information is collected to verify your eligibility to access controlled facilities and for issuing badges for use in entering facilities.

**Routine Use:**

- *For Law Enforcement Purposes*: To disclose pertinent information to the appropriate Federal, state, or local agency 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 a civil or criminal law or regulation.
    - *For Litigation*: To disclose information to, include but not limited 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.
    - *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.
    - *For National Archives and Records Administration*: To disclose information to the National Archives and Records Administration for use in records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.
    - *For Congressional Inquiry*: To provide information to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
    - *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:** Mandatory

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

There are no opportunities to opt-out. The individual records in this system are not created by the individual and are created in accordance with law and court or legal other authority

## 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 personnel who need to gain access to the SMART 21 system submit a computer access form. That form is then reviewed by a staff member who is responsible for system access. Once approved, the user is set up with data access and assigned to a user group that allows the user to view and edit rights.

The SMART 21 System Administrators, Database Administrators and Developers

have local administrator rights to the servers in order to install the application, install the database software (SQL Server), make changes to the application code, manage the interfaces, configure the software, and troubleshoot problems and issues. As requested/authorized by the users, a limited number of data changes are performed directly in the database.

The CSOSA Infrastructure and Information Security Teams have admin rights to all servers, including the servers that the SMART 21 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.

There is limited data sharing required internally because approved users of SMART 21 are in all offices/divisions of CSOSA. One or more users in each division/office have access to the information in SMART 21 related to his/her job.

Data from the SMART 21 database is made available electronically to the CSOSA Office of Research and Evaluation (ORE) for analysis purposes.

5.3. What information will be shared and with whom?

A limited set of SMART21 data and/or system generated documents is shared via memorandum of understanding with the DC Criminal Justice Coordinating Council (CJCC) and CSOSA approved CJCC partners; The FBI NCIC Supervised Release File, the National Instant Criminal Background Check system (NICS).

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

Via secure electronic web services

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?

Various identifying numbers required for matching offender information and various fields required for sharing of relevant data with other law enforcement partners and systems such as the National Crime Information Center (NCIC)/Supervised Release system, and JUSTIS (Criminal Justice Coordinating Council (CJCC) portal for information on arrests, defendants, offenders, and those being released from prison).

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

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 requires employees to complete mandatory Security & Privacy Awareness, Records Management and Ethics training in accordance with Federal regulations, all which have sections on the proper handling, retention and disposition of offender information, including personally identifiable information.

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

All access to the SMART 21 system and all the data within the system is monitored, tracked and recorded:

The SMART 21 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 SMART 21 users are made aware that accessing the SMART 21 system constitutes agreement to be monitored through a warning that displays when he/she logs into the SMART 21 system. 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.

5.9. What information will be shared and with whom?

Through the interfaces with various systems, SMART 21 is updated with the following:

- Automated interface from NCIC, MPD (through JUSTIS), Maryland and Virginia: Notifications to supervision officers and supervisors of supervision officers of arrests potentially involving offenders under CSOSA supervision.
- Automated interface from Pre-trial Services (sister agency): Results of drug tests.
- Automated interface with Veritracks (external service provider): Information on GPS – location, out of range messages, low battery indicators, other warnings.
- Automated interface from NCIC: Law enforcement inquiries and warrants potentially involving offenders under CSOSA Supervision.
- GUNStat: This is a manual upload of information on offenders on a particular MPD watch list.
- Most Violent Person: This is a manual upload of information on offenders on a particular MPD watch list.
- Automated interface from DC Superior Court (through JUSTIS): Information on current and upcoming offender cases including Pre-Sentence Investigations,

Deferred Sentencing Agreements, Probation, Domestic Violence, and Civil Protection Order.

- Dept of Youth Rehabilitation Services (DYRS): This is a manual upload of information on offenders on that are supervised by CSOSA and DYRS.
- Automated interface from JUSTIS: Data from the DC Superior Courts on charges, new charges, and requests for Pre-sentencing Investigations.
- Automated interface from USPC: Responses to Alleged Violation Reports submitted by CSOSA on offenders who are non-compliant with the terms of their supervision.

Through the interfaces with various systems, SMART 21 shares (sends) or may provide direct access to the following:

- Automated interface to Pre-trial Services (sister agency): Requests for drug testing. PSA also has direct access to view running records.
- Automated interface with Veritracks (external service provider): Provide offender information for offenders who are on GPS monitoring.
- Automated interface to Office of the Chief Technology Officer (DC) GIS: Address information to confirm the address is a verifiable DC address and retrieve the associated Police Servicing Area/District.
- Automated interface to NCIC – Supervised Release (SR) system: Provide identifying information, general personal data, supervision start and end dates, name and phone of the supervising officer as required by the NCIC-SR system to create, modify and delete records for offenders who are under active supervision at CSOSA.
- Automated interface to NICS: Provide identifying information, general personal data, supervision start and end dates, name and phone of the supervising officer as required by the NICS system to create, modify and delete records for offenders who are under active supervision and testing positive for drugs at CSOSA.
- Automated interface to the Sex Offender Registry (SOR) (CSOSA system): For offenders under supervision by CSOSA, SMART 21 updates SOR with the names and phone numbers of the supervision officer and his/her supervisor.
- Automated interface to the DC Sentencing Commission GSS: Provide information on the assigned supervision officer and his/her supervisor for Pre-Sentencing Investigations.
- Automated interface to the USPC: Submit Alleged Violation Reports on offenders who are non-compliant with the terms of their supervision where the USPC is the releasing authority.

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 purpose of sharing the specified information is to provide offender information required by other law enforcement partners and systems as established in regulations, MOUs and other agreements. Information shared is generally limited to information

required for successful matching of records or required by the external system to successfully create, update or maintain a record for the offender.

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

The information is used by the external agency and approved users of the external agency systems in support of law enforcement inquiries and actions such as processing offenders for required drug testing, background checks, coordination by staff members at CSOSA and partner law enforcement agencies, processing of alleged violation reports, and other law enforcement actions.

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

For the interfaces, CSOSA has a number of controls in place to minimize risk including usernames, strong passwords, use of https, IP restricted firewall rules (only allow certain IP Addresses to connect), and limiting data exchanged to data which is necessary to successfully add, update and maintain records.

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?

CSOSA does not share SMART21 system information for computer matching purposes. CSOSA shares limited SMART21 in accordance with law enforcement routine use law, per the Memorandum of Understanding with the DC Criminal Justice Coordination Council (CJCC), and as required by laws and compliance requirements of the FBI.

## 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?

The Bureau of prisons will send an email notifying those individuals of any changes regarding how their information is being collected, maintained, or disseminated by the system. Those updates will also be documented in this PIA. Individuals can review this PIA for public updates.

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

An individual participant will have to submit a Freedom of Information Act (FOIA) request to obtain information about themselves that the agency maintains in the system. Under the provisions of the Privacy Act and 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 702
Washington, DC 20002
ATTN: FOIA/Privacy Act Request

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

When seeking records about yourself from any CSOSA system of records, the request must conform with the Privacy Act regulations set forth in 49 CFR Part 10. The request must be signed, and the requestor's signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Freedom of Information Act Officer, https://www.csosa.gov/foia/

In addition, the requestor should provide the following:

- An explanation of why the requestor believes the agency would have information on him/her;
- Identify which component(s) of the agency the requestor believes may have the relevant information;
- Specify when the requestor believes the records would have been created;
- Provide any other information that will help the FOIA staff determine which CSOSA component agency may have responsive records; and if the requestor is seeking records pertaining to another living individual, the requestor must include a statement from that individual certifying his/her agreement for the requestor to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and the request may be denied due to lack of specificity or lack of compliance with applicable regulations.

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

The Bureau of prisons will send an email notifying those individuals of the procedures.

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

The Bureau of prisons will send an email notifying those individuals of the procedures.

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

Individuals do not have the opportunity to consent or dissent.

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)?

The agency provides notice to individuals that their PII may be shared with other agencies via this published PIA and SORN.

## 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. The system security plan and authorization to operate incorporates all 800-53 controls including privacy controls and the system is assessed accordingly.

7.2. Do contractors have access to the system?

CSOSA staff members and some contractors collect, enter and maintain information in the system. A limited number of staff members at external agencies have access to SMART 21. The staff members who maintain the CSOSA 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.

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

Users of SMART 21 are selected based on their job at CSOSA (e.g. Community Supervision Officer) or by their respective management personnel. If the person is a new user, CSOSA requires that personnel who need to gain access to the SMART 21 system submit a computer access form. The form is to be signed by a supervisor. That form is reviewed by a staff member in the Office of Information Technology who is responsible for system access. Once the network account is created, if the individual requires access to SMART 21, either OIT Customer Support adds the user to the SMART 21 system, or a request is sent to the Development Team Quality Assurance

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

member to add the user to SMART 21.

There is a System Admin role in SMART 21 that has access to User Accounts functionality which displays information on all users who have access to SMART 21. Through the Users Accounts functionality, staff members on the SMART 21 Development Team can add new users; add, change, update, and make inactive user roles in SMART 21; change user information, and/or make the user inactive in the SMART 21 system.

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

Physical safeguards:

- Access to all CSOSA office spaces (not lobbies) is controlled by 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.
- Desktop workstations used by CSOSA staff members are located within CSOSA office spaces. Some CSOSA staff members use CSOSA owned and issued laptops, surface (mobile technology), Macs, and other mobile computing devices. CSOSA staff members are accountable for the mobile devices issued to them by the agency.
- Only CSOSA issued devices are directly connected to CSOSA's network. CSOSA does not allow workstations or laptops not issued by CSOSA to be directly connected to the network.
- CSOSA does support remote access for CSOSA staff members, external users and some contractors. Extra authentication in the form of a PIN and code from a token is required to authenticate to the network. Once a CSOSA staff member has successfully authenticated to the network, SMART 21 can be accessed if the CSOSA staff member is an authorized user of SMART 21 (username and password required).
- The servers running the SMART 21 application, housing the SMART 21 database, and 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. Access to the data center is controlled using key cards. 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.

Technical safeguards:

- All equipment and components for the SMART 21 system run on the CSOSA network and are logically located behind the internal firewall.
- The SMART 21 application is web-based to make it available on CSOSA's

Intranet. All workstation access to the SMART 21 application server is protected by a Secure Socket Layer (SSL) Certificate, which encrypts information between the workstation and the SMART 21 application server.

- Access to SMART 21 by authorized users is controlled by Active Directory. Each time an authorized staff member logs onto the SMART 21 system, his/her entered username and password are verified by Active Directory as being a successful match before access to the SMART 21 system is given.
- All access within the SMART 21 system (which parts of the SMART 21 system, which offenders, and what data) is controlled by the information entered in the User Accounts functionality by the System Admin (role). Through the Users Accounts functionality, staff members on the SMART 21 Development Team can add new users; add, change, update, and make inactive user roles in SMART 21; change user information, and/or make the user inactive in the SMART 21 system.

Administrative safeguards:

- The SMART 21 system captures audit trail information at the record level. Every table in the database includes fields for created by, created date, updated by and updated date.
- All authorized users are made aware that accessing the SMART 21 system constitutes agreement to be monitored through a warning that displays when he/she logs into SMART 21.
- System logs are a critical component of managing authorized and unauthorized access to the SMART 21 system. The IIS logs monitor accessing of the SMART 21 application, the SQL Server logs monitor accessing of the SMART 21 data and database, and server logs which contain events captured in Windows Event Viewer monitor accessing of the operating system and other components on the servers.
- 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 logs are reviewed manually on a periodic basis.
- The SMART 21 database is backed up on a daily basis. The backup capability at CSOSA is centralized and managed by CSOSA Office of Information Technology. The backup schedule and plan includes storage of backups on-site at CSOSA, and off-site.
- Security and other audits of the SMART 21 system (e.g. review of the SMART 21 System Security Plan, annual FISMA audit, annual financial audit) are completed as scheduled by CSOSA Office of Information Technology and CSOSA Office of Management and Administration.

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

Yes, an ATO has been granted.

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

Yes, routine record audits are completed to ensure compliance with all federal guidelines for documentation standards and record keeping.

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?

There is a System Admin role in SMART 21 that has access to User Accounts functionality which displays information on all users who have access to SMART 21. Through the Users Accounts functionality, staff members on the SMART 21 Development Team can set the access a particular user has to SMART 21 and the data in the database. In addition, coding has been used when needed to limit staff access below the role and organization level, such as limiting Running Record entries to certain users, allowing only certain users to change an offender's supervision level, etc.

Because of the high level of PII in CSOSA systems associated with offender case initiation and supervision, CSOSA has procedural guidance in place about the use and misuse of the information that is collected and saved in CSOSA systems. Misuse of the information carries significant penalties, including termination. The CSOSA Office of Professional Responsibility is authorized to investigate any alleged misuse of data collected and saved in CSOSA systems, including SMART 21, by CSOSA staff members.

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

Yes. All successful logons and unsuccessful attempts are logged. Logged data includes account name (user ID), date/Time stamp, and source IP address. Periodic log audits are conducted. Session timeout of 15 minutes prevents reduces risk of unauthorized access by someone other than the person who logged in. SMART uses Active Directory (AD) for authentication. AD requires passwords be complex (12 characters, numbers, upper and lower case letters), passwords be changed every 60 days (new password creation prevents from using previously used passwords).

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

Yes. Privacy training is provided during the annual security awareness training.

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

All authorized users of SMART 21 (employee, contractor, external), staff in the Office of Information Technology, and staff who work on the interfacing systems, are responsible for assuring the correct use of the information and safeguarding of PII. The SMART 21 Development Team is responsible for configuring and coding any safeguards into the application. The Infrastructure Team and SMART 21 Development Team are jointly responsible for any safeguards at the server, network, operating system and software levels such as server hardening, patching, configuring security benchmarks, and other similar safeguards.

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

If PII is unlawfully disclosed, individuals may be exposed to the common risks associated with identity fraud.

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)?

Yes. This is part of the security clearance and orientation process for contractors.

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

Nothing in addition to what has already been documented within 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?

System users must complete annual IT Security and Privacy Awareness courses.

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

Risks to privacy breach associated with this system exist as risk cannot be entirely eliminated. Controls in place to reduce and mitigate risk are identified in this document – including access controls and many other aforementioned controls.

## 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?

The SMART21 system employs constraints and rules in many of its transactional functions. For example, only valid addresses matched against a derivative of the US Postal Service database can be saved. Social Security Numbers and other identifiers are checked against the database for duplication. Not all data can be explicitly quality controlled by the system however and so accuracy and completeness is thereby a function of CSOSA policies and training.

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?

The Privacy Act Statement is provided via the publication of the PIA. The full statement can be found in section 4.2.

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

CSOSAs privacy policy is publicly viewable on the CSOSA website homepage.
https://www.csosa.gov/privacy-policy/

## Authorizing Signatures

This Privacy Impact Assessment has been conducted by the Office of Information and Technology and has been reviewed by Sheila Stokes, the Senior Agency Privacy Official, for accuracy.

Frank Lu
System Owner Name (Please Print)

Frank Lu — 1/13/2021
System Owner Signature — Date

Sheila Stokes
Senior Agency Official for Privacy (Print)

Sheila Stokes, Esq. — 1/24/2022
Senior Agency Official for Privacy Signature — Date

Sheila Stokes
General Counsel (Print)

SHEILA STOKES Digitally signed by SHEILA STOKES Date: 2022.01.24 12:25:52 -05'00'
General Counsel Signature — Date