Court Services and Offender Supervision Agency (CSOSA)

STOP VeriTracks v11 Monitoring System
Privacy Impact Assessment

CONTROLLED UNCLASSIFIED INFORMATION

____, 2021

Global Positioning Systems Unit
Court Services and Offender Supervision Agency
633 Indiana Avenue, NW, Washington, DC 20004

Overview of STOP VeriTracks v11 Monitoring System

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. To further this mission, the Office of Information & Technology (OIT) established VeriTracks Monitoring system, designed to reduce criminal recidivism by tracking and monitoring offenders and promoting accountability, community protection and offender rehabilitation through behavior modification. The vendor for VeriTracks is Satellite Tracking of People (STOP) LLC.

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

VeriTracks is a public safety solution designed to significantly reduce criminal recidivism, prevent crimes though behavior modification, establish geographic zone "inclusion and exclusion" areas, provide crime analysis tools across jurisdictional boundaries, and enhance the effectiveness and efficiency of law enforcement and corrections by way of actionable information. This data integration tool combines Global Positioning Satellite (GPS) offender tracking technology with current criminal incident data reported to local law enforcement. All offender data is pulled from the Supervision Management Automated Record Tracking (SMART) system and submitted by electronic referral to the CSOSA GPS office via email.

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

The purpose for which PII is collected, used, maintained, and/or shared in the system is to track and monitor offenders enrolled in VeriTracks. Information in VeriTracks is used for criminal law enforcement activities and to create an offender profile using their name, date of birth (DOB), CSOSA ID, PDID. This information is used to ensure that all enrollee profiles in VeriTracks are unique. The stored PII is used to identify the enrollee within the VeriTracks system.

The vendor, STOP LLC collects real time crime data that might contain PII from the Metropolitan Police Department. The data is used for crime analysis purposes. The real time crime report is analyzed against past and real time geographic locations of offenders to determine correlation or any behavioral pattern for the sole purposes of crime solving.

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

Veritracks is currently in operation and has been in operation since December 9, 2016.

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?

Veritracks is operated by CSOSA and STOP LLC.

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 Veritracks?

- CSOSA Policy Statement 4008: Global Positioning System (GPS) Tracking of Offenders Policy Statement 4008, effective May 7, 2009.
- National Capital Revitalization and Self-Government Improvement Act of 1997, D.C. Official Code § 24-133 (c) (2001 Edition).
- 28 C.F.R. § 2.85(a)(15) (Conditions of release; D.C. Code parolees)
- 28 C.F.R. 800.3 (Functions and Responsibilities)

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.

Yes. Information in Veritracks is retrieved by a name or personal identifier. This system will need to be covered by a Privacy Act SORN.

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.

VeriTracks records are temporary and can be destroyed 20 years after the calendar year in which the case is closed, but longer retention is authorized if required for business use. Disposition Authority is DAA-0562-2013-0025.

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

Yes. Records are disposed of appropriately and accordance with the NARA schedule. Records are disposed manually by the vendor, once CSOSA has identified records for disposal.

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

The vendor, STOP LLC, ensures that VeriTracks security and privacy controls have been implemented within the infrastructure to protect the collection, transmission, storage and processing of PII. Annual mandatory security, privacy and role based training is provided to all employees including contractors.

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		File/Case ID	X	Financial Account	
Taxpayer ID		Driver's License		Financial Transaction	
Employee ID		Credit Card			
Other identifying numbers (please specify):					

General Personal Data					
Name	X	Date of Birth	X	Religion	
Maiden Name		Place of Birth		Financial Information	
Alias		Home Address	X	Medical Information	
Gender	X	Telephone Number	X	Military Service	
Age	X	Email address		Physical Characteristics	X
Race/Ethnicity	X	Education			
Other general personal data (specify):					

Work-related Data					
Occupation		Telephone number		Salary	
Job title		Email address		Work history	
Work address		Business associates			
Other work-related data (please specify): Enrollee real time Geographic Location					

Distinguishing Features/Biometrics					
Fingerprints		Photos		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	x	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 collected from stated sources (paper form, webpage, database, etc.).

Directly from individual about whom the information pertains					
In person	X	Hard copy: mail/fax		Online	
Telephone		Email			
Other (please specify): Releasing Authority or United States Parole Commission (USPC) All offender data is pulled from the Supervision Management Automated Record Tracking (SMART) system and submitted by electronic referral to the GPS office via email.					

Government Sources					
Within the Component		Other CSOSA components		Other federal entities	x
State, local, tribal	-	Foreign			
Other (please specify): United States Parole Commission (USPC)					

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?

All PII is stored in each offender's unique profile within the Veritracks system. The system is only accessible to individuals with approved access. Each user login is captured at the time of login.

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

The source of and requirement for use of the PII is used to accurately coordinate the information in the system (e.g., GPS location(s)) with the identity and other characteristics of offenders in order to make law enforcement, legal, and case management decisions. Controls designed to mitigate threats are described in the security section, Section 7, of this PIA. SSNs were proactively omitted from inclusion in this system as they were deemed not to be necessary for identification given the use of the case ID. All other information was determined to be essential for law enforcement, legal, and case management purposes.

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.

Information in the system is collected, used, maintained, and/or shared in the system is to track and monitor offenders enrolled in VeriTracks. Information in VeriTracks is used for criminal law enforcement activities and to create an offender profile using their name, date of birth (DOB), CSOSA ID, and PDID. This information is used to ensure that all enrollee profiles in VeriTracks are unique. The stored PII is used to identify the enrollee within the VeriTracks system. All users who access VeriTracks with PII do so for the sole purpose of tracking and monitoring offenders enrolled in the system. All offenders are tracked and monitored according to their approved schedules by a leasing authority, or by authority given in Code of Federal Regulations.

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	
To conduct analysis concerning subjects of		To promote information sharing	

investigative or other interest		initiatives	
To conduct analysis to identify previously unknown areas of note, concern, or pattern	X	For administering human resources programs	
For litigation			
Other purpose (please specify):			

Social Security Numbers

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

No social security numbers (SSN) are collected.

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

No alternatives necessary as SSNs are not collected. The CSOSA ID is used.

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.

All enrollees complete and sign the GPS Monitoring Referral Form, the CSOSA Global Positioning System (GPS) Contract, and the District of Columbia Official Code (D.C. Code § 22-1211: Tampering with a detection device , referred to collectively as the "GPS Contract". The Contract is completed before the offender is enrolled in the Veritracks system. The Contract notified enrollees, in part, that, "All movement will be tracked and stored as an official record." The contract and the GPS Monitoring Referral Form includes a Privacy Act Statement.

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

Enrollees are notified in the GPS Contract that, "All GPS data including tracking and suspected violation data are accessible to various…law enforcement agencies. In addition to CSOSA, your device may be monitored by these law enforcement agencies."

The contract and the GPS Monitoring form (paper form) includes the following Privacy Act Statement:

Authority:

- Global Positioning System (GPS) Tracking of Offenders Policy Statement 4008, dated 5/7/09

- National Capital Revitalization and Self-Government Improvement Act of 1997, D.C. Official Code § 24-133 (c) (2001 Edition).

- 28 C.F.R. § 2.85(a)(15) (Conditions of release; D.C. Code parolees)

Purpose:
Information in the system is collected, used, maintained, and/or shared in the system is to track and monitor offenders enrolled in VeriTracks. Information in VeriTracks is used for criminal law enforcement activities and to create an offender profile using their name, date of birth (DOB), CSOSA ID, PDID. This information is used to ensure that all enrollee profiles in VeriTracks are unique. The stored PII is used to identify the enrollee within the VeriTracks system.

Routine Use:

Standard CSOSA Routine Uses:

- *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 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:
Disclosure is mandatory.

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

The GPS monitoring system is used as a law enforcement tool to provide heightened supervision monitoring. An offender's enrollment in GPS monitoring is either a requirement of the releasing authority or imposed as a sanction for non-compliance pursuant to 28 C.F.R. § 810.3. Therefore there are no opportunities to opt-out without the offender experiencing a negative consequence in the form of an administrative sanction or a formal allegation to the releasing authority of non-compliance with

supervision which could include loss of liberty.

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.)?

All access is granted through the CSOSA GPS Program Office. All end users have to be formally trained, and are then provided individual user accounts with permissions based on their role.

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

Yes, information will be shared internally with the Office of the General Counsel (OGC), Office of Research and Evaluation (ORE), Office of Financial Management (OFM)/Office of Administration (OA), Office of Information Technology (OIT), and the Office of the Director (OD).

5.3. What information will be shared and with whom?

Information is shared with OGC for legal matters, e-discovery, and FOIA requests. VeriTracks information is shared with OIT on an as needed basis for technical issues, ORE for research, OA/OFM for contract/financial management, and OD for executive management.

5.4. How will the information be shared?

Information will be shared electronically through internal communication channels.

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

The information is shared with OGC for legal reasons, OIT for technical issues, ORE for research, OA/OFM for contract/financial management. Yes, this purpose aligns with the stated purpose in Question 1.2 above.

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.

The GPS Program Office only collects data as necessary to conduct agency operations and achieve its purpose. All data is safeguarded by GPS staff and in accordance with NIST 800-53 requirements. Data is securely uploaded through the proper internal

channels (SMART) within 48 hours. All PII is discarded in accordance with the approved NARA schedule. Only authorized users with usernames and passwords can access this data.

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

Yes. All user logins are captured in the Veritracks system.

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?

CSOSA allows the District of Columbia's Metropolitan Police Department (MPD) limited access to VeriTracks and thereby to its GPS and enrollee data through the analysis function of the site. In addition, information may be shared with our law enforcement partners and the courts pursuant to established routine uses or exceptions under the Privacy Act of 1974. Routine uses are established and published in the System of Records Notice (SORN) for this system.

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 is to assist in active criminal investigations with local law enforcement. This purpose aligns with the stated purpose in section 1.2. Offenders are notified in the GPS contract that the data may be shared with law enforcement. Written request can be made via the FOIA and/or subpoena.

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

Authorized external users have read-only access to this data. Access is only granted after approval is received through the Agency Director, and proper training is received from the GPS Program Manager. The information is used by law enforcement to assist with active investigations, and is limited to the analysis section of the Veritracks system.

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

Users have read-only access. No data can be manipulated. See the security section (Section 7) for the list of controls implemented to minimize risk.

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?

Yes. The agency has an MOU with MPD.

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?

Offender will be notified in writing if there are any changes. Such notification will be done prior to implementation. If any changes occur after implementation, the information will be provided to the offender's primary Community Supervision Officer (CSO). The CSO will then notify the offender verbally or in writing of the changes.

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 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

When seeking records about yourself from any CSOSA system of records, the request must conform with the Privacy Act regulations set forth in 49 C.F.R. 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 Freedom of Information Act (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?

All referral data is reviewed with offenders prior to them being placed on GPS. Any discrepancies identified will be submitted to their Community Supervision Officer (CSO) and an updated referral document will be requested prior to placement. Any other changes necessary after placement will be sent to GPS Help mailbox by supervision CSO or Supervisory Community Supervision Officer (SCSO). GPS staff will update information accordingly.

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

Offenders are informed in person that any changes need to be requested though their CSO, and forwarded to the GPS office via GPS Help as stated above in 6.3.

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

Offenders are notified in the GPS contract; however, due to the requirements of probation, the only means for offenders to dissent is decline to sign the GPS contract.

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)?

1. They are notified prior to installation in the GPS contract. Item number 14 in the GPS contract states that “All GPS data including tracking and suspected violation data are

accessible to various local (i.e. Metropolitan Police Department) and national (i.e. U.S. Capitol Police) law enforcement agencies. In addition to CSOSA, your device may be monitored by these law enforcement agencies."
. The GPS contract and referral form include a Privacy Act statement.

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.

7.2 Do contractors have access to the system?

Yes.

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

Only individuals who have a need based on their role in the agency will be permitted access. Such access is only granted after proper training is received. All user accounts are setup based on the user's role. All staff outside of the GPS Program Office have read-only access and are unable to edit offender PII.

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

Security Authorization (ATO) per FISMA, NIST SP 800-37, SP800-53, and associated standards and guidance required for Security Authorization.

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

Yes. It was granted on May 29, 2019.

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

Yes.

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?

Users outside of the GPS Program Office have read only access to the data. Additionally, no user is authorized to release GPS data outside of the agency without written approval from the CSOSA OGC. Any user who fails to adhere to such requirements are subject to

corrective action from the agency. External users must submit a weekly log to OGC to justify their use of the system.

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

VeriTracks tracks invalid user login attempts. The system will lock out a user after three unsuccessful attempts. An invalid attempt would be someone with invalid credentials (username/password) or authorization (i.e., has been deactivated and no longer has access to VeriTracks).

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

Yes. Training is required annually.

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

Users of the VeriTracks system, the program office and Contracting Officer Representative (COR) are responsible, with assistance and collaboration of OIT and OGC.

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

If information is unlawfully disclosed, individuals could be harmed by embarrassment or blackmail. To prevent this from happening CSOSA implements the proper safeguards to protect the integrity and confidentiality of the data stored in Veritracks.

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)?

CSOSA does not currently utilize contractors in the GPS Program Office.

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

A technical solution was implemented so that the system is not accessible over the general Internet. A user must be coming from the CSOSA network and have a valid network account. The following security controls have been put in place to prevent the misuse of PII data by those having access to the STOP VeriTracks v11 Monitoring System:

- Logical Access Control: access is configured based on roles and provided on a need to know basis. All user roles are assigned the least privileges needed to carry out their job functions. Access is restricted through security configurations in place on the system and application level.

- Access Monitoring: System and application level access is monitored, logged and reviewed to prevent misuse. Automated monitoring is in place to prevent access misuse and monitor unauthorized logical (privilege escalation, access to PII, use of privileged accounts etc.) and physical access to the system.
- Communications Protections: Network layered access and defense –in depth protections are in place to monitor user access and restrict access to only authorized users configured directly through the network VPN or domain controller. IP whitelisting and access control list (ACLS) are in place on the firewalls to restrict access to only approved ports, services and IPs.
- Information Integrity Protections: Security configurations are in place, such as the Group Policy Objects on the domain controllers to restrict the use of removable media, preventing unauthorized copying and moving of PII data.
- Physical Security Controls: physical security controls such as proximity access readers, biometric readers etc. are in place to restrict physical access to only authorized users. Cameras and access records are used to monitor physical access and to ensure that there is no misuse of physical access to the system.

8 Auditing and Accountability

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

CSOSA suspends user access after 90 days of inactivity in VeriTracks. STOP implements effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the agency is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals. STOP implements automated tools to monitor logs for traffic from malicious sources and audit logs can alert to unauthorized activity. A Federal Information Processing Standards (FIPS) security audit is conducted annually to ensure compliance. Additionally, a security assessment is required for the system to operate, which will assess privacy controls.

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

Privacy risks are minimized because the data is collected in real-time through continuous monitoring of the enrollee. Risks are mitigated through accountability and auditing.

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?

PII in the VeriTracks profile is compared with the PII listed in SMART at each device

installation and deactivation/removal by a CSOSA employee who is conducting these tasks.

Any discrepancies observed in tracking data will immediately be addressed with the contractor by the Contracting Officer's Representative.

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?

Privacy risks are minimized because data is collected in real-time through continuous monitoring of the enrollee. Also, human error of inputting incorrect data is minimized by cross-checking the information entered into VeriTracks with information contained in SMART.

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.

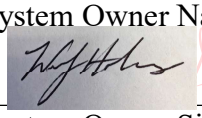
10.2 Is the privacy policy publicly viewable? If so where?

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

Authorizing Signatures

This Privacy Impact Assessment has been conducted by Global Positioning Systems Unit and has been reviewed by SHEILA STOKES Digitally signed by SHEILA STOKES Date: 2021.08.10 09:16:17 -04'00', the Senior Agency Privacy Official, for accuracy.

_Wesley Holmes_____
System Owner Name (Please Print)


Digitally signed by Wesley Holmes
Date: 2021.05.24 09:34:07 -04'00'

_____ _____5/24/2021_____
System Owner Signature Date

_____
Senior Agency Official for Privacy (Print)

SHEILA STOKES Digitally signed by SHEILA STOKES
Date: 2021.08.10 09:17:09 -04'00'

_____ _____
Senior Agency Official for Privacy Signature Date

_____
General Counsel (Print)

SHEILA STOKES Digitally signed by SHEILA STOKES
Date: 2021.08.10 09:19:17 -04'00'

_____ _____
General Counsel Signature Date