Court Services and Offender Supervision Agency (CSOSA)

Biometric Verification System

Privacy Impact Assessment

July 5, 2012

Court Services and Offender Supervision Agency (CSOSA)
633 Indiana Avenue, NW, Washington, DC 20004

SECTION 1.0

Purpose of collection

CSOSA will state the purpose and legal authority for collecting personally identifiable information ("PII").

1.1 Why is the information being collected?

CSOSA supervises the approximately 15,000 residents of the District of Columbia on probation, parole, supervised release, civil protection orders, and deferred sentencing agreements. As part of the supervision processes, offenders may be required to submit to drug testing, attend programs (e.g., vocational training, school to earn a GED, anger management, other treatment related groups), report to the office to see his/her Community Supervision Officer, or participate in residential treatment programs, as required by the terms and conditions of his/her release, or as required by CSOSA based on the needs of the offender.

CSOSA business practice is to have the offender sign a log when checking in for office visits, drug testing, and various intervention/assistance programs. This practice does not provide the electronic data necessary for efficient accounting of an offender's participation in required events. This practice also does not provide for proper verification of the offender's identity at the time of check-in. To mitigate the risks associated with the sign-in (e.g., inaccurate accounting for attendance, someone signing in for the offender), the biometric verification pilot will allow all offenders under CSOSA supervision to electronically "check-in" for office visits, programs, and drug lab testing using a PIN and hand biometric recognition to verify the identity of the offender. The goal of the pilot is more accurate tracking of offender attendance, and accurate verification of offender identity.

1.2 What legal authority and/or agreements allow the information to be collected?

Information maintained in the biometric verification system is collected pursuant to a delegation by Congress, that CSOSA will exercise the powers and functions for the District of Columbia pursuant to the National Capital Revitalization and Self-Government Improvement Act of 1997, and shall provide supervision for District offenders on probation, parole, and supervised release on behalf of the court or agency having jurisdiction over the offender being supervised.

1.3 Is the information searchable by a personal identifier – like a name or Social Security number? If so, what Privacy Act System of Records Notice(s) apply/applies to the information being collected?

Offenders who are enrolled in the biometric verification program can only check-in for an office visit or program or drug test by entering his/her PIN and scanning his/her right hand. Offenders cannot search the information or search for information on other offenders who might be enrolled in the biometric verification program.

CSOSA staff members are able to search and retrieve the information by a number of personal identifiers: Last name, First name, Date of birth, PDID, CSOSA Number or Probationer ID (PIN). At this time, there is no Privacy Act System of Records Notice for the biometric verification system as this is a new system for CSOSA. This Privacy Impact Assessment was requested to provide the documentation needed to review the status of the biometric verification system and determine if a separate System of Records Notice is needed.

1.4 Is there a records retention schedule that has been approved by the National Archives and Records Administration ("NARA") for the information system(s)? Explain how long and for what reason the information is retained.

It is unknown if there is a current records retention schedule that has been approved by the National Archives and Records Administration, however, since the system is new, the assumption is there is no records retention schedule at this time. The Records Management Inventory questionnaire was completed on 6/11/2012 and is currently under review in order to determine what type of records retention schedule is needed. The current assumption is that the information will need to be retained for the same period of time as the SMART (CSOSA's case management system) data is being retained as this information is about offenders whose information is also maintained in SMART.

1.5 Are there any forms or surveys that are associated with the collection of the information that would be covered by the Paperwork Reduction Act ("PRA")?

There are no forms or surveys associated with collecting the information. The forms associated with an offender's enrollment and use of the biometric verification system are:

- Biometric Verification Enrollment Receipt: At the time the offender is enrolled/registered in the biometric verification system (initial hand scan is captured), the offender is given a receipt with his/her PIN, general information about the biometric verification program, and how to obtain assistance if he/she encounters issues.

1.6 Are there any privacy risks for this system that relate to the purpose of the collection? If so, how will CSOSA mitigate these risks?

The only known risk is whether the offender is informed of the purpose for collecting the information and how CSOSA will use the information. CSOSA Office of Information Technology will work with CSOSA Community Supervision Services and CSOSA Office of General Counsel to prepare materials for educating CSOSA staff members and offenders on the purpose of the biometric verification system, and the benefits to offenders and CSOSA staff members when using the system. These materials will include information on why the offender is required to provide this specific information, how CSOSA maintains the privacy of personally identifiable information, and how CSOSA uses the provided information.

SECTION 2.0

Openness and transparency

CSOSA will be open and transparent. We should tell individuals about the PII we collect and how we will protect it, use it, and share it. We will provide an easy way for individuals to learn about what is happening to their PII.

2.1 Will individuals be given notice prior to the collection of personal information about them? If not, please explain.

When the offender is enrolled/registered in the biometric verification system, a CSOSA staff member searches for existing information on the offender using one or more of the following search criteria: Last name, First name, Date of birth, PDID, or CSOSA Number.

Upon a successful match, existing data on the offender is made available for viewing from staging tables which contain up-to-date information from CSOSA's case management system. This information consists of: Photo, Last name, First name, Date of birth, PDID, CSOSA Number, Community Supervision Officer's name, Team Number, and Branch. All offenders should be aware of the information (Photo, Last name, First name, Date of birth) in CSOSA's case management system and staging database/staging tables as the offender would have been responsible for providing much of the information to the Community Supervision Officer.

At enrollment, the offender has the option to review the information with the CSOSA staff member responsible for assisting the offender with enrollment/registration. Because the information is made available via a "view", the information is not maintained in the biometric verification system database except for several identifiers which are used to correctly match the offender with the data available from the staging database/staging tables. If issues or discrepancies are found, the CSOSA staff member or the offender can notify the offender's assigned Community Supervision Officer. Issues and discrepancies will be investigated by the assigned Community Supervision Officer, and the data in CSOSA's case management system will be corrected if needed. This information would then be made available to the biometric verification system via updates to the staging database/staging tables.

At the time of enrollment/registration, the offender will be given the Biometric Verification Enrollment Receipt which provides information about the personal information collected from the offender while "checking-in" through the biometric verification system. CSOSA Office of Information Technology is currently working with CSOSA Office of General Counsel to review the proposed Biometric Verification Enrollment Receipt, and enhance the receipt with a privacy statement which emphasizes why the offender is required to provide this specific information, how CSOSA maintains the privacy of personally identifiable information, and how CSOSA uses the provided information. The enrollment receipt is retained by the offender.

2.2 Will individuals be given notice prior to their information being shared? If not, please explain.

Through the Biometric Verification Enrollment Receipt, offenders will be given notice as to how CSOSA uses the information provided by the offender, including sharing of offender data. NOTE: Information from the biometric verification system is not shared directly from the biometric verification system, with CSOSA staff members who do not have a need to know, or any external agencies or parties. Any sharing of information with law enforcement partners would be either from CSOSA's case management system, or from CSOSA's Enterprise Data Warehouse.

2.3 Are there any privacy risks for this system that relate to openness, and transparency? If so, how will CSOSA mitigate these risks?

The only known risk is keeping the offender informed should the information collected about an offender change, or there are changes to what information is shared. Because these offenders do report in person, changes to the biometric verification system, including changes to the information that is to be collected or information that is to be shared, would be posted by the network-attached hand readers used for the biometric scan, and made available for offender review when he/she completes a "check-in" through the biometric verification system.

SECTION 3.0

Data minimization

CSOSA will limit the collection of PII to what is needed to accomplish the stated purpose for its collection. CSOSA should keep PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system?

The majority of the information in the biometric verification system about the offenders is basic identifiers (First name, Last name, Probationer ID, CSOSA #, and PDID # (if the offender has one)). This is needed for the views in order to obtain and display the correct offender's data from the staging database/staging tables.

In addition, there is information on those CSOSA staff members who are authorized to access and use the biometric verification system.

3.2 What PII will the system include?

When an offender is initially enrolled for biometric verification, as well as during every check-in, existing data on the offender is made available via a view from CSOSA's case management system via a staging database/staging tables. This information consists of the following on each offender:

- Offender's photo
- last name
- first name
- date of birth
- Police Department ID (PDID)
- CSOSA Number
- Community Supervision Officer's name
- Team Number
- Branch
- Probationer ID (PIN): Once the offender is enrolled, this displays each time
- Date and time of last successful biometric scan: Once the offender is enrolled, this displays each time

Upon successful check-in, the following information is captured:

- Date of check-in
- Time of check-in
- Location of check-in
- Venue
- If Venue is Program Attendance, then a program type is captured
- If Venue is Census, then a floor is captured

The system also maintains information on CSOSA staff members authorized to access the biometric verification system. That information includes:

- Logon information (username)
- Assigned role/permission level in the biometric verification system
- Name (first and last)
- Phone number
- Job title
- Supervisor
- Location (which CSOSA site/office the staff member is assigned to and normally reports to)
- Default hand reader (biometric hand reader closest to the staff member's office)
- Email

3.3 Why is the collection and use of the PII necessary to the project or system?

The personally identifiable information collected and used through the biometric verification system is necessary to achieve a number of purposes:

- The data which is pulled in by the view from the staging database/staging tables associated with CSOSA's case management system (e.g., name, date of birth, CSOSA Number,) is used by CSOSA staff members to accurately identify the offender at enrollment into the biometric verification system and at each check-in. This addresses one of the main purposes of the biometric verification system: Accurate offender identification (e.g., minimizes the risk of someone else checking-in in place of the offender as the hand biometric scan would fail, and the photo/physical description would not match). Use of a view eliminates the need to store the information in the biometric verification system as the data is already stored in and available from CSOSA's case management system.
- The Probationer ID (PIN) is generated by the biometric verification system. The PIN, in conjunction with the hand biometric scan, allows the offender to properly identify him or herself to the biometric verification system at each check-in.
- The personally identifiable information captured/added by the biometric verification system at successful check-in, (date, time, location, and venue) allows the Community Supervision Officer to view and confirm offender attendance at scheduled and required events. This addresses the other main purpose of the biometric verification system: More accurate accounting for offender attendance through the availability of electronic check-in information (versus having to look through hard copy sign-in sheets).
- The personally identifiable information on the CSOSA staff members is used to verify and validate that appropriate individuals are given access to the biometric verification system, and to follow up as needed should there be issues with the accounts, access to the system, etc.

3.4 Will the system aggregate previously unavailable data about the individual or create new data about the individual? If so, how will this data be maintained and used?

The biometric verification system aggregates existing data about the offender (pulled from the staging database/staging tables associated with CSOSA's case management system) with new data created within the biometric verification system (e.g., the PIN, date of check-in, time of check-in, etc.), or entered by CSOSA staff members into the biometric verification system (e.g., by-pass flag). The data that is pulled in and displayed from the staging database/staging tables associated with CSOSA's case management system is listed in the response to Question 3.2, and is data that is previously available to CSOSA staff members and others involved in law enforcement. New data that is unique to the biometric verification system includes:

- The Probationer ID (PIN). The biometric verification system generates the PIN.
- A hand biometric scan.
- The information about each successful check-in (date of check-in, time of check-in. location, and venue).
- A record of successful and failed check-in attempts by the offender, and the CSOSA staff member who provided assistance.
- A by-pass flag for the hand biometric scan, which is added, updated and maintained by CSOSA staff members

Information maintenance and use: The information in the biometric verification system is maintained by a combination of CSOSA staff members and the offender. Information about the offender from the staging database/staging tables provided through the view is maintained through CSOSA's case management system (maintenance is outside of the biometric verification system). The Probationer ID/CSOSA # is used to link all of the information in the biometric verification system about an offender together – both the information from the staging database/staging tables associated with CSOSA's case management system, and the new information entered through the biometric verification system. All check-ins are CSOSA staff assisted: A CSOSA staff member selects the venue and the hand reader to be used. The offender enters his/her PIN, and provides his/her right hand for the biometric scan. The biometric verification system then confirms the hand scan, and adds the date, time, location and venue information. The information in the biometric verification system provides the basis for several reports (e.g., check-ins by offender, check-ins by date, check-ins by venue, etc.), and allows a Community Supervision Officer to determine if an offender did not check-in for a schedule or required event.

3.5 What controls exist to protect the consolidated data and prevent unauthorized access?

Entry of data by the offender is limited to entry of his/her PIN and the hand biometric scan, which are required every time the offender checks-in for an event. A by-pass for the hand biometric scan can be given (e.g., in a situation where the offender has a broken hand or arm), however, entry of the PIN is always required.

Access to the data by CSOSA staff members is controlled by username, password and role. CSOSA uses Active Directory to maintain a central username and password for each CSOSA staff member. Each time a CSOSA staff member logs onto the biometric verification system, his/her username and password are verified by Active Directory as being a successful match before access to the biometric verification system is given. All CSOSA staff member access within the biometric verification system is controlled by role. Roles define who can do what within the biometric verification system. For example: Check-in for drug testing, check-in for office visit, and check-in for a specific program (e.g., educational instruction, treatment program), are all separate functions performed by CSOSA staff members in different roles within the biometric verification system.

The biometric verification system is in the process of meeting the federal requirements for system security. The System Security Plan documents the system controls needed for the biometric verification system (technical, public access, information sharing, contingency planning, and personnel) and how the controls have been implemented. More information can be found in Section 6.0 SECURITY of this Privacy Impact Assessment.

3.6 Will the system monitor the public?

The only "public" users with access to the biometric verification system are those offenders under CSOSA supervision who have been enrolled into the biometric verification system. For every offender check-in, the biometric verification system records and maintains successful and failed check-in attempts, and the CSOSA staff member who assisted.

All systems at CSOSA are monitored through the technology used to implement the system. This monitoring is not evident or available for review through the biometric verification system technology. For the biometric verification system, there are IIS logs (monitors accesses of the biometric verification application), SQL Server logs (monitors accesses of the database) and server logs which contain events captured in Windows Event Viewer. 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 from the biometric verification system are aggregated with logs from other systems and automated tools go through the aggregated logs searching for global intrusions and unauthorized access. The logs are reviewed manually on a periodic basis. The logs are used when an offender or CSOSA staff member questions how information was entered into the biometric verification system or by whom, or there are questions about how information in the biometric verification system was used by CSOSA staff members.

3.7 Will the system monitor employees or contractors?

The biometric verification system/database maintains a history of each successful check-in by the offender, as well as the name of the CSOSA staff member who assisted the offender with the check-in.

Contractors do not have access to the biometric system.

All systems at CSOSA are monitored through the technology used to implement the system. This monitoring is not evident or available for review through the biometric verification system technology. All CSOSA staff members are made aware that accessing any system, including the biometric verification system, constitutes agreement to be monitored through a warning that displays when he/she logs into the system. For the biometric verification system, there are IIS logs (monitors accesses of the biometric verification application), SQL Server logs (monitors accesses of the database) and server logs which contain events captured in Windows Event Viewer. 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 from the biometric verification system are aggregated with logs from other systems and automated tools go through the aggregated logs searching for global intrusions and unauthorized access. The logs are reviewed manually on a periodic basis. The logs are used when an offender or CSOSA staff member questions how information was entered into the biometric verification system or by whom, or there are questions about how information in the biometric verification system was used by CSOSA staff members.

3.8 What kinds of reports can be produced on individuals? Will the data included in the reports produced be anonymized?

The biometric verification system does not contain or produce any reports. The information is pulled into CSOSA's Enterprise Data Warehouse. Reports are generated from CSOSA's Enterprise Data Warehouse.

Alerts and reports are made available to CSOSA staff members (only – offenders do not have access to reports) through the CSOSA Portal (CSOSA staff view into CSOSA's Enterprise Data Warehouse) based on the data in CSOSA's Enterprise Data Warehouse. The alerts and reports made available through the CSOSA Portal for offenders who checked-in through the biometric verification system include: Check-ins by offender, check-ins by date, check-ins by location, check-ins by venue, etc. The information in the reports is not anonymized as the Community Supervision Officer needs to know the exact offender in order to follow up and take appropriate action.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will CSOSA mitigate these risks?

As noted in the response to Question 3.3, all of the data in the biometric verification system relates to and supports one or more of the stated purposes. Offenders who are enrolled in the biometric verification system are made aware of the data they will be required to provide. The option to decline use of the biometric verification system is being explored, but is dependent on finding an alternative solution which is more robust than the current physical sign-in logs for accurate offender identification.

There currently are no identified privacy risks associated with data minimization at this time.

SECTION 4.0

Limits on uses of information

CSOSA will publish a notice about how we plan to use and share the PII that we collect from you. We will only share your PII in ways that are compatible with the notice or as stated in the Privacy Act.

4.1 Is the information in the project limited to only the information that is needed to carry out the purpose of the collection?

As described in the response to Question 3.3, the personally identifiable information collected and used through the biometric verification system is limited to the personally identifiable information needed to meet the purposes of the biometric verification system. The collected information allows CSOSA staff members to verify the identity of the offender electronically "checking-in" for office visits, programs, and drug lab testing, as well as provides an electronic tracking of offender attendance. Use of a view of offender data from the staging database/staging tables eliminates the need to re-collect and store personally identifiable information in the biometric verification system which is already available through CSOSA's case management system.

CSOSA ensures that the personally identifiable information collected through the biometric verification system is used in ways that are compatible with the purposes for which the information was collected through the following:

- Policy: CSOSA is currently working on a Operational Instruction that will describe the data to be collected from the offender, the venues where biometric verification will be available and used, when the hand biometric by-pass functionality is to be used, actions to be taken by CSOSA staff members when assisting an offender with checking-in through biometric verification, CSOSA staff member verification of offender identity at check-in, and alternatives should an offender decline participation in biometric verification.
- Reports through CSOSA's Enterprise Data Warehouse: The alerts and reports made available through the CSOSA Portal to CSOSA staff members about offenders who are checking-in through the biometric verification system are limited to the information available from the biometric verification system. These alerts and reports provide CSOSA staff members with the information needed to confirm an offender attended required events and programs so that CSOSA staff members can follow up (such as not finding check-in information on an offender who was scheduled to attend a specific event).

4.2 Will CSOSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will CSOSA share the information?

There is no sharing of information directly from the biometric verification system/database with individuals or systems external to CSOSA.

Any information shared on offenders would be aggregated within CSOSA's Enterprise Data Warehouse, and shared at a summary level; or would be limited to sharing of information from CSOSA's case management system with individuals performing a law enforcement function who have a need to know, as allowed by the Privacy Act and other similar regulations (e.g., HIPPA).

As a Federal agency, CSOSA is required to respond to Freedom of Information Act requests. CSOSA does exercise privacy and other controls allowed by the Freedom of Information Act, such as the redacting of individual information, when needed.

4.3 Is the information collected directly from the individual or is it taken from another source?

The information in the biometric verification system/database comes from one of four sources:

- From another CSOSA IT system: When an offender is enrolled in or checks in through the biometric verification system, specific existing data on the offender is pulled in and displayed from a staging database/staging tables associated with CSOSA's case management system. The list of data is included in the response to Question 3.2.
- The individual (offender): The offender enters his/her PIN, and uses his/her right hand for the biometric scan each time the offender checks-in through the biometric verification system.
- Generated by the biometric verification system: The biometric verification system generates the Probationer ID, which is the key used throughout the system to link the offender's information together regardless of the source of entry. The biometric verification system also generates the date of check-in, time of check-in, location (as defined by the location associated with the selected hand reader), and venue (as defined by the CSOSA staff member who is assisting with the check-in).
- Entered by CSOSA staff: CSOSA staff members are responsible for maintaining and updating the system settings for on-going use of the biometric verification system by the offender. The information entered by staff includes the capture of the hand biometric (offender's right hand), recapture of the hand biometric when needed, entry of the biometric by-pass (if needed), and assisting with all check-ins by selecting the venue and the hand reader to be used for the check-in.

4.4 Will the project interact with other systems, whether within CSOSA or outside of CSOSA? If so, how?

The biometric verification system does interact with other systems internal to CSOSA, but does not interact with any system external to CSOSA.

The internal systems the biometric verification system/database interacts with are:

- CSOSA's case management system:
  - Existing data on the offender is pulled in and displayed through the biometric verification system from a staging database/staging tables associated with CSOSA's

  case management system. The real-time electronic pull of the data for the offender is triggered by the manual search for the data of an offender, or the successful completion of a biometric hand scan while checking-in.
  - The information is read-only from the staging database/staging tables and is pulled in for display through the biometric verification system electronically.
  - Access to the staging database/staging tables is read-only. Only CSOSA's case management system can write data to the staging database/staging tables. All other access, including the biometric verification system, is read-only.
  - The System Security Plan defines the system boundaries for the biometric verification system. The SMART System Security Plan defines the system boundaries for CSOSA's case management system. These documents contain the technical details for the access controls and the parameters of the information sharing.
- CSOSA's Enterprise Data Warehouse:
  - Information on offender check-ins is pulled electronically from the biometric verification database into CSOSA's Enterprise Data Warehouse on a nightly basis. Check-ins by offender, check-ins by date, and check-ins by venue are some of the reports available to CSOSA staff members through CSOSA's Enterprise Data Warehouse.
  - The information is read-only from the biometric verification database and is pulled by CSOSA's Enterprise Data Warehouse.
  - The System Security Plan defines the system boundaries for the biometric verification system. The EDW System Security Plan defines the system boundaries for CSOSA's Enterprise Data Warehouse. These documents contain the technical details for the access controls and the parameters of the information sharing.
- General Support Structure (GSS):
  - The GSS provides the network, connectivity, network-attached hand readers, system security, and workstations needed by the biometric verification system.
  - CSOSA uses Active Directory to maintain a central username and password for each CSOSA staff member. Each time a CSOSA staff member logs onto the CSOSA network, his/her username and password is verified by Active Directory as being a successful match before access to any specific system is given. A separate login is required for each system, including the biometric verification system.
  - The System Security Plan defines the system boundaries for the biometric verification system. The GSS System Security Plan defines the system boundaries for CSOSA's General Support Structure. These documents contain the technical details for the access controls and the parameters of the information sharing.

4.5 Are there any privacy risks for this project that relate to use limitation? If so, how will CSOSA mitigate these risks?

The biometric verification system does interact with other systems internal to CSOSA, but does not interact with any system external to CSOSA.

The privacy risks related to the internal use of the information are:

- The individual (offender): Making sure the offender understands how the biometric verification system information is used by CSOSA staff members.

- From another CSOSA IT system: Making sure that CSOSA staff members responsible for check-ins follow up with the Community Supervision Officer in cases where discrepancies are found with the information from the staging database/staging tables associated with CSOSA's case management system.
- Staff training: CSOSA staff members are trained on an annual basis regarding what information about an offender can be released and to whom. While there is no electronic sharing of data from the biometric verification system/database with external parties, CSOSA staff members need to be reminded this includes the lookup and printing of data directly from the biometric verification system.
- CSOSA's Enterprise Data Warehouse: CSOSA staff members who work with CSOSA's Enterprise Data Warehouse are trained on an annual basis regarding what information about an offender can be released and to whom. Release of information from CSOSA's Enterprise Data Warehouse is tightly monitored.

SECTION 5.0

Data quality and integrity

CSOSA will make reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected be verified for accuracy and completeness?

How the information will be verified for accuracy and completeness depends on the source of the data:

- Information from another CSOSA IT system: When an offender is enrolled in or checks-in through the biometric verification system, specific existing data on the offender is pulled and displayed from a staging database/staging tables associated with CSOSA's case management system. The enrollment is done with the offender present because the initial hand scan is captured at enrollment. At the time of enrollment, the CSOSA staff member and the offender are able to review the data pulled and displayed. If issues or discrepancies are found, the CSOSA staff member or the offender can notify the offender's assigned Community Supervision Officer. Issues and discrepancies will be investigated by the assigned Community Supervision Officer, and the data in CSOSA's case management system will be corrected if needed. This information would then be made available to the biometric verification system via updates to the staging database/staging tables.
- Generated by the biometric verification system: Information generated by the biometric verification system will be verified for accuracy and completeness during a database review conducted by CSOSA Office of Information Technology staff members. The database review may be requested or initiated by the offender, the Community Supervision Officer, CSOSA Office of Information Technology staff members, CSOSA staff members working with CSOSA's Enterprise Data Warehouse, or an auditor.
- Viewed by a CSOSA staff member: One of the main purposes of the biometric verification system is accurate verification of offender identity. The display of the data from the staging database/staging tables associated with CSOSA's case management system allows CSOSA staff members to verify the identity of the offender including the use of photo identification, and/or use of descriptive information (such as asking the offender his/her date of birth or for the name of his/her Community Supervision Officer).
- Entered by a CSOSA staff member: Supervisors are responsible for following up and verifying the accuracy of information entered by staff including: The capture of the hand biometric (offender's right hand), recapture of the hand biometric when needed, and entry of the biometric by-pass (if needed). Supervisors are also responsible for following up on CSOSA staff members responsible for assisting with check-ins and verifying the staff know how to use the system and are consistent in the selection of the network-attached hand reader, selection of program (Program venue), and/or selection of floor (Census venue).

5.2 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?

As the offenders and CSOSA staff members continue to use the biometric verification system, they uncover situations where data (such as a hand scan) cannot be captured, or the biometric verification system does not perform as designed. As issues are identified with the biometric verification system, the issues are documented and investigated. If the issue is specific to that offender’s data, either the Community Supervision Officer, or CSOSA Office of Information Technology staff will correct the data. If the issue is determined to be within the application, the Development Team assigned to work on enhancing the biometric verification system will prepare and test a fix so the issues are resolved.

SECTION 6.0

Security

CSOSA must protect PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who will have access to the data in the project? What is the authorization process for access to the project?

Access within the biometric verification system is role based. The following are the roles in the biometric verification system:

- Intake Biometric Attendant: The intake biometric attendant can enroll/register offenders for biometric verification (office visit, program attendance, census, ISCU); capture hand biometrics and provide offenders with their Biometric Verification PIN.
- RSC Census Attendant: The RSC attendant will enroll/register offenders for biometric verification and perform biometric check-in of offenders at the RSC.
- Illegal Substance Collection Unit (ISCU) Attendant: The ISCU attendant will enroll/register offenders for biometric verification; perform biometric check-in of offenders at the ISCU, and manage offenders in the various queues (check-in, process in, and check out).
- Program Attendant: The program attendant will enroll/register offenders for biometric verification and perform biometric check-in of offenders attending various assigned programs (e.g., group sessions, the VOTEE lab, the Day Reporting Center, etc.).
- Office Visit Attendant: An office visit attendant will enroll/register offenders for biometric verification and perform biometric check-in of offenders for office visits.
- Business Analysts: Can assign CSOSA staff members to the various roles in the biometric verification system; edit staff information; maintain lookup values; add and edit messages by location; and set drug testing parameters.
- SuperUser: This role would have the combined abilities of all of the other roles, and can capture and re-capture the offender hand biometric. This is needed by OIT in order to assist users with troubleshooting issues, problems with the biometric verification, offender reporting problems, problems with the hand readers, etc.

CSOSA staff member assignment to each of the roles above is based on supervisory review and approval by the Office to which the staff member is assigned (CSOSA Community Supervision Services, CSOSA Community Justice Programs, CSOSA Office of Information Technology), or a combination of Offices in the case of CSOSA staff member assignment to the Business Analyst or SuperUser roles. A CSOSA staff member can only be assigned to one role in the biometric verification system at a time (a CSOSA staff member can be switched to a different role if needed, but can only have one active role).

- Process and authorization for access: CSOSA staff members who need access to an application submit a Request for Computer Access form (CSOSA/IT-0001) indicating to which system access is needed. The form is reviewed and signed by a Supervisor. Once the network account is established or verified, a work ticket will be opened for an individual in the Business Analyst role to complete the account in the biometric

verification system, including the assignment of the biometric verification role based on the CSOSA staff member's duties.
- Process and policies surrounding termination: CSOSA Policy Statement 2003 provides guidance, procedures and actions regarding handling of network and system accounts in the event of a termination. Notification of a termination can come in several forms: Email, CSOSA staff member formal checkout, or work ticket, depending on the severity of the situation and urgency in getting the account closed. An individual in the Business Analyst role would disable the biometric verification system account.

The following individuals will have access to the data in the biometric verification system:

- Community Supervision Services – Community Supervision Officer, Supervisory Community Supervision Officer, Branch Chief, and Management:
  - Access: Individuals within CSOSA Community Supervision Services would be given access to all of the biometric verification system-related data reports in the CSOSA Portal.
  - Process and authorization for access: CSOSA staff members who need access to an application submit a Request for Computer Access form (CSOSA/IT-0001) indicating to which system access is needed. The form is reviewed and signed by a Supervisor. Once the network account is established or verified, a work ticket will be opened for an individual in the Business Analyst role to complete the account in the biometric verification system, including the assignment of the biometric verification role based on the CSOSA staff member's duties.
  - Process and policies surrounding termination: CSOSA Policy Statement 2003 provides guidance, procedures and actions regarding handling of network and system accounts in the event of a termination. Notification of a termination can come in several forms: Email, CSOSA staff member formal checkout, or work ticket, depending on the severity of the situation and urgency in getting the account closed. An individual in the Business Analyst role would disable the biometric verification system account.
- Development and Database Administrators:
  - Access: Development Team members and database administrators would not have application (offender or user) access in Production. For testing purposes, Development Team members would be given application (offender and user) access in the test environment. Development Team members would have local administrator access to all the biometric verification servers (test and production), access to the application code, access to stored procedures, access to the database through SQL, and access to other necessary components on the servers.
  - Process and authorization for access: The current process consists of an email request to the Infrastructure Team. Approval from the Infrastructure Manager is needed before local administrator access will be granted/implemented. For access to SQL Server and the database, the current process consists of an email request to the database administrator as only the database administrator is authorized to grant access to SQL Server.
  - Process and policies surrounding termination: CSOSA Policy Statement 2003 provides guidance, procedures and actions regarding handling of network and system

accounts in the event of a termination. Notification of a termination can come in several forms: Email, CSOSA staff member formal checkout, or work ticket, depending on the severity of the situation and urgency in getting the account closed.

- Enterprise Data Warehouse Staff:
    - Access: Select staff who work with CSOSA's Enterprise Data Warehouse would be given access to the database server and access to SQL in order to develop the scripts needed to pull the data from the biometric verification database into CSOSA's Enterprise Data Warehouse to generate reports.
    - Process and authorization for access: The current process consists of an email request to the database administrator as only the database administrator is authorized to grant access to SQL Server.
    - Process and policies surrounding termination: CSOSA Policy Statement 2003 provides guidance, procedures and actions regarding handling of network and system accounts in the event of a termination. Notification of a termination can come in several forms: Email, CSOSA staff member formal checkout, or work ticket, depending on the severity of the situation and urgency in getting the account closed.
- Infrastructure:
    - Access: Infrastructure Team members would not have access to the biometric verification application or database. Infrastructure is responsible for the servers and network on which the biometric verification system runs. Infrastructure Team members build new servers, connect servers to the network, troubleshoot issues with the network and connectivity, troubleshoot issues when servers do not respond, patch operating system and other components, perform backups on servers, perform restores of databases and servers, and manage the transfer of applications and data to the disaster recovery site.
    - Process and authorization for access: Approval from the Infrastructure Manager is needed before the local administrator access will be granted/implemented.
    - Process and policies surrounding termination: CSOSA Policy Statement 2003 provides guidance, procedures and actions regarding handling of network and system accounts in the event of a termination. Notification of a termination can come in several forms: Email, CSOSA staff member formal checkout, or work ticket, depending on the severity of the situation and urgency in getting the account closed.

6.2 Has CSOSA completed a system security plan for the information system(s) supporting the project?

The System Security Plan is currently in process of being reviewed and revised. The system identification section of the plan is completed. The Team is currently assessing the security controls selected for the system, and documenting the descriptive information needed to explain how each control has been implemented. Next steps will be to have an independent assessor test the security control implementation, and provide a System Assessment Report – which details if there are any gaps in the way in which the security controls have been implemented, if additional controls need to be implemented, or if some of the controls need to be implemented in a different way. Completed documentation of the Security controls, associated testing and the Security Assessment Report is targeted for mid August 2012.

Completion of the Certification and Accreditation, and the Authority to Operate, are dependent on the results of the assessment of this Privacy Impact Assessment document. The pending determination is whether the biometric verification system is its own system of record, and if a System of Record Notice (SORN) is required. If so, the associated process for publishing the SORN in the Federal Register needs to be resolved before the Certification and Accreditation, and the Authority to Operate, can be completed. If a SORN is required, then the Certification and Accreditation, and the Authority to Operate, will be completed at the point in time the SORN becomes final and public.

6.3 How will the system be secured?

The biometric verification system will be secured through the following controls:

- Physical controls:
  - Network-attached hand readers are located near to the staff responsible for assisting with the check-ins. Some are wall-mounted next to a receptionist desk. Some are within CSOSA office spaces which are accessible through a card reader.
  - Lock boxes have been placed on the Local Area Network jacks and the power outlets to eliminate "inadvertent" unplugging of the hand readers.
  - 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.
  - Workstations used by CSOSA staff members are located within CSOSA office spaces.
  - Only CSOSA issued workstations are connected to CSOSA's network. CSOSA does not allow workstations or laptops not issued by CSOSA to be connected to the network.
  - The servers running the biometric verification application, housing the biometric verification database, and housing the staging database/staging tables for CSOSA's case management system 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 controls:
  - All equipment and components for the biometric verification system run on the CSOSA network and are logically located behind the internal firewall.
  - The servers running the biometric verification application, housing the biometric verification database, and housing the staging database/staging tables for CSOSA's case management system are on a back-channel (isolated) network segment of the CSOSA network. This protects the biometric verification information "in motion" between the application server and the database server, and protects the data while it is being electronically pulled from the staging database/staging tables.
  - There is an IPSEC tunnel between the biometric verification database server and CSOSA's Enterprise Data Warehouse (server) in order to protect the biometric

verification data while it is being electronically pulled by CSOSA's Enterprise Data Warehouse for generating reports.
  - Even though all components are located on the CSOSA network, the biometric verification application is web-based to make it available on CSOSA's Intranet.
  - CSOSA staff member access to the biometric verification application server from their workstations is protected by a Secure Socket Layer (SSL) Certificate.
  - The physical database on the biometric verification database server is protected using transparent data encryption, which protects the data when in the database.
  - A by-pass for the hand biometric scan can be given (e.g., in a situation where the offender has a broken hand or arm), however, entry of the PIN is required every time the offender checks-in through the biometric verification system. If there is no by-pass, the PIN and hand biometric scan are required every time the offender checks-in through the biometric verification system.
  - Access to the data by CSOSA staff members is controlled by username and password. Each time a CSOSA staff member logs onto the biometric verification system, his/her username and password are verified by Active Directory as being a successful match before access to the biometric verification system is given.
  - All staff access within the biometric verification system is controlled by role. Roles define who can do what within the biometric verification system. Please see the response to Question 6.1 for a description of the roles in the biometric verification system.

- Administrative controls:
  - The biometric verification 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 CSOSA staff members are made aware that accessing the biometric verification system constitutes agreement to be monitored through a warning that displays when he/she logs into the biometric verification system.
  - System logs are a critical component of managing authorized and unauthorized access to the biometric verification system. The IIS logs monitor accessing of the biometric verification application, the SQL Server logs monitor accessing of the biometric verification 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 (offenders and CSOSA staff members) are accessing the system, and to search for and identify any unauthorized accesses to the system.
  - The logs from the biometric verification system are aggregated with logs from other systems and automated tools go through the aggregated logs searching for global intrusions and unauthorized access.
  - The logs are reviewed manually on a periodic basis.
  - All components on all biometric verification servers (biometric verification application server, biometric verification database server, and the server housing the staging database/staging tables) are 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.

- Reviews/audits of the database are performed based on a request from the offender, the Community Supervision Officer, CSOSA Office of Information Technology staff members, CSOSA staff members working with CSOSA's Enterprise Data Warehouse, or an auditor
- Security and other audits of the biometric verification system (e.g. review of the System Security Plan, annual FISMA audit, annual financial audit) will be completed as scheduled by CSOSA Office of Information Technology and CSOSA Office of Management and Administration

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

Yes. CSOSA utilizes various network and security technologies, coupled with both automated and manual auditing methods, to monitor network devices, systems, and applications in an effort to detect actual or attempted unauthorized access to agency systems and information.

6.5 Are there any privacy risks for this system that relate to security? If so, how will CSOSA mitigate these risks?

Many of the key documents needed to establish full security for the biometric verification system are still in progress (not completed). Completion of the following activities is critical to establishing and maintaining security for the biometric verification system, including privacy information:

- Privacy Impact Assessment review and the System of Record determination.
- If the biometric verification system is a system of record, all work associated with a System of Record Notice and posting of the final notice in the Federal Register.
- Sign-off on the Records Management Inventory Questionnaire and establishment of a records retention schedule approved by NARA.
- The System Security Plan, including documentation of all security controls. NOTE: This is critical for establishing auditing requirements in addition to accountability.
- The Security Assessment Report (documented findings from the security control and vulnerability testing).
- The plan of action and milestones (actions needed to address any shortcomings identified in the Security Assessment Report).
- A signed Authority to Operate.

The work associated with these activities is being accomplished. CSOSA staff members need to continue to make progress until the work is completed and the documents are signed.

SECTION 7.0

Individual participation

CSOSA will give individuals, in most cases, the ability to access their PII, and allow them to correct or amend their PII if it is inaccurate.

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

At the time that CSOSA implements the biometric verification system CSOSA will:

- Provide an orientation to the biometric verification system for the offender to include information on why the offender is required to provide this specific information, how CSOSA maintains the privacy of personally identifiable information, and how CSOSA uses the provided information.
- Provide a Biometric Verification Enrollment Receipt with a privacy statement which emphasizes why the offender is required to provide this specific information, how CSOSA maintains the privacy of personally identifiable information, and how CSOSA uses the provided information. The enrollment receipt is retained by the offender.

On-going consent to providing the information is assumed each time the offender checks-in through the biometric verification system since the offender is entering his/her PIN and using his/her right hand for the check-in process.

The ability for an offender to opt out of or decline participation in the use of the biometric verification system is being explored, but is dependent on finding an alternative solution for accurate offender identification which is more robust than the current physical sign-in logs.

7.2 What procedures will allow individuals to access their information?

The offender can request a review of his/her information by contacting his/her Community Supervision Officer and setting up a time for the review.

7.3 Can individuals amend information about themselves in the system? If so, how?

Offenders cannot personally amend or update information about themselves in the biometric verification system. Once a check-in is recorded (even in error), it will remain in the system until CSOSA staff members in CSOSA Office of Information Technology are asked to remove the check-in information. The offender can request a review of his/her information by contacting his/her Community Supervision Officer and setting up a time for the review. If discrepancies are found, the issue/discrepancy will be investigated by the assigned Community Supervision Officer, and the data in CSOSA's case management system will be corrected if needed. This information would then be made available to the biometric verification system via updates to the staging database/staging tables. If the discrepancy is found in the check-in data from the biometric verification system, the Community Supervision Officer must request the information be removed by CSOSA staff members in CSOSA Office of Information Technology.

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will CSOSA mitigate these risks?

There currently are no identified privacy risks associated with individual participation at this time.

SECTION 8.0

Awareness and training

CSOSA will train all personnel about the proper treatment of PII.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

CSOSA staff members are trained on an annual basis regarding what information about an offender can be released and to whom. This training includes information on the Privacy Act. This training is general in nature as there are a number of systems in use at CSOSA that help capture, track and manage the large amount of data associated with offender supervision.

Specific to the biometric verification system, CSOSA Office of Information Technology will work with CSOSA Community Supervision Services and CSOSA Office of General Counsel to review the materials being provided to the offenders, and confirm and/or enhance the materials to include information on why CSOSA has chosen to use biometric verification for check-in, how that helps the offender, how CSOSA maintains the privacy of personally identifiable information, and how CSOSA uses the provided information. In reviewing and revising the materials with the CSOSA staff members, those staff members will be given “re-fresher” training on privacy.

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will CSOSA mitigate these risks?

It can be difficult to remember information learned during training on privacy while executing the day-to-day tasks associated with managing offenders on supervision. CSOSA staff members need to be reminded that privacy and the proper handling of personally identifiable information applies to printed materials (e.g., enrollment receipts, orientation materials, printed emails, and hard copy print outs of system issues, etc.), in addition to the system and the electronic information. Follow up reminders are provided by the Supervisors and by CSOSA Office of General Counsel between annual training sessions.

The CSOSA staff members responsible for enrolling/registering offenders for biometric verification need to reinforce with the offender that he/she is responsible for the receipts and printed materials and that those materials contain personal information.

SECTION 9.0

Accountability and auditing

CSOSA is accountable for complying with these principles. We will regularly check that we are meeting the requirements and take appropriate action if we are not doing so.

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

The biometric verification system has several tools and processes associated with the system to ensure that the information is used in accordance with the stated practices. Those tools and processes include:

- The System Security Plan:
  - Documents the boundaries of the biometric verification system including the purpose of the system, the system architecture (interfacing systems), users, roles, and the information included in the system. The plan is signed, confirming the scope of the system meets the stated purpose and objectives without extraneous and redundant information, and putting boundaries around the biometric verification system in order to align use of the biometric verification system with the stated purpose.
  - Documents 200+ security controls (policies, processes, activities, application logs, technical auditing capabilities, etc.) including access (identification and authentication), account management, auditing, configuration management, contingency planning, incident response, media protection, physical and environment needs, personnel, risk, acquisition, connectivity, and information integrity security controls. The biometric verification system is assessed against each of the security controls to validate the system, processes and staff members comply with the requirements of each control as it pertains to the biometric verification system, and that the information in the biometric verification system is used in accordance with the stated practices.
  - Is reviewed each year on a schedule set by CSOSA Office of Information Technology to determine if any changes have been made, document the changes, and re-certify the system for continued operations within federal system security guidelines.
- Audits of the biometric verification system by third parties (e.g. annual FISMA audit, annual financial audit) will be completed as scheduled by CSOSA Office of Information Technology and CSOSA Office of Management and Administration.
- Review of offender interaction with the biometric verification system: The review of offender interaction with the biometric verification system is a key source for validating that the information in the biometric verification system is used for the stated practices. This includes review of successful check-ins, unsuccessful check-ins, CSOSA staff member frequency of successful verifications of the offender’s identity, and offender feedback about issues and problems with the biometric verification system.
- Review of staff actions and use of reports: The review of CSOSA staff member interaction with the biometric verification system is another key source of validation that the information in the biometric verification system is used for the stated practices. This includes the frequency which CSOSA staff members have to re-capture the hand

biometric, and CSOSA staff member feedback about issues and problems with the biometric verification system. In addition, CSOSA staff member frequency of the review and use of the reports and alerts made available through the CSOSA Portal, and CSOSA staff member assessment of the accuracy of the data in the reports, provides insight into the capabilities of the biometric verification system to produce information that aligns with the stated practices.

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will CSOSA mitigate these risks?

Many of the key documents needed to establish accountability for the biometric verification system are still in progress (not completed). Completion of the following activities is critical to establishing and maintaining accountability for the biometric verification system, including privacy information:

- Privacy Impact Assessment review and the System of Record determination.
- If the biometric verification is a system of record, all work associated with a System of Record Notice and posting of the final notice in the Federal Register.
- Sign-off on the Records Management Inventory Questionnaire and establishment of a records retention schedule approved by NARA.
- The System Security Plan, including documentation of all security controls. NOTE: This is critical for establishing auditing requirements in addition to accountability.
- The Security Assessment Report (documented findings from the security control and vulnerability testing).
- The plan of action and milestones (actions needed to address any shortcomings identified in the Security Assessment Report).
- A signed Authority to Operate.

The work associated with these activities is being accomplished. CSOSA staff members need to continue to make progress until the work is completed and the documents are signed.